ESPIONAGE

DISINFORMATION

COUNTER-PROPAGANDA

NEUROSECURITY

MEMETICS

DECEPTION THEORY & PRACTICE

TABLE OF CONTENTS

3 GLOSSARIES AT THE END

ADVERSARY TARGETING CLEARANCE HOLDERS ON SOCIAL MEDIA 20

Air Force CI Legal Briefing 23

COGNITIVE EMOTIONAL CONFLICT 280

COMBATTING DISINFO CAMPAIGNS 293

1 Acknowledgments 295

2 Team Members 296

3 Scope 297

4 Executive Summary 298

5 Recommendations 300

6 1. Disinformation Campaigns Are National Security Threats 303

7 2. Reducing the Supply of Disinformation 306

7.1 2.1. Source Attribution and Anonymity 308

7.1.1 2.1.1. Identifying Foreign Actors 308

7.1.2 2.1.2. Identifying Domestic Actors 311

7.1.3 2.1.3. Uncovering Imposters 314

7.2 2.2. Social Media Algorithms & Fact-Checking 316

7.2.1 2.2.1. Social Media Algorithms 316

7.2.2 2.2.2. Fact-checking 318

8 3. The Demand for Disinformation 323

8.1 3.1. Cognitive Bias 325

8.1.1 Confirmation bias 325

8.1.2 Belief bias 326

8.1.3 Bandwagon effect 326

8.2 3.2. Emotional reactions to disinformation 328
8.3 3.3. The Psychology Behind Sharing Information Online 329
9 4. Media Literacy and Critical Thinking Skills 331
10 Conclusion 336
11 combatting_targeted_cover page.pdf
11.1 Acknowledgments
11.2 Team Members
11.3 Scope
11.4 Executive Summary
11.5 Recommendations
11.6 1. Disinformation Campaigns Are National Security Threats
11.7 2. Reducing the Supply of Disinformation
11.7.1 2.1. Source Attribution and Anonymity
11.7.1.1 2.1.1. Identifying Foreign Actors
11.7.1.2 2.1.2. Identifying Domestic Actors
11.7.1.3 2.1.3. Uncovering Imposters
11.7.2 2.2. Social Media Algorithms & Fact-Checking
11.7.2.1 2.2.1. Social Media Algorithms
11.7.2.2 2.2.2. Fact-checking
11.8 3. The Demand for Disinformation
11.8.1 3.1. Cognitive Bias
11.8.1.1 Confirmation bias
11.8.1.2 Belief bias
11.8.1.3 Bandwagon effect
11.8.2 3.2. Emotional reactions to disinformation

11.8.3 3.3. The Psychology Behind Sharing Information Online

11.9 4. Media Literacy and Critical Thinking Skills

11.10 Conclusion

COMPETING IN GRAY ZONE 341

1 rr2791_cover_for_approval 341

2 rr2791_fnlcompiled_v2 342

COUNTERINTEL AND SEC PROGRAMS 1986 424

Counterintelligence-Documentary-Look 583

DECEPTION THEORY AND PRACTICE 693

Defensive Information Operations 866

DHS-ChineseSocialMediaAntiUS 1223

1 23-123-IA_Social Media China and US_ICPS 17378_CY_V15_19Apr23 1226

2 China Municipal Government Publishing Anti-US Pro-China Social Media Content With Limited Reach_last edits (2)_SIR_unsourced 1223

DHS-CombattingDisinformation-2019 1230

1 Structure Bookmarks

DHS-OnlineForeignInfluenceSnapshot 1258

1 (U--FOUO) IIV - Online Foreign Influence Snapshot August 2022 09232022 1258

1.1 22-389-IA_CYMC Aug Snapshot_ICPS 18195_V9_22Sep22 1258

1.2 FINAL (U--FOUO) IIV - Online Foreign Influence Snapshot August 2022 09232022 1259

2 17-024-IA - IA Customer FDBK_A-LAN_INT_v5 12092021

DISCOVERING DECEPTION ONLINE 1261

DoD-CI-Inquiries 1293

1 INSTRUCTION 1293

FARA ACT 1302
FBI-ChineseTalentPrograms 1304
FBI-DefenseContractorsAPT 1309
FIGHTING BEARS AND TROLLS 1313
1 21Sep_Chan_Elvis_First8 1313
2 21Sep_Chan_Elvis 1321
2.1 I. russia rises from the ashes of the cold war 1337
2.1.1 A. problem statement 1338
2.1.2 B. research question 1339
2.1.3 C. literature review 1340
2.1.3.1 1. Russian Online Influence Activities from 2014 to 2020 1341
2.1.3.2 2. Countermeasures by the Private Sector and the U.S. Government 1346
2.1.3.3 3. Framework for Understanding Russian Hybrid Warfare 1348
2.1.3.4 4. Recommendations for Countering Russian Influence Campaigns 1351
2.1.3.5 5. Conclusions from Literature Review 1354
2.1.4 D. research design 1355
2.2 II. opening moves – scope and background 1359
2.2.1 A. scope of thesis 1360
2.2.1.1 1. Relevant Time Periods 1360
2.2.1.2 2. Types Of Russian Influence Operations 1361
2.2.1.3 3. Targeted Social Media Platforms 1362
2.2.2 B. recent history – the campaigns From 2016 to 2018 1363
2.2.2.1 1. What Happened During the 2016 U.S. Elections? 1365

a. The IRA's Social Media Activities 1366
b. Private Sector Countermeasures 1372
c. U.S. Government Countermeasures 1373
d. Using the Kartapolov Framework to Evaluate Russian & American Measures in 2016 1375
2.2.2.2 2. What Happened During the 2018 U.S. Midterm Elections? 1379
a. The IRA's Social Media Activities 1379
b. Private Sector Countermeasures 1381
c. U.S. Government Countermeasures 1384
d. Using the Kartapolov Framework to Evaluate Russian and American Measures in 2018 1388
2.2.3 C. CONCLUSIONS FROM THE 2016 AND 2018 ELECTIONS 1391
2.3 III. THE 2020 ELECTIONS – RUSSIAN GAMBIT AND AMERICAN COUNTERPLAY 1393
2.3.1 A. THE IRA AND OTHER PROXIES' SOCIAL MEDIA ACTIVITIES 1395
2.3.2 B. PRIVATE SECTOR COUNTERMEASURES 1404
2.3.3 C. U.S. GOVERNMENT COUNTERMEASURES 1411
2.3.4 D. USING THE KARTAPOLOV FRAMEWORK TO EVALUATE RUSSIAN AND AMERICAN MEASURES IN 2020 1416
2.3.4.1 1. The IRA and Other Proxies – Impact and Evolution 1416
2.3.4.2 2. The Private Sector Companies' Impact and Adaptations 1419
2.3.4.3 3. The U.S. Government's Impact – Transparency and Private Sector Partnerships 1421
2.3.5 E. Voter Turnout in the 2020 Elections 1424

2.3.6 F. Conclusions from the 2020 U.S. Elections 1425

2.4 IV. CONCLUSIONS AND RECOMMENDATIONS TO COUNTER RUSSIA IN THE FUTURE 1427

2.4.1 A. CONCLUSIONS – THERE IS NO END GAME 1427

2.4.2 B. RECOMMENDATIONS FOR PROTECTING FUTURE ELECTIONS FROM RUSSIAN INTERFERENCE 1430

2.4.2.1 1. Security Measures 1431

2.4.2.2 2. Transparency Measures 1435

2.4.2.3 3. Resiliency Measures 1439

2.5 LIST OF REFERENCES 1443

2.6 initial distribution list 1461

INFORMATION OPERATIONS AND COUNTERPROPAGANDA 1462

Internal-Counterintelligence-Program-ICIP-ZF0119146W 1499

IRAN INFLUENCE OPS 2406

1 (U--FOUO) IIF - Iranian Influence Efforts Primarily use Online Tools 03032021 2406

2 17-024-IA - IA Customer FDBK_A-LAN_EXT_v6

JOINT CYBER ADVISORY PRC STATE ACTORS 2410

1 Summary 2411

2 Table of Contents 2413

3 Technical Details 2415

3.1 Overview of Activity 2415

3.2 Observed TTPs 2418

3.2.1 Reconnaissance 2418

3.2.2 Resource Development 2418

3.2.3 Initial Access 2418

3.2.4 Execution 2418

4 Summary 2419

4.1 Discovery 2420

4.2 Lateral Movement 2422
4.3 Collection and Exfiltration 2423
4.4 Command and Control 2424
5 Detection/Hunt Recommendations 2425
5.1 Apply Living off the Land Detection Best Practices 2425
5.2 Review Application, Security, and System Event Logs 2425
5.3 Monitor and Review OT System Logs 2428
5.4 Use gait to Detect Possible Network Proxy Activities 2429
5.5 Review Logins for Impossible Travel 2429
5.6 Review Standard Directories for Unusual Files 2429
6 Incident Response 2429
7 Mitigations 2432
7.1 IT Network Administrators and Defenders 2432
7.1.1 Harden the Attack Surface 2432
7.1.2 Secure Credentials 2433
7.1.3 Secure Accounts 2433
7.1.4 Secure Remote Access Services 2434
7.1.5 Secure Sensitive Data 2435
7.1.6 Implement Network Segmentation 2435
7.1.7 Secure Cloud Assets 2435
7.1.8 Be Prepared 2436
7.2 OT Administrators and Defenders 2437
8 Contact Information 2438
9 Validate Security Controls 2439
10 References 2439
11 Resources 2439

12 Disclaimer 2439
13 Acknowledgements 2440
14 Version History 2440
15 Appendix A: Volt Typhoon Observed Commands / LOTL Activity 2441
16 Appendix B: Indicators of Compromise 2445
17 Appendix C: MITRE ATT&CK Tactics and Techniques 2446
MEMES INFORMATION WARFARE 2455
1 21Jun_Cisewski_Katherine_First8 2455
2 21Jun_Cisewski_Katherine 2463
2.1 I. introduction 2473
2.1.1 A. social media, the news, and marketing: what could go wrong? 2473
2.1.2 B. Key Information Dissemination Tools: Tweets and Image macro memes 2474
2.1.3 C. What makes memetic research important? 2476
2.1.4 D. Problem Statement 2479
2.1.5 E. Purpose Statement 2479
2.1.6 F. Research Design 2480
2.2 II. Background 2483
2.2.1 A. The Rise of Social Media 2483
2.2.1.1 1. Social Media as a Community 2484
2.2.1.2 2. Social Media and Activism 2484
2.2.1.3 3. Social Media and Political Appointees 2485
2.2.1.4 4. Social Media and Marketing 2485
2.2.2 B. What makes a meme, a meme? 2486
2.2.3 C. What is Information Disorder? 2490

2.2.4 D. A MEME’S role in Information Disorder Campaigns 2494

2.2.5 E. Twitter’s role in Information Disorder 2496

2.3 III. Related Work 2499

2.3.1 A. Research on Information Disorder with Memes 2499

2.3.1.1 1. Political Memes and Fake News Discourses on Instagram 2499

2.3.1.2 2. Inferring Social Influence and Meme Interaction with Hawkes Processes 2499

2.3.1.3 3. The Evolution of Political Memes: Detecting and Characterizing Internet Memes with Multi-Modal Deep Learning 2500

2.3.2 B. Research on information disorder using Twitter 2500

2.3.2.1 1. Coronavirus Goes Viral: Quantifying the COVID-19 Misinformation Epidemic on Twitter 2501

2.3.2.2 2. The Spread of True and False News Online 2501

2.3.3 C. Influence Effectiveness of Information Disorder 2502

2.3.3.1 1. Does Russian Propaganda Work? 2502

2.3.3.2 2. Understanding What Makes Terrorist Groups’ Propaganda Effective: An Integrative Complexity Analysis of ISIL and Al Qaeda 2503

2.3.4 D. Categorization and Decision Making 2503

2.3.4.1 1. Interference Effects of Categorization on Decision Making 2504

2.3.4.2 2. An Evidential Dynamical Model to Predict the Interference Effect of Categorization on Decision Making Results 2504

2.4 IV. Methodology 2507
2.4.1 A. Hypotheses 2507
2.4.2 B. Experimental Design Overview 2508
2.4.3 C. Tweets and Memes Used 2511
2.4.3.1 1. Tweets Used in the Experimental Design 2511
2.4.3.2 2. Memetics Used in Experimental Design 2525
2.4.4 D. Qualtrics 2539
2.4.4.1 1. Steps to Create the Experiment Designed in this Thesis 2540
2.4.4.2 2. Testing the Survey 2550
2.4.5 E. Limitations 2550
2.5 V. future work, implications, conclusion 2551
2.5.1 A. future work 2551
2.5.2 B. Implications 2551
2.5.3 C. conclusion 2552
2.6 List of References 2553
2.7 initial distribution list 2563
NCIS CI RULES 2564
NCSC-CyberEconomicEspionage 2566
NEUROSECURITY HUMAN BRAIN ELETRO OPTICAL SIGNALS AS MASINT 2586
Office of Public Affairs Former U.S. Military Pilot Admits Acting as Paid Agent of China and Lying on National Security Background Forms United States Department of Justice 2594
Office of Public Affairs Maryland Nuclear Engineer and Wife Sentenced for Espionage-Related Offenses United States Department of Justice 2596

Office of Public Affairs U.S. Government Contractor Arrested on Espionage Charges United States Department of Justice 2597

Office of Public Affairs U.S. Navy Sailor Sentenced to 27 Months in Prison for Transmitting Sensitive U.S. Military Information to Chinese Intelligence United States Department of Justice 2598

Office of Public Affairs U.S. Navy Service Member Pleads Guilty to Transmitting Sensitive U.S. Military Information to Chinese Intelligence Officer United States Department of Justice 2599

OVERVIEW OF PSYCHOLOGICAL OPERATIONS 2600

PSYCHOLOGICAL RESILENCE 2641

1 22Mar_Lkhagvasuren_Bayasgalan_First8 2641

2 22Mar_Lkhagvasuren_Bayasgalan 2649

2.1 I. INTRODUCTION 2657

2.2 II. the literature review and approach 2661

2.2.1 A. Brief Overview of the Literature and Similar Cases 2661

2.2.2 B. Approach 2664

2.3 III. education 2667

2.3.1 A. Youth 2668

2.3.2 B. Government entities 2670

2.3.3 C. Private and Civic sectors 2672

2.3.4 D. Military and law enforcement agencies 2676

2.4 IV. information 2677

2.4.1 A. Social media vulnerabilities 2677

2.4.2 B. Existing political debates 2679

2.4.3 C. Press 2680

2.4.4 D. countermeasures and Mongolian exposures 2682

2.4.5 E. civic-government partnership on information 2683
2.5 V. SOCIAL INCLUSION FOR YOUNG PEOPLE 2685
2.5.1 A. WHAT IS SOCIAL INCLUSION? 2685
2.5.2 B. WHY IS IT IMPORTANT? 2685
2.5.3 C. WHAT ARE THE CURRENT EFFORTS? 2686
2.5.3.1 1. National Identity and Shared National Values 2687
2.5.3.2 2. National Language and Script 2689
2.5.3.3 3. Mongolia and Nomadic Lifestyles 2691
2.6 VI. CONCLUSION AND RECOMMENDATIONs 2693
2.6.1 A. RECOMMENDATIONs 2695
2.6.2 B. AREAS FOR FURTHER STUdY 2699
2.7 List of References 2701
2.8 initial distribution list 2709
PSYCHOLOGY OF DISINFORMAITON KEY MECHANISMS 2710
1 Cover for Disinfo Pt 1 2710
2 DRM-2021-U-029337-1Rev revised for public release 2714
3 Cover for Disinfo Pt 1 2782
4 Blank Page 2713
REPORTING OF COUNTERINTEL AND SECURITY INDICATORS BY SUPERVISOR AND COWORKERS 2784
ROLE OF OVERT AND COVERT COMMS ONLINE 2841
1 22Mar_Dimitrov_Boyan_First8 2841
2 22Mar_Dimitrov_Boyan 2849
2.1 I. INTRODUCTION 2859
2.2 II. LITERATURE REVIEW 2863
2.2.1 A. iNFORMATION OPERATIONS AND SOCIAL MEDIA 2863

2.2.2 B. methods of STUDYING iNFORMATION OPERATIONS 2869
2.3 III. information warfare: The Bear and the dragon 2873
2.3.1 A. Information confrontation, Information warfare, and Information Operations 2873
2.3.2 B. social media in Information Warfare 2878
2.4 IV. RESEARCH METHODS 2887
2.4.1 A. HYPOTHESES 2887
2.4.2 B. DATA AND METHODS 2887
2.4.2.1 1. Datasets 2887
2.4.2.2 2. Sentiment Analysis and Text Processing of Social Media Data 2888
2.4.2.3 3. Network Topography Measures 2889
2.4.2.4 4. Dependent Variables 2889
2.4.2.5 5. Independent Variables 2890
2.4.2.6 6. Control Variables 2891
2.4.3 C. REGRESSION ANALYSIS 2892
2.5 V. REGRESSION RESULTS 2893
2.5.1 A. russian online influence ON Social Media sentiment 2893
2.5.1.1 1. Findings 2893
2.5.1.2 2. Analysis of the Findings 2896
2.5.2 B. NETWORK MEASURES AND RUSSIAN ONLINE INFLUENCE 2900
2.5.2.1 1. Analysis of the Findings 2902
2.5.3 C. DiscussioN 2904
2.6 VI. conclusions 2909
2.7 List of References 2913
2.8 initial distribution list 2919

SOF INFORMATION SYSTEMS 2920
1 Cover 2920
2 Contents 2922
3 Preface 2927
4 Chapter 1: Fundamentals 2928
4.1 INFORMATION OPERATIONS 2929
4.2 THE INFORMATION ENVIRONMENT 2930
4.3 INFORMATION SUPERIORITY 2931
4.4 INFORMATION OPERATIONS CAPABILITIES 2932
4.5 CONSIDERATIONS 2932
4.6 CONCLUSION 2932
5 Chapter 2: Information Operations Capabilities and Tactics 2934
5.1 OPERATIONS SECURITY 2935
5.2 MILITARY DECEPTION 2938
5.3 MILITARY INFORMATION SUPPORT OPERATIONS 2944
5.4 ELECTRONIC WARFARE 2948
5.5 COMPUTER NETWORK OPERATIONS 2949
5.6 COMBAT CAMERA 2950
5.7 LOCAL POPULACE AND KEY-LEADER ENGAGEMENTS 2952
5.8 COUNTERING ADVERSARY INFORMATION ACTIVITIES 2959
5.9 REWARDS PROGRAMS 2962
5.10 CIVIL-MILITARY OPERATIONS 2963
5.11 PUBLIC AFFAIRS 2964
5.12 DEFENSE SUPPORT TO PUBLIC DIPLOMACY 2964
6 Chapter 3: Planning Information Operations 2974
6.1 THE STAFF ESTIMATE FOR INFORMATION OPERATIONS 2975

6.2 PLANNING CONSIDERATIONS DURING MISSION ANALYSIS 2975
6.3 MISSION ANALYSIS WORK SHEET 2980
6.4 COURSE OF ACTION DEVELOPMENT 2980
6.5 CONSIDERATIONS 2992
6.6 CONSEQUENCE MANAGEMENT 2992
7 Chapter 4: Execution of Information Operations 2994
7.1 MONITORING 2994
7.2 EVALUATING 2994
7.3 ADJUSTING 2996
7.4 REPORTING 3001
8 Chapter 5: Intelligence Support to Information Operations 3002
8.1 INFORMATION OPERATIONS AND THE INTELLIGENCE CYCLE 3003
8.2 INTELLIGENCE “PUSH” AND “PULL” 3003
8.3 REQUESTS FOR INFORMATION 3004
8.4 INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT 3004
8.5 VISUALIZING THE INFORMATION ENVIRONMENT 3004
8.6 THE COMBINED INFORMATION OVERLAY 3006
8.7 ADVERSARY OPERATIONS IN THE INFORMATION ENVIRONMENT 3007
8.8 TEMPLATING USING CENTER-OF-GRAVITY ANALYSIS 3008
8.9 ADVERSARY ACTIVITIES IN THE INFORMATION ENVIRONMENT 3010
8.10 CONSIDERATIONS 3010
9 Appendix A: Planning Aids 3012
10 Appendix B: Tactical Deception Aid 3038
11 Appendix C: Tactical Operations Security Aid 3042

12 Appendix D: Media Assessment Aid 3046
13 Appendix E: Conducting Face-to-Face Meetings 3052
14 Appendix F: How to Use Translators 3054
15 Glossary 3056
16 References 3060
17 Index 3062
18 Authentication 3064
19 PIN 3065
SUBVERSIVE INFLUENCE VULNERABILITIES OF THE US AND ITS ELECTIONS TO RUSSIAN INTERF 3066
1 20Dec_Mcmasters_Daniel_First8 3066
2 20Dec_McMasters_Daniel 3074
2.1 I. Introduction 3084
2.1.1 A. RESEARCH QUESTION 3085
2.1.2 B. LITERATURE REVIEW 3086
2.1.2.1 1. Russia’s Intent, Capability, and Mechanisms 3086
2.1.2.2 2. 21st Century Vulnerabilities 3090
2.1.3 C. RESEARCH DESIGN 3095
2.1.4 D. OVERVIEW OF CHAPTERS 3095
2.2 II. A Century of Kremlin Interference: Dirty Tricks Past and Present 3098
2.2.1 A. THE ORIGINAL THREAT 3098
2.2.1.1 1. Media Manipulation 3099
2.2.1.2 2. Secret Proxy Organizations 3104
2.2.1.3 3. Forgeries and Rumors 3106
2.2.1.4 4. Manipulating Multiple Sides, Instigating Groups against Each Other, and Inciting Violence 3108

2.2.1.5 5. Diminishing Returns, Lasting Impacts 3109
2.2.2 B. CONTEMPORARY ADAPTATIONS AND NEW THREATS 3111
2.2.2.1 1. Media Manipulation 3111
a. Co-opting Journalists and Using Outside Media to Influence News Coverage 3116
b. Inventing and Planting Stories in the Internet Age 3116
2.2.2.2 2. Proxy Organizations 3121
2.2.2.3 3. New Threats and Force Multipliers: Cyberattacks 3127
2.2.2.4 4. Relative Impunity 3132
2.3 III. Election Interference 3134
2.3.1 A. Soviet Meddling in U.S. Elections 3134
2.3.2 B. Modern Meddling in U.S. Elections 3137
2.3.2.1 1. State-Run Media 3137
2.3.2.2 2. Social Media 3140
2.3.2.3 3. Microtargeting 3147
2.3.2.4 4. Hacking and Cyberattacks 3148
2.3.3 C. Other Modern Russian Efforts to Influence Foreign Elections 3151
2.4 IV. Fallout and Vulnerabilities 3158
2.5 V. Conclusion 3170
2.6 List of References 3172
2.7 initial distribution list 3202
THE EVOLUTION OF STRATEGIC INFLUENCE 3203
US Army intelligence analyst charged with selling military secrets to China Reuters 3264
Counter Intelligence Glossary - Terms and Definitions of Interest for CI Professionals - Joint Military Intelligence College (1997) 3265

1 Cover 3265
2 Abbreviations and Acronyms 3270
2.1 A 3270
2.2 B 3292
2.3 C 3297
2.4 D 3323
2.5 E 3338
2.6 F 3346
2.7 G 3355
2.8 H 3360
2.9 I 3365
2.10 J 3378
2.11 K 3388
2.12 L 3390
2.13 M 3397
2.14 N 3411
2.15 O 3424
2.16 P 3430
2.17 Q 3440
2.18 R 3441
2.19 S 3448
2.20 T 3468
2.21 U 3481
2.22 V 3489
2.23 W 3492
2.24 X 3495
2.25 Y 3496
2.26 Z 3498

3 Codes for Goepolitical Areas 3499
4 Geopolitical Areas by Code 3508
COUNTERINTELLIGENCE GLOSSARY 3518
INFOSEC GLOSSARY 3877

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

INFORMATION TECHNOLOGY SECTOR

1 April 2019 **LIR 190401001**

US Adversaries Exploit Social Media Information to Target US Individuals and Government Clearance Holders

The FBI's Washington Field Office, in coordination with the FBI's Office of Private Sector (OPS), is informing private sector partners regarding foreign intelligence services' (FIS) exploitation of social media platforms[a] and data to target corporate and US government (USG) clearance holders. FIS and US adversary intelligence officers are using popular US-based social media platforms to identify, recruit, and conduct operations against USG clearance holders, to include private sector employees or contractors supporting the USG. FIS officers will use popular US-based platforms and their respective countries' social media platforms for personal and intelligence gathering/operations purposes.

The FBI reminds US clearance holders and/or individuals with access to US sensitive/proprietary information to remain vigilant, and adhere to strict operational security protocols in their physical and online presence. Increasing physical and online operational security awareness, using best practices, and training may limit FIS solicitation attempts/activities. Visit the FBI's Domestic Security Alliance Council, InfraGard, and the FBI's Counterintelligence homepage for information and brochures related to FIS, as well as, material on insider threat awareness:

- www.fbi.gov/investigative/counterintelligence
- www.dsac.gov
- www.infragard.org

FIS Primary Targets: Former/Active USG Clearance Holders

In 2017, an FIS used a popular professional networking website to contact a former USG employee who held an expired Top Secret level clearance. The employee listed their intelligence/national security background on their website profile. A separated but recruited individual later acted as the "middleperson" who introduced the employee to the FIS. In February 2017, the employee traveled overseas to meet the FIS and established a covert communication channel. That communication channel served as a mean to pass Secret and Top Secret information to a US adversary. In mid-2017, the USG arrested and charged the employee for conducting espionage against the United States.

FIS Private Sector Targets: USG Contractor Clearance Holders

A known FIS front company used a publicaly available employment website to target USG defense contractors who posted their resume online. The FIS used the website to target, assess, and recruit

[a] The term **social media platform** refers to as a broad range of private to public communication, employment networking, interaction, and file sharing featured tool via websites, as well as, applications on smart-devices and/or computer systems.

employees of US-based defense contracting companies supporting the USG who have specialized skills in the aviation technology.

Social Engineering Method: FIS use Fictitious Social Media Accounts to Obtain Access to Sensitive and Classified Data from USG and Corporate Employee

An FIS created a fictitious US military social media profile on several platforms. The FIS used the profile to establish online relationships/social network with a wide range of USG, US military personnel, and multiple US-based cleared defense contractors. The FIS used the social network to develop and assess a targeted pool of profiles.

Bridging the Physical and Online Introductions Gap: FIS Used Physical Events and Online Research for Social Media Usage to Establish Relationships

In early 2018, a US-based cleared defense contractor with a Top Secret level clearance attended a technical trade show conference in the United States. An FIS who operated a vender booth at the conference approached the contractor several times and offered sales of products/services. As a means to deter the aggressive sales pitches, the contractor indicated to the FIS his/her affiliation with the USG and offered the FIS a business card. A week after the conference, the FIS located the contractor on a popular professional linking website. The FIS sent an online request to the contractor via the website. The FIS is likely associated with an identified US adversarial military unit.

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Air Force Office of Special Investigations

Eyes of the Eagle

CI Cyber Authorities Legal Briefing

Sept 2016

U.S. AIR FORCE

Overview

- Legal Framework
- DoDM 5240.01 Overview
- Computer Trespasser Exception
- Scenarios

Page 24 of 3957

CI Cyber Legal Framework

Legal Framework—The Basics

- U.S. Constitution
- U.S. Code
  - FISA
  - ECPA
  - Computer Fraud and Abuse Act
  - Computer Trespasser Exception
  - National Security Letters
- Executive Order 12333
- DoD/USAF Issuances
  - DoDM 5240.01 (Procs 1-10)
  - DoD 5240.1-R (Procs 11-15)
  - AFI 71-101 v4

Legal Framework—History

- Spying is one of the oldest professions
  - General George Washington noted during the War of Independence "it was the British spies he feared the most."

- Today's laws and policies are the direct result of unfettered intelligence collection by DoD, FBI and CIA in the 1960's and 1970's.
  - Physical surveillance of public figures involved with the anti-Vietnam war and civil rights protests, e.g., MLK
  - Mail openings
  - Break-ins of the offices, vehicles and houses of U.S. persons
  - Undisclosed participation on university campuses

Legal Framework—History

- The Church and Pike congressional committees found the IC lacked policy on how to conduct its mission in regards to U.S. persons
  - Recommended "reining" in Executive Branch powers in using intelligence elements against U.S. persons
  - Created the Permanent Select Committee on Intelligence (Senate) and the Congressional Committee on Intelligence
  - The Foreign Intelligence Surveillance Act was enacted in 1978
- Before Congress passed legislation to correct this deficiency, E.O. 11905 was signed, which was later replaced by E.O. 12333 (standing E.O. on Intelligence Oversight)

DoDM 5240.01 Overview

DoD MANUAL 5240.01

PROCEDURES GOVERNING THE CONDUCT OF DoD INTELLIGENCE ACTIVITIES

Originating Component	Office of the Deputy Chief Management Officer of the Department of Defense
Effective:	Month Day, Year
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.dtic.mil/whs/directives
Incorporates and Cancels:	Directive-type Memorandum 08-011, "Intelligence Oversight Policy Guidance," March 20, 2008 Procedures 1-10 of DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982
Approved by:	Loretta E. Lynch, Attorney General of the United States Ashton B. Carter, Secretary of Defense

Purpose: In accordance with the authority in DoD Directive 5240.01 and Executive Order (E.O.) 12333, this issuance:

- Establishes procedures to enable DoD to conduct authorized intelligence activities in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons. DoD authorized intelligence activities are foreign intelligence and counterintelligence (CI) activities unless otherwise specified in this issuance.
- Authorizes the Defense Intelligence Components to collect, retain, and disseminate information concerning U.S. persons in compliance with applicable laws, Executive orders, policies, and regulations.

Page 29 of 3957

DoDM 5240.01 Overview

- Signed by SecDef and Attorney General August 2016
- Replaces Procedures 1-10 of DoD 5240.01-R (December 1982)
- Ten (10) Procedures
  - Proc 2, Collection
  - Proc 3, Retention
  - Proc 4, Dissemination
  - Proc 5, Electronic Surveillance
  - Proc 6: Concealed Monitor
  - Proc 7, Physical Search
  - Proc 8, Mail Search/Cover
  - Proc 9, Physical Surveillance
  - Proc 10, Undisclosed Participation

DoDM 5240.01, Counterintelligence

- **Defined: Information gathered and activities conducted to *identify, deceive, exploit, disrupt,* or *protect* against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.**

Procedure 2, Introduction

- **Intentional Collection of USPI: We may *intentionally* collect USPI *only* if:**
  - **the information sought is *reasonably believed* to be *necessary* for the performance of an authorized counterintelligence mission;**
  - **the USPI falls within one of the following 13 categories below; and**
  - **we use the least intrusive means.**

- **U.S. Person Information (USPI) defined: Information that is reasonably likely to identify one or more specific U.S. persons.**

- **Collection takes place upon receipt**
  - **Regardless of when you use it**
  - **Computers can collect**
  - **Intel is collected only once**
  - **May be disseminated multiple times**
  - **Encrypted data is considered collected upon receipt**

Procedure 2, Reasonable Belief

- **Defined: When the facts and circumstances are such that a reasonable person would hold the belief.**
  - **Must rest on facts and circumstances that can be articulated;**
  - **Hunches or intuitions are not sufficient; and**
  - **Can be based on experience, training, and knowledge of CI activities as applied to particular facts and circumstances.**

Procedure 2 Categories

1. Publicly Available
2. Consent
3. Foreign Intelligence (FI)
4. Counterintelligence (CI)
5. Threats to Safety
6. Protection of Sources/Methods
7. Current, Former, or Potential Sources
8. Persons in Contact With Sources or Potential Sources
9. Personnel Security
10. Physical Security
11. Communications Security
12. Overhead and Airborne Reconnaissance
13. Administrative Purposes

Procedure 2 Categories

1. **Publicly Available Information**
2. **Consent**
   - **Defined: An agreement by a person or organization to permit a Defense Intelligence Component to take particular actions affecting that person or organization.**
   - **The legal advisor [OSI/JA] will determine whether a notice or policy is adequate and lawful, before the Component takes or refrains from taking action on the basis of implied consent.**
3. **Foreign Intelligence**

Procedure 2 Categories

4. **Counterintelligence: The information is *reasonably believed* to constitute CI and the U.S. person is one of the following:**
   - (a) **An individual, organization, or group reasonably believed to be engaged in or preparing to engage in espionage, other intelligence activities, sabotage, or assassination on behalf of a *foreign* power, organization, or person, or on behalf of an agent of a *foreign* power, organization, or person;**
   - (b) **An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist activities;**
   - (c) **An individual, organization, or group reasonably believed to be acting for, or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States; or**
   - (d) **An individual, organization, or group *in contact with a person described above* for the purpose of identifying such individual, organization, or group and assessing any relationship with the person described therein.**

Procedure 2, Other

- **Special Circumstances Collection**
  - Defense Intelligence Components will consider whether collection opportunities raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information.
- **Amount of Information Collected**
  - In collecting non-publicly available USPI, to the extent practicable, collect no more information than is reasonably necessary.
- **Least Intrusive Means**
  - Use the least intrusive collection techniques feasible within the United States or directed against a U.S. person abroad.
    1. Publicly available sources or with the consent of the person concerned
    2. Cooperating sources
    3. Techniques that do *not* require a judicial warrant or AG approval
    4. Techniques that do require a judicial warrant or AG approval

Procedure 3, Retention

- **Permanent Retention standard**
  - Retention is reasonably believed to be necessary for the performance of an authorized intelligence mission; and
  - The information was lawfully collected or disseminated to the Component
    - Meets one of the 13 collection categories; or
    - Is necessary to understand or assess CI, e.g., information about a U.S. person that provides important background or context for CI.

Procedure 3, Retention

- Three primary evaluation periods to determine retention of USPI
  - Promptly
  - Five (5) years
  - Twenty-five (25) years

- Intentional Collection of USPI
  - Must be evaluated promptly; and
  - If *necessary*, may retain the information for evaluation for up to 5 years, subject to extension.

Procedure 3, Retention

- **Incidental Collection of USPI**
  - Defined: collection of USPI that is not deliberately sought, but is nonetheless collected
  - *In the United States,* may retain all of the incidentally collected information for evaluation for up to 5 years, unless extended
  - *Outside the United States, may* retain all of the incidentally collected information for evaluation for up to 25 years.

- **Voluntarily Provided USPI**
  - About a U.S. person, evaluate the information promptly, up to 5 years, unless extended.
  - About a non-U.S. person, evaluation for up to 25 years.

Procedure 3, Retention

- **Unintelligible information**
  - The time periods begin when the information is processed into intelligible form
  - Includes information that a Component cannot decrypt or understand in the original format.
  - To the extent practicable, unintelligible information will be processed into an intelligible form.
  - A foreign language is considered intelligible

- **Deletion of Information.**
  - Unless the standards for permanent retention are met, must delete all USPI from the Component's automated systems of records.

Procedure 4, Dissemination

- We may disseminate USPI based upon the following criteria:
  - Any person or entity: Information is publicly available or U.S. person has consented to the dissemination.
  - Other intelligence community elements
  - Other DoD elements; federal government entities; state, local, tribal, or territorial governments: recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.
  - Foreign governments or international organizations
    - Recipient is reasonably believed to have a need to receive such information for its lawful missions or functions; and
    - Disclosure is consistent with applicable international agreements and foreign disclosure policy
  - Protective Purposes: Necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security.

Procedure 5, Electronic Surveillance

- Implements FISA and E.O. 12333
- Defined
  - The installation or use of any monitoring device in the United States where a person has a reasonable expectation of privacy, as determined by *OSI/JA*, and
  - A warrant would be required for law enforcement purposes.
- Fourth Amendment
  - All electronic surveillance must comply with the Fourth Amendment
  - *OSI/JA* will assess the reasonableness of collection, retention, and dissemination

Procedure 5, Electronic Surveillance

- In the United States
  - Attorney General or the Foreign Intelligence Surveillance Court (FISC) may authorize, except for emergency situations.
  - May only conduct such surveillance if both:
    - A *significant purpose* of the electronic surveillance is to obtain foreign intelligence information; and
    - There is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power.

Procedure 5, Electronic Surveillance

- Outside the United States
  - U.S. person
    - Governed by FISA and E.O. 12333; or
    - Approval under exigent circumstances exception
  - Non-U.S. person: governed by Title I or Section 702
- Emergency situations: Attorney General approval
- Technical Surveillance Countermeasures (TSCM)
  - Applies to the use of electronic equipment and specialized techniques to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance.

Procedure 6, Concealed Monitoring

- **Defined as the following:**
  - Hidden electronic, optical, or mechanical devices,
  - to monitor a particular person or a group of persons,
  - without *consent*,
  - in a surreptitious manner,
  - over a period of time, and
  - no *reasonable expectation of privacy*.
- **Examples**
  - Video monitoring or sound recording of a subject in a place where he or she has no reasonable expectation of privacy if conducted over a period of time
  - Taking one photograph of a subject would ***not*** qualify.

Procedure 6, Concealed Monitoring

- **Scope**
  - ***Any*** **person inside the United States, or**
  - **Any U.S. person outside the United States**
- **In the United States**
  - **On DoD facilities**
  - **Outside DoD facilities, after coordination with the FBI.**
- **Outside the United States**
  - **On DoD facilities**
  - **Outside DoD facilities must be coordinated with the CIA, and appropriate host country officials in accordance with any applicable SOFA or other international agreement.**

Procedure 6, Concealed Monitoring

- Approval: AFOSI/CC or delegee
- OSI/JA will determine whether the following criteria have been met:
  - There is no reasonable expectation of privacy;
  - Such monitoring is necessary to conduct an assigned CI function;
  - A trespass will not be necessary to effect the monitoring; and
  - The monitoring is not subject to Procedure 5

Procedure 7, Physical Searches

- Scope: Applies to *nonconsensual* physical searches in the United States *and* of U.S. persons/property outside the United States.
- Defined: Any intrusion on a person or property that would require a *warrant* for law enforcement purposes.
- Does *not* include examinations of
  - Areas that are in plain view and visible to the unaided eye if there is no physical trespass;
  - Publicly available information;
  - Abandoned property in a public place;
  - Items where we have consent; and
  - Government property pursuant to Military Rule of Evidence 314(d)

Procedure 7, Physical Searches

- **Active duty**
  - Approval: Attorney General or FISC
- **Other persons inside the United States**
  - We may *NOT* conduct searches of other persons
  - We may request the FBI to conduct such a search
- **Other U.S. persons outside the United States**
  - The search is for an authorized foreign intelligence or CI purpose;
  - The search is appropriately coordinated with the CIA; and
  - The FISC or the Attorney General has authorized the search.
  - Authority to Request
    - Does *not* include AFOSI/CC
    - SecDef, DSD, USD(I); SecAF; USecAF; DIRNSA/CHCSS; Director, DIA; Director, NGA; or Director, NRO

Procedure 8, Mail Searches and Cover

- **Mail Searches**
  - See Procedure 7

- **Mail cover**
  - In U.S. postal service channels, request the USPS IAW 39 CFR 233.3(e)(2)
  - In foreign postal channels, may request a mail cover for mail that is to or from a U.S. person consistent foreign law and any applicable SOFA

Procedure 9, Physical Surveillance

- **Who can we surveil in the United States:**
  - **Military service members;**
  - **Present or former military or civilian employees of a DIC;**
  - **Present or former contractors of a DIC;**
  - **Present or former employees of such a contractor;**
  - **Applicants for such employment or contracting;**
  - **Non-U.S. persons; and**
  - **Other persons, "when detailed to the FBI or when operating under FBI authorities."**

Procedure 9, Physical Surveillance

- **Scope**
  - Any person inside the United States or any U.S. person outside the United States.
  - Applies to any devices used to observe the subject of the surveillance (not Procedure 6).

- **Defined**
  - Deliberate and continuous observation of a person, and
  - Where the person has no reasonable expectation of privacy.
  - Does *not* apply to surveillance detection or counter surveillance used to detect and elude foreign physical surveillance

Procedure 9, Physical Surveillance

- **Approval and coordination**
  - **Approval: AFOSI/CC or delegee**
  - **Coordination**
    - **In the United States**
      - No coordination req'd for surveillance of active duty, on-base
      - FBI for off-base surveillance
      - FBI for surveillance on-base, non-active duty
    - **Outside the United States**
      - CIA for off-base surveillance
      - Consider with SOFA and foreign law/policy

Procedure 10, Undisclosed Participation (UDP)

- **Scope: Governs the *participation* by DICs and anyone acting on behalf of a DIC, e.g., sources, in any *organization* in the United States or any organization outside the United States that constitutes a U.S. person.**
- **Organization defined**
  - **An association of two or more individuals formed for any *lawful* purpose whose existence is formalized in some manner**
  - **Includes those that meet and communicate through the use of technologies**
- **Participation defined**
  - **When a person is tasked or asked to participate in an organization for the benefit of the DIC**
  - **Actions undertaken "for the benefit of" a DIC may include collecting information, identifying potential sources or contacts, or establishing or maintaining cover.**

Page 55 of 3957

Procedure 10, UDP

- **Exclusions**
  - Personal participation
  - Voluntarily provided information
  - Publicly available information on the Internet
    - Collection of publicly available information on the Internet in a way that does *not* require a person to provide identifying information (such as an email address) as a condition of access and does not involve communication with a human being.
- **Approval depends on the activity**
  - No specific level of approval
  - AFOSI/CC or delegee
  - AFOSI/CC or single delegee

Procedure 10, UDP

- **Standards for review and approval: approving official must make the following determinations:**
  - **The potential benefits to national security outweigh any adverse impact on civil liberties or privacy of U.S. persons.**
  - **The proposed UDP complies with the limitations on UDP; and**
  - **The proposed UDP is the least intrusive means feasible and conforms to the requirements of Procedure 2.**

Procedure 10, UDP

- UDP requiring no specific level of approval
  - Education or training
  - Cover Activities: Participation in an organization solely for the purpose of obtaining or renewing membership status *in accordance with DoD cover policy*
  - Published or posted information: Participation in an organization whose membership is open to the public solely for the purpose of obtaining information published or posted by the organization or its members and generally available to members; must not involve elicitation.
  - Public forums: Employment affiliation not required and no elicitation of USPI; and
  - Foreign entity

Procedure 10, UDP

- **UDP That May Be Approved by a DIC Head or Delegee**
  - **Non-U.S. persons as potential sources of assistance**
  - **Public forums: employment affiliation required or elicitation of USPI may be authorized**
  - **Cover activities beyond obtaining or renewing membership for the purpose of maintaining or enhancing cover**
  - **U.S. person organizations outside the United States involving participation from or about a non-U.S. person located outside the United States.**

Procedure 10, UDP

- **UDP That May Be Approved by a Defense Intelligence Component Head or a Single Delegee**
  - To conduct authorized CI activities not otherwise addressed in or outside the United States, after required coordination with the FBI or CIA.
  - To collect information inside the United States necessary to identify a U.S. person as a potential source of assistance to foreign intelligence or CI activities.
  - To collect information outside the United States necessary to assess a U.S. person as a potential source of assistance to foreign intelligence or CI activities.

Cyber Authorities

- Data at Rest
  - The Stored Communications Act (SCA)
- Live data
  - Pen Register/Trap & Trace Act
  - The Wiretap Act

Stored Communications Act

- Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712
  - Provides statutory and procedural protections to customer records and contents of communications when held in electronic storage
  - Electronic storage: "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"
- Applies to all electronic communications services, e.g., Yahoo, Google, and military networks

Stored Communications Act

- § 2701 prohibits ***unauthorized access*** to stored communications
- Service provider exception
  - Allows person or entity providing a wire or electronic communications service to access stored communications, e.g., sys ads
- Q: Ever wonder how Google knows that you're in the market for . . . a feng shui brass rooster?

Stored Communications Act

- § 2702. Disclosure of Contents
  - Prohibits a person or entity providing an electronic communication service [ECS] ***to the public*** from releasing the contents of a communication while in electronic storage by that service; and
  - Prohibits a person or entity providing remote computing service [RCS] ***to the public*** from releasing the contents of any communication which is carried or maintained on that service

Stored Communicatio!

- Strict requirements apply to public service providers only, per 18 U.S.C. § 2702
- DoD is not a public service provider. See Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. IL 1998)
- In theory, no substantial limits for DoD system admins when accessing s communications on our networks

Stored Communications Act

- To gain access to most records of interest, LE needs to either obtain a *search warrant* or a § 2703(d) order (used when the records are "relevant and material to an ongoing criminal investigation")
- These must be obtained from a "court of competent jurisdiction"
  - Excludes military courts

SCA, Compelled Disclosure, 18 USC § 2703

Information Sought	Public Provider	Non-Public
Basic subscriber, session, and billing information	Subpoena; 2703(d) order; or search warrant § 2703(c)(2)	Subpoena; 2703(d) order; or search warrant § 2703(c)(2)
Other transactional and account records	2703(d) order or search warrant § 2703(c)(1)	2703(d) order or search warrant § 2703(c)(1)
Retrieved communications and the content of other stored files	Subpoena with notice; 2703(d) order with notice; or search warrant § 2703(b)	Subpoena; SCA does not apply § 2711(2)
Unretrieved communications, including email and voice mail (in electronic storage *more than 180 days*)	Subpoena with notice; 2703(d) order with notice; or search warrant § 2703(a), (b)	Subpoena with notice; 2703(d) order with notice; or search warrant § 2703(a), (b)
Unretrieved communications, including email and voice mail (in electronic storage *180 days or less*)	Search warrant § 2703(a)	Search warrant § 2703(a)

SCA Practice Tips

If an electronic communication may contain evidence relevant to the investigation:

- **Immediately send a preservation request to the provider (renew for 90 days)**
- **Work with local US Attorney's office to obtain a search warrant or court order from a Federal District Court**
- **For subscriber information, i.e., non-content, trial counsel and/or DoD IG subpoena is sufficient**

Real-Time "Live" Data

- Pen Register / Trap & Trace (non-content)
- Wiretap Act (content)

Pen Register / Trap & Trace

- Pen/Trap captures all ***non-content*** information in a communication, i.e., meta data (address on an envelope)
  - Requires a court order, unless an exception met

- Initially applied to telephones only
  - Pen Register: records numbers dialed *from* a particular phone, e.g., 867-5309
  - Trap & Trace: records what numbers dialed *to* a particular phone, i.e., caller ID

- Now includes land lines, cell phones, internet user accounts, email accounts, and IP addresses

Pen Register / Trap & Trace

- Permits providers or wire communication services authority to use pen/trap devices on their own networks without a court order
  - Perform operation, maintenance, and testing
  - Protect provider's property
  - Protect users from abuse / unlawful use of service

- On AFIN, would also apply to "proxy logs" containing records of web page activity

Wiretap Act

The Wiretap Statute

- **Federal Wiretap Statute, 18 U.S.C. § 2510-2520**
  - **BLUF: Wiretapping is illegal, unless an exception applies**
  - **Broadly prohibits eavesdropping everywhere by people in the US (not just the government)**
  - **Wiretap defined: *intercepting communications* using an electronic, mechanical, or other device**
    - **"Communications" means content**
    - **"Intercept" means acquiring contemporaneously with transmission, i.e., "live or real-time" communication**
    - **Applies to Internet communications**
  - **Air Force is a provider of electronic communications services**

Wiretap Statute Exceptions

- Consent, § 2511(2)(c)-(d)
- Accessible to the public, § 2511(2)(g)(i)
- Court order, § 2518
- Service Provider Exception, § 2511(2)(a)(i)
- Computer Trespasser Exception, § 2511(2)(i)
- Extension telephone exception, § 2510(5)(a)
- Inadvertently obtained criminal evidence, § 2511(3)(b)(iv)

Service Provider Exception

- Applies to "provider[s] of electronic communication services"
- System providers are authorized to intercept, disclose, or use network communications to protect rights & property of the provider or to ensure the system continues to provide service
- Allows real-time monitoring w/o a warrant to improve service
  - For example, it is appropriate to scan (intercept) all incoming emails for malicious code, but it is likely not appropriate to scan all emails for certain words.

Computer Trespasser Exception

- This is the primary exception used by LE/CI (AFOSI), 18 USC § 2511
  - Investigators may monitor a computer trespasser if:
    - System owner consents
    - Part of a lawful investigation (AFOSI);
    - *Reasonable grounds* exist to believe the contents of trespasser's communications will be relevant to the investigation; and
    - Interception is limited only to those communications "to and from the trespasser"
  - A trespasser does not include a lawful user of the system who exceeds their authorized access, i.e., "insider threat"
- AFOSI/JA will provide legal advice and staff to AFOSI/CC

Final Thoughts

- Fourth Amendment violation where GPS was attached to a car without a warrant and Joneses' movements were tracked for 28 days. United States v Jones, 132 S. Ct. 945 (2012)
  - "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." J. Sotomayer, concurring.

Final Thoughts

- Search of a cell phone incident to arrest requires a warrant. Riley v. California, 134 S. Ct. 2473 (2014).
  - "Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form-unless the phone is." (emphasis in original)

Recap

- What is "cyber law"?
- Reasonable Expectation of Privacy
- Search and Seizure on the AFNET
- Stored Communications Act
- Pen Register / Trap Trace
- Wiretap Act
- Final Thoughts

Stored Communications Act

- Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712
  - Provides statutory and procedural protections to customer records and contents of communications when held in electronic storage
  - Electronic storage: "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"
- Applies to all electronic communications services, e.g., Yahoo, Google, and military networks

Topics

Status

- February 2016: DoD SIOO sends out 5240.01M for informal coord ✓
- February – March 2016: Working and DoJ adjudicate approximately 170 comments from informal coord ✓
- 7 March 2016: "Clean" 5240.01M sent to WHS for formatting ✓
- 11/14 March 2016: SIOO to send 5240.01M for formal coord ✓
- 1 April 2016: Suspense for formal coord ✓
- 15 April 2016: Complete adjudication of comments (DoD, DoJ) ✓
- April – May 2016: Legal/security/PCLOB reviews ✓
- July 2016: Anticipated signing by AG and SECDEF

Overview

- 5240.01M remains DoD implementing policy for E.O. 12333
- Follows same structure as 5240.1-R
  - Procedure 1 – General Provisions
  - Procedure 2 – Collection
  - Procedure 3 – Retention
  - Procedure 4 – Dissemination
  - Procedure 5 – Electronic Surveillance
  - Procedure 6 – Concealed Monitoring
  - Procedure 7 – Physical Search
  - Procedure 8 – Mail Searches and Cover
  - Procedure 9 – Physical Surveillance
  - Procedure 10 – Undisclosed Participation
- Procedures 11 – 15 removed from 5240.01M; AG approval not needed
  - To be published in other DoD issuance

Key Changes

- **New definition of collection**
  - Information is collected when it is received
  - Exception is when information not intelligible (e.g. encrypted)
  - Dissemination received from another agency is NOT collection
- **Concepts of shared repository and special collection added**
- **Counterintelligence exception expanded to account for HVE**
- **New retention timeframes for incidental collection**
  - Domestic incidental collection may be retained up to five years
  - Overseas incidental collection may be retained up to 25 years
  - DIC Heads and single delegee may approve extensions

Key Changes

- **Military magistrates may no longer authorize Procedure 7**
  - Only MCIOs may conduct searches against AD personnel
  - Must obtain FISA
- **Three approval levels for UDP**
  - No specific approval
  - DIC Head or delegee(s)
  - DIC Head or single delegee
- **Definitions of organization in US and outside US expanded to account for internet activity**
- **List of Defense Intelligence Components and their heads updated**

MAJOR CHANGES BY PROCEDURE

Procedure 1

General Provisions

Procedure 1 – General Provisions

- Para 3.1.b. – Adds concept of shared repositories
  - Para 3.1.b.2. – Procedures for components hosting shared repositories
  - Para 3.1.b.3. – Procedures for components acting as participants in shared repositories
- Paras 3.1.c. – 3.1.e. – DoD Senior Intelligence Oversight Official (SIOO) added as cognizant entity for interpretation, exceptions, amendments to 5240.01M

Procedure 2

Collection of US Person Information

Procedure 2 – Collections

- Para 3.2.c.4.c. – Counterintelligence: exception expands foreign terrorist connection to include individuals "*reasonably believed to be acting for or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States.*"
  - Permits collection when no specific connection to foreign terrorist(s) has been established – HVE (e.g. San Bernardino, Orlando)

- Para 3.2.c.5.b. – Threats to Safety: Allows DIC heads or delegee to authorize collection when they have determined a "*persons' life or physical safety is reasonably believed to be in imminent danger;*"

Procedure 2 – Collections

- Para 3.2.c.8. – Persons in Contact With Sources or Potential Sources: New exemption category added.

- Para 3.2.c.10. – Physical Security: This exemption now includes a requirement that there exist a "*reasonable belief in…the foreign connection of the U.S. persons…and the physical security threat they pose.*"

- Para 3.2.c.12. – Overhead and Airborne Reconnaissance: This exemption now includes requirements to comply with DoD or NGA policies and procedures

- Former exemption for Narcotics has been removed (replaced by 3.2.c.8.)

Procedure 2 – Collections

- Para 3.2.e. – Adds notion of Special Circumstances Collection
  - "(C)*ollection opportunities raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information.*"
  - DIC head or delegee must approve such collection and report approval to DoD SIOO
- Para 3.2.f.3. – Requires that in any collection of non-publicly available information the DICs must "*to the extent practicable, take steps to collect no more information that is reasonably necessary.*"

Procedure 3

Retention of US Person Information

Procedure 3 – Retention

- Para 3.3.c.1. – Intentional Collection of USPI: DIC must evaluate information promptly, but may retain for up to five years for evaluation
    - DIC Head or single delegee may approve an extended period
- Para 3.3.c.2.a. – Information collected incidentally in the US, or about a place in the US, may be retained for five years for evaluation
    - DIC Head or single delegee may approve an extended period
- Para 3.3.c.2.b. - Information collected incidentally outside the US, or about a place outside the US, may be retained for 25 years for evaluation
    - DIC Head or single delegee may approve an extended period

Procedure 3 – Retention

- Para 3.3.c.3. – Voluntarily Provided USPI: DIC may retain such information for up to five years for evaluation
    - DIC Head or single delegee may approve an extended period
    - If DIC receives voluntarily provided information about individual believed to be a non-US Person, but info may contain USPI, retention period is 25 years
- Para 3.3.c.4. – Special Circumstances: Such information may be retained for up to five years
    - USD(I) may approve an extended period
- Para 3.3.c.5. – Extended Retention

Procedure 3 – Retention

- Para 3.3.c.6. – Retention time frames do not begin until information has been processed into intelligible form (e.g. decryption)

- Para 3.3.d. – Information received from another component or IC element will be subject to the same, concurrent retention time limits as originating agency (i.e. clock does not restart for receiving entity)

- Para 3.3.e. – Addresses criteria for permanent retention

- Para 3.3.f.1.b. – Requires that "*when retrieving information electronically, tailor queries…to the greatest extent practicable to minimize the amount of USPI returned that is not pertinent…*"

- Para 3.3.f.1.c. – DICs must "*take reasonable steps to audit access to information systems containing USPI and to audit queries…to assess compliance with this issuance.*"

Procedure 3 – Retention

- Para 3.3.f.1.d. – When developing and implementing information systems for use with USPI, DICs must "*take reasonable steps to ensure effective auditing and reporting…*"
- Para 3.3.f.1.e. – When retaining information DICs are required to "*(e)stablish documented procedures for retaining data containing USPI and recording the reason…and the authority approving the retention.*"
- Para 3.3.f.1.f. – Requires annual training for employees accessing or using USPI
- Para 3.3.f.2. – DICs must employ reasonable measures to identify and mark files containing USPI
- Para 3.3.f.3. – DoD SIOO will periodically review DIC practices

Procedure 3 – Retention

- Para 3.3.g. – Enhanced Safeguards: DIC Head or delegee must assess need for enhanced safeguards when there is special circumstances collection
  - Factors to consider include
    - Intrusiveness of collection method(s)
    - Volume or sensitivity of USPI
    - Potential for harm, embarrassment, inconvenience, unfairness
    - Uses of USPI being retained
    - Length of retention
  - Para 3.3.g.2. – Details potential enhanced safeguard measures

Procedure 4

Dissemination of US Person Information

Procedure 4 – Dissemination

- Para 3.4.c. – Criteria for Dissemination: Several new categories added
  - Para 3.4.c.1. – Any Person or Entity: Dissemination to any person or entity permitted if information is publicly available or collected via consent
  - Para 3.4.c.8. – Protective Purposes: Dissemination permitted if necessary to protect safety/security of persons or property, or to protect against crime or threat to national security
- Para 3.4.d. – DICs may disseminate large amounts of unevaluated USPI (defined in Para 3.4.c.3.) with approval of DIC Head or single delegee, after notification to DoD SIOO

Procedure 4 – Dissemination

- Para 3.4.e. – DICs should not include USPI in dissemination "*if pertinent information can be conveyed in an understandable way without including the identifying information.*"
    - If dissemination includes USPI the receiving entity must be so notified
- Para 3.4.g. – Special considerations/controls on dissemination of information to the White House
- Para 3.4.h. – DICs must have procedures in place to address improper dissemination of USPI

Procedure 5

Electronic Surveillance

Procedure 5 – Electronic Surveillance

- Para 3.5.c.2. – Adds Attorney General (AG) to Foreign Intelligence Surveillance Court (FISC) as authorizing entities for electronic surveillance in the US
    - Paras 3.5.c.2.a. and 3.5.c.2.b. add criteria which DICs must meet in order to conduct such surveillance
- Para 3.5.c.3. – Add USD(I) as DoD entity authorized to request electronic surveillance of US Person in US
- Para 3.5.d.3. – Add USD(I) as DoD entity authorized to request electronic surveillance of US Person outside US
- Para 3.5.e. – Does NOT apply to MCIO CI activities against non-US Persons outside of the US

Procedure 5 – Electronic Surveillance

- Para 3.5.g. – In emergency situations, DICs may obtain approval from AG
    - Request for AG approval must be made by
        - SECDEF/DEPSECDEF
        - USD(I)
        - SECAF/USECAF (SECNAV/USECNAV, SECAR/USECAR)
        - DIRNSA
- Para 3.5.h. – In exigent circumstances, DICs may target US Persons outside of the US when AG approval is not practical if:
    - Person's life or physical safety in danger; or
    - Physical security of USG property in danger from foreign power; or
    - Time required for AG approval would result in harm to national security

Procedure 5 – Electronic Surveillance

- Para 3.5.h.2. – Approval of exigent circumstance electronic surveillance limited to :
  - SECDEF/DEPSECDEF
  - USD(I)
  - SECAF/USECAF (SECNAV/USECNAV, SECAR/USECAR)
  - DIRNSA/Deputy DIRNSA
  - NSA SIGINT Director
  - DIRNSA Senior Representative
  - Any flag/general office at overseas location in question w/responsibility for subject or endangered resources
- Para 3.5.i.2.b.1. – Adds allowance for collection of incidental information during TSCM when it is not reasonable to obtain consent of persons subject to incidental collection

Procedure 5 – Electronic Surveillance

- Para 3.5.i.2.c. – Adds criteria for retention and dissemination of information obtained during TSCM

- Para 3.5.i.3.c. – Adds several permissible targets of electronic surveillance for training purposes (sub-paras 3, 4, 5 and 6)

- Para 3.5.i.3.d. – Lists five conditions which must be met to train against targets other than those listed in 3.5.i.3.c.

    - Surveillance not targeted at particular person without consent
    - Not reasonable to obtain consent of persons incidentally subjected to surveillance
    - Not reasonable to train without engaging in such surveillance
    - Surveillance limited in extent and duration to that necessary
    - Minimal acquisition of information permitted for calibration

Procedure 6

Concealed Monitoring

Procedure 6 – Concealed Monitoring

- Para 3.6.a.2. – Procedure does not apply to concealed monitoring for testing or training when subjects consent; otherwise subject to Procedure 6

- Para 3.6.c.1. – DICs may conduct concealed monitoring outside DoD facilities in the US after coordination with FBI and in accordance with all DoJ/FBI agreements

- Para 3.6.c.3. – Concealed monitoring may be approved by DIC Head or a delegee

Procedure 7

Physical Searches

Procedure 7 – Physical Searches

- **NOTE: Searches based upon military magistrate authorization pursuant to Military Rules of Evidence are no longer permitted under Procedure 7**
  - Search authorizations may be used to pursue potential UCMJ violations under Military Rules of Evidence
- Para 3.7.c. – Searches Against Active Duty Military Personnel: only MCIOs may be authorized to conduct
  - Must be conducted under FISA with AG or FISC approval
  - SECDEF/DEPSECDEF, USD(I), SECAF/USECAF may seek approval
  - In emergency situations MCIO Head or delegee may make request to DoD GC to seek AG authorization

Page 110 of 3957

Procedure 7 – Physical Searches

- Para 3.7.d. – Searches Against Other Persons in the US: DICs may not conduct, but may request FBI to conduct if two conditions met

  1. Search must be for authorized FI or CI purpose

  2. Search must meet definition of physical search under FISA

  - SECDEF/DEPSECDEF, USD(I), SECAF/USECAF, DIRNSA, Director DIA, Director NGA, Director NRO may seek approval

  - In emergency situations MCIO Head may make request to DoD GC ask FBI to conduct search

Procedure 7 – Physical Searches

- Para 3.7.e. – Searches of Other US Persons or Their Property Outside the US: DICs may conduct such searches if three conditions met

  1. Search is for authorized FI or CI purpose; and

  2. Search is appropriately coordinated with CIA; and

  3. FISC or AG has approved search

  - SECDEF/DEPSECDEF, USD(I), SECAF/USECAF, DIRNSA, Director DIA, Director NGA, Director NRO may seek approval

  - In emergency situations MCIO Head may make request to DoD GC to seek AG authorization

Procedure 8

Searches of Mail and Mail Covers

Procedure 8 – Searches of Mail and Mail Covers

- Para 3.8.a. – Clarifies that this Procedure does not apply to items transported by a commercial carrier (e.g. Federal Express, UPS, etc.)

- Para 3.8.c.1. – Searches of Mail: subject to Procedure 7 limitations and approvals

- Para 3.8.d. – Mail covers: DICs may request USPS conduct mail cover for items in USPS channels

  - For mail in foreign channels DICs may request mail cover for items to/from US Person in accordance with local law and SOFA

  - No specific DIC official(s) identified as required to make request

Procedure 9

Physical Surveillance

Page 115 of 3957

Procedure 9 – Physical Surveillance

- Para 3.9.c.1.a. – DICs may conduct surveillance of US Persons in US if they fall into the existing 5240.1-R categories
- Para 3.9.c.1.b. – DICs may conduct surveillance of non-US Persons in US for authorized FI or CI purpose
- Para 3.9.c.1.c. – DIC Head or delegee must approve authorized physical surveillance
  - Physical surveillance in the US must be coordinated with FBI per existing agreements with DoJ/FBI
  - DICs can participate in physical surveillance of other US Persons in US when detailed to, or operating under the authorities of, the FBI

Procedure 9 – Physical Surveillance

- Para 3.9.c.1.d. – DIC Head or delegee may approve DIC participation in authorized FBI physical surveillance in US when FBI requests and authorizes DIC participation in writing

- Para 3.9.c.2.c. – DIC Head or a delegee may approve physical surveillance of any US person outside of the US

  - Physical surveillance outside the US conducted off of a military installation must be coordinated with the CIA

  - Approving official must consider host nation laws and SOFA

Procedure 10

Undisclosed Participation

Page 118 of 3957

Procedure 10 – Undisclosed Participation

- Para 3.10.a. – Clarifies that Procedure 10 applies to sources
- Para 3.10.b. – Identified three categories of excluded activities
  - Personal participation (i.e. undertaken for personal reasons and at personal expense)
  - Voluntarily provided information from existing members without request from DIC
  - Publicly available information on the internet collected in such a way that provision of personal identifying information is not required, and no communication with human being occurs

Procedure 10 – Undisclosed Participation

- Para 3.10.e. – Limitations on Undisclosed Participation: adds two additional limitations not found in 5240.1-R
  - UDP may not be authorized to collect on domestic activities of US persons
  - All UDP must be coordinated with FBI, CIA or other agency in accordance with EO 12333 and other policies/agreements
- Para 3.10.e.6.b. – DICs wishing to engage in UDP to influence activities of an organization per Para 3.10.e.6.a. must make request to USD(I) through DoD/GC
- Para 3.10.e.6.c. – Prohibition on influencing organizations does not apply to non-US Persons located outside the US

Procedure 10 – Undisclosed Participation

- Para 3.10.f. – Required Approvals: Approvals now authorized at three levels

1. No Specific Approval Required: Recognizes activity as UDP but no specific approval required
   - Education or training
   - Participation to maintain cover; no further activity in organization
   - Information published or posted by an organization open to the public when information is available to all members and no elicitation occurs (e.g. Subscription to Washington Post)
   - Public forums, to include social media, when employment affiliation is not required and no elicitation occurs (e.g. Facebook public profiles)
   - Foreign entities

Procedure 10 – Undisclosed Participation

2. UDP that may be approved by DIC Head or delegee

- Information collected to identify and assess non-US Person as potential source of assistance
- Public forums, to include social media, when employment affiliation is required and/or elicitation occurs (e.g. Facebook non-public profiles)
- Cover activities beyond obtaining or renewing membership
- Information collected outside the US from or about a non-US Person located outside the US

Procedure 10 – Undisclosed Participation

3. UDP that may be approved by DIC Head or ***single*** delegee

   - Collection of FI outside of US from or about a specific US Person, or from or about a non-US Person in the US
   - To conduct CI activities not addressed previously, in or outside the US
   - Collection of information inside the US needed to identify a US Person as potential source
   - Collection of information outside the US needed to assess a US Person as potential source

- Para 3.10.f.4. – UDP not addressed elsewhere in Procedure may be authorized by USD(I) or DIC Head with notice to DoD SIOO

Procedure 10 – Undisclosed Participation

- Para 3.10.f.5. – Approving official must make following determinations
  - "*Potential benefits to national security outweigh any adverse impact on civil liberties or privacy of US Persons.*"
  - UDP complies with requirements of Para 3.10.e.
  - UDP is least intrusive means feasible to obtain information and conforms to Procedure 2
- Para 3.10.g. – Disclosure requirement: Disclosure of DIC affiliation must be sufficient to apprise appropriate official(s) of the affiliation
  - If official to whom disclosure would be made acting on behalf of DIC, his/her knowledge not sufficient unless senior official of organization
  - DIC will maintain written record of disclosures, including to whom made

Definitions

Definitions

THE FOLLOWING DEFINITION HAVE BEEN ADDED OR NOTABLY CHANGED FROM 5240.1-R
(Definitions below are summarized)

- Agent of a Foreign Power – any person, including a US Person, acting for or on behalf of a foreign power
- Collection – information is collected ***when it is received by a DIC***
- Defense Intelligence Components – now defined as:
  - NSA/CSS
  - DIA
  - NRO
  - NGA
  - FI and CI elements of the Military Departments
  - Senior Intelligence Officials of the COCOMs

Definitions

- Defense Intelligence Component Head – now includes:
  - Director NSA
  - Director DIA
  - Director NRO
  - Director NGA
  - Deputy Chief of Staff, G2, Department of the Army
    - Commander, Army INSCOM
  - Director of Naval Intelligence
    - Director of Naval Intelligence Activity
    - Commander, ONI
  - Commander, US Fleet Cyber Command
  - Director, NCIS
  - Director of Intelligence, USMC
  - Commander, Marine Corps Intelligence Activity
  - Deputy Chief of Staff, ISR, Department of the Air Force
    - Commander, 25th Air Force
  - Commander, AFOSI

Page 127 of 3957

Definitions

- Detail – an employee of one agency operating under the authorities of another agency
- Dissemination – transmission of information outside of a DIC
- DoD Facility – Installations/facilities owned, leased or occupied by accommodation by DoD
- Foreign Connection – US Person in contact with a foreign person for purposes harmful to US national security
- Host of a Shared Repository – entity maintaining a shared repository
- Imagery – likeness of any feature and positional data thereof
- Incidental Collection of USPI – USPI collection not deliberately sought by a DIC but which is nonetheless collected
- Intelligence – includes FI and CI

Definitions

- Intentional Collection of USPI – USPI collection deliberately sought by a DIC
- Organization – expanded to include entities which meet and communicate principally through the use of technology
- Organization in the US – expanded to include organizations primarily meeting via the internet substantially composed of persons located in the US
- Organization Outside the US Constituting a US Person - organization physically located outside the US but substantially composed of US Persons or organization primarily meeting via the internet substantially composed of US Persons located outside the US
- Overhead Reconnaissance – activities of space-based capabilities conducting imagery collection

Definitions

- Physical Search – expanded to include electronic data
- Shared Repository– database or other repository maintained for the use of more than one agency
- Transmission Media Vulnerability Survey– acquisition of transmissions to determine vulnerability to interception
- Undisclosed Participation – participation in an organization without disclosure of DIC affiliation
- USPI – information reasonably likely to identify a specific US Person

Definitions

THE FOLLOWING DEFINITION HAVE BEEN REMOVED FROM 5240.01M

- Counterintelligence Investigation
- Lawful Investigation
- Physical Security
- Physical Security Investigation
- Signals Intelligence

QUESTIONS?

Air Force Office of Special Investigations

Eyes of the Eagle

DoDM 5240.01 Legal Primer

29 Sept 2016

U.S. AIR FORCE

Page 133 of 3957

Topics

- DoDM 5240.01 Overview
- DoDM 5240.01 Procedures
  - Proc 2, Collection
  - Proc 3, Retention
  - Proc 4, Dissemination
  - Proc 5, Electronic Surveillance
  - Proc 6, Concealed Monitor
  - Proc 7, Physical Search
  - Proc 8, Mail Search/Cover
  - Proc 9, Physical Surveillance
  - Proc 10, Undisclosed Participation
- JA Checklist

DoDM 5240.01, Overview

DoD MANUAL 5240.01

PROCEDURES GOVERNING THE CONDUCT OF DoD INTELLIGENCE ACTIVITIES

Originating Component:	Office of the Deputy Chief Management Officer of the Department of Defense
Effective:	Month Day, Year
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.dtic.mil/whs/directives
Incorporates and Cancels:	Directive-type Memorandum 08-031, "Intelligence Oversight Policy Guidance," March 20, 2008 Procedures 1-10 of DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982
Approved by:	Loretta E. Lynch, Attorney General of the United States Ashton B. Carter, Secretary of Defense

Purpose: In accordance with the authority in DoD Directive 5240.01 and Executive Order (E.O.) 12333, this issuance:

- Establishes procedures to enable DoD to conduct authorized intelligence activities in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons. DoD authorized intelligence activities are foreign intelligence and counterintelligence (CI) activities unless otherwise specified in this issuance.
- Authorizes the Defense Intelligence Components to collect, retain, and disseminate information concerning U.S. persons in compliance with applicable laws, Executive orders, policies, and regulations.

DoDM 5240.01, Overview

- Effective 8 Aug 2016; signed by SecDef and AG
- Changes are substantial, but not significant
- Replaces Procedures 1-10 of DoD 5240.1-R (Dec 1982)
- DoD 5240.01-R, Procedures 11-15, remain in effect
- No changes to Executive Order 12333

DoDM 5240.01, Overview

- CI Defined: Information gathered and activities conducted to *identify, deceive, exploit, disrupt,* or *protect* against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

Procedure 2, Collection—Introduction

- **Intentional Collection of USPI: We may *intentionally* collect USPI *only* if:**
  - the information sought is ***reasonably believed;***
  - to be *necessary* for the performance of an authorized CI mission; and
  - the USPI falls within one of the following 13 categories below.
    - CI2MS *requires* that you indicate a Proc 2 collection category

- **U.S. Person Information (USPI) defined: Information that is reasonably likely to identify one or more specific U.S. persons.**

- **Collection takes place upon receipt**
  - Regardless of when you use it
  - Computers can collect
  - Intel is collected only once
  - May be disseminated multiple times
  - Encrypted data is considered collected upon receipt

Procedure 2, Collection—Reasonable Belief

- **Defined: When the facts and circumstances are such that a reasonable person would hold the belief.**
  - **Must rest on facts and circumstances that can be articulated;**
  - **Hunches or intuitions are not sufficient; and**
  - **Can be based on experience, training, and knowledge of CI activities as applied to particular facts and circumstances.**

Procedure 2, Collection—Categories

1. Publicly Available
2. Consent
3. Foreign Intelligence (FI)
4. Counterintelligence (CI)
5. Threats to Safety
6. Protection of Sources/Methods
7. Current, Former, or Potential Sources
8. Persons in Contact With Sources or Potential Sources
9. Personnel Security
10. Physical Security
11. Communications Security
12. Overhead and Airborne Reconnaissance
13. Administrative Purposes

Procedure 2, Collection Categories

1. **Publicly Available Information**

2. **Consent**
   - **The legal advisor must determine whether a notice or policy is adequate and lawful, before the Component takes or refrains from taking action on the basis of implied consent (DoDM 5240.01, G.2.)**

3. **Foreign Intelligence**
   - **AFOSI does not have a foreign intelligence mission**

Procedure 2, Collection—Categories

4. Counterintelligence: The information is reasonably believed to constitute CI and the U.S. person is one of the following:

- **(a) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in espionage, other intelligence activities, sabotage, or assassination on behalf of a *foreign* power, organization, or person, or on behalf of an agent of a *foreign* power, organization, or person;**
- **(b) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist activities;**
- **(c) An individual, organization, or group reasonably believed to be acting for, or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States; or**
- **(d) An individual, organization, or group *in contact with a person described above* for the purpose of identifying such individual, organization, or group and assessing any relationship with the person described therein.**

Procedure 2, Collection—Categories

5. Threats to safety: information needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations, if:

- **The threat has a foreign connection;**
- **AFOSI/CC or delegee has determined that a person's life or physical safety is reasonably believed to be in imminent danger; *or***
- **The information is needed to maintain maritime or aeronautical safety of navigation.**

Procedure 2, Collection—Categories

6. **Protection of Intelligence Sources, Methods, and Activities**
   - The information is about U.S. persons who have access to, had access to, will have access to, or are otherwise in possession of information that reveals foreign intelligence or CI sources, methods, or activities, when collection is **reasonably believed** necessary to protect against the unauthorized disclosure of such information.

7. **Current, Former, or Potential Sources of Assistance**
   - The information is about those who are or have been sources of information or assistance, or are **reasonably believed** to be potential sources of information or assistance, to intelligence activities for the purpose of assessing their suitability or credibility.

8. **Persons in Contact With Sources or Potential Sources**
   - The information is about persons in contact with sources or potential sources, for the purpose of assessing the suitability or credibility of such sources or potential sources.

9. **Personnel Security**
   - The information is arising from a lawful personnel security investigation.

Procedure 2, Collection—Categories

10. Physical Security

- The information is about U.S. persons **reasonably believed** to have a *foreign* connection and who pose a threat to the physical security of DoD personnel, installations, operations, or visitors.
- Must have or be supporting an authorized physical security mission and must be able to articulate a **reasonable belief** in both the foreign connection of the U.S. persons who are collection targets and the physical security threat they pose.

11. Communications Security Investigation

- The information is arising from a lawful communications security investigation.

Procedure 2, Collection—Categories

12. Overhead and Airborne Reconnaissance

- May intentionally collect imagery that contains USPI provided that the collection is ***not*** directed at a specific U.S. person or, if the collection is directed at a specific U.S. person, the collection falls in one of the other 12 categories
- Includes information obtained from unmanned aircraft systems
- See SecDef Memo Feb 2016

13. Administrative Purposes

Procedure 2, Collection—Other Considerations

- **Least Intrusive Means**
  - Use the least intrusive collection techniques feasible within the United States *or* directed against a U.S. person abroad.
    1. Publicly available sources or with consent
    2. Cooperating sources
    3. Techniques that do *not* require a judicial warrant or AG approval
    4. Techniques that do require a judicial warrant or AG approval
- **Amount of Information Collected**
  - In collecting non-publicly available USPI, to the extent practicable, collect no more information than is reasonably necessary.
- **Special Circumstances Collection [BIG data]**
  - Components will consider whether collection opportunities raise special circumstances based on the *volume*, *proportion*, and *sensitivity* of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information.

Procedure 3, Retention

- **Permanent Retention standard**
  - Retention is **reasonably believed** to be necessary for the performance of an authorized intelligence mission; *and*
  - The information was lawfully collected or disseminated to the Component:
    - Meets one of the 13 Proc 2 collection categories; or
    - Is necessary to understand or assess CI, e.g., information about a U.S. person that provides important background or context for CI.

Procedure 3, Retention

- Three primary evaluation periods to determine permanent retention of USPI
  - Promptly
  - Five (5) years
  - Twenty-five (25) years

- Intentional Collection of USPI
  - Must be evaluated promptly; and
  - If *necessary*, may retain the information for evaluation for up to 5 years, subject to extension

Procedure 3, Retention

- **Incidental Collection of USPI**
  - Defined: collection of USPI that is not deliberately sought, but is nonetheless collected
  - *In the United States,* may retain all of the incidentally collected information for evaluation for up to **5 years**, unless extended
  - *Outside the United States, may* retain all of the incidentally collected information for evaluation for up to **25 years**

- **Voluntarily Provided USPI**
  - About a U.S. person, evaluate the information **promptly**, up to **5 years**, unless extended
  - About a non-U.S. person, evaluation for up to **25 years**

Procedure 3, Retention

- **Unintelligible information**
  - Includes information that a Component cannot decrypt or understand in the original format
  - The time periods begin when the information is processed into intelligible form
  - To the extent practicable, unintelligible information will be processed into an intelligible form
  - A foreign language is considered intelligible

- **Deletion of Information**
  - Unless the standards for permanent retention are met, must delete all USPI from the Component's automated systems of records

Procedure 4, Dissemination

- We may disseminate USPI based upon the following criteria:
  - Any person or entity: Information is publicly available or U.S. person has consented to the dissemination
  - Other intelligence community elements
  - Other DoD elements; federal government entities; state, local, tribal, or territorial governments: recipient is **reasonably believed** to have a need to receive such information for the performance of its lawful missions or functions.
  - Foreign governments or international organizations
    - Recipient is **reasonably believed** to have a need to receive such information for its lawful missions or functions; and
    - Disclosure is consistent with applicable international agreements and foreign disclosure policy
  - Protective Purposes
    - Necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security

Procedure 5, Electronic Surveillance

- Implements FISA and E.O. 12333
- Defined for U.S. collection
  - The installation or use of any monitoring device in the United States where a person has a reasonable expectation of privacy, as determined by JA, and
  - A warrant would be required for law enforcement purposes
- Fourth Amendment
  - All electronic surveillance must comply with the Fourth Amendment
  - JA must assess the reasonableness of collection, retention, and dissemination (DoDM 5240.01, para. 3.5.b.)

Procedure 5, Electronic Surveillance

- **In the United States**
  - **Attorney General or the Foreign Intelligence Surveillance Court (FISC) must authorize, except in emergency situations.**
  - **May only conduct such surveillance if both:**
    - **A *significant purpose* of the electronic surveillance is to obtain foreign intelligence information; and**
    - **There is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power.**

Procedure 5, Electronic Surveillance

- Outside the United States
  - U.S. person
    - Governed by FISA and E.O. 12333; or
    - Approval under exigent circumstances exception
  - Non-U.S. person: governed by Title I or Section 702
- Emergency situations: Attorney General approval
- Technical Surveillance Countermeasures (TSCM)
  - Applies to the use of electronic equipment and specialized techniques to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance.

Procedure 6, Concealed Monitoring

- **Defined as the following:**
  - Hidden electronic, optical, or mechanical devices,
  - to monitor a particular person or a group of persons,
  - without *consent*,
  - in a surreptitious manner,
  - over a period of time, and
  - no *reasonable expectation of privacy*
- **Examples**
  - Video monitoring or sound recording of a subject in a place where he or she has no reasonable expectation of privacy if conducted over a period of time
  - Taking one photograph of a subject would *not* qualify

Procedure 6, Concealed Monitoring

- Scope
  - *Any* person inside the United States, or
  - Any U.S. person outside the United States
- Procedures
  - In the United States
    - On DoD facilities
    - Outside DoD facilities, after coordination with the FBI
  - Outside the United States
    - On DoD facilities
    - Outside DoD facilities must be coordinated with the CIA, and appropriate host country officials in accordance with any applicable SOFA or other international agreement.

Procedure 6, Concealed Monitoring

- **Approval: AFOSI/CC or delegee (*new*)**

- **The following criteria must be met:**
  - **There is no reasonable expectation of privacy;**
  - **Such monitoring is necessary to conduct an assigned CI function;**
  - **A trespass will not be necessary to effect the monitoring; and**
  - **The monitoring is not subject to Procedure 5 (DoDM 5240.01, 3.6.c.(3))**

Procedure 7, Physical Searches

- Scope: Applies to *nonconsensual* physical searches in the United States ***and*** of U.S. persons/property outside the United States.
- Defined: Any intrusion on a person or property that would require a *warrant* for law enforcement purposes.
- Does ***not*** include examinations of
  - Areas that are in plain view;
  - Publicly available information;
  - Abandoned property in a public place;
  - Items where we have consent; and
  - Government property pursuant to Military Rule of Evidence 314(d)

Procedure 7, Physical Searches

- **Active duty**
  - Approval: Attorney General (AG) or FISC (*new*)
- **Other persons inside the United States**
  - We may ***NOT*** conduct searches of other persons
  - We may request the FBI to conduct such a search
- **Other U.S. persons outside the United States**
  - The search is for an authorized foreign intelligence or CI purpose;
  - The search is appropriately coordinated with the CIA; and
  - The FISC or the AG has authorized the search
  - Who can request
    - SecDef, DSD, USD(I); SecAF; USecAF; DIRNSA/CHCSS; Director, DIA; Director, NGA; or Director, NRO

Procedure 8, Mail Searches and Cover

- **Mail searches**
  - See Procedure 7
- **Mail cover**
  - In U.S. postal service channels, request the USPS IAW 39 CFR 233.3(e)(2)
  - In foreign postal channels, may request a mail cover for mail that is to or from a U.S. person consistent foreign law and any applicable SOFA

Procedure 9, Physical Surveillance

- **Who can we surveil *in* the United States:**
  - Military service members;
  - Present or former military or civilian employees of a DIC;
  - Present or former contractors of a DIC;
  - Present or former employees of such a contractor;
  - Applicants for such employment or contracting;
  - Non-U.S. persons (*new*); and
  - Other persons
    - "when **detailed** to the FBI, or
    - when operating **under FBI authorities**."
- ***Outside*** **of the United States**
  - "Any U.S. person . . . for an authorized foreign intelligence or CI purpose" (DoDM 5240.01, para. 3.9.c.(2)(a))

Procedure 9, Physical Surveillance

- **Scope**
  - Any person inside the United States or any U.S. person outside the United States.
  - Also applies to any devices used to observe the subject of the surveillance (not Procedure 6).

- **Defined**
  - Deliberate and continuous observation of a person, and
  - Where the person has no reasonable expectation of privacy
  - Does ***not*** apply to surveillance detection or counter surveillance used to detect and elude foreign physical surveillance

Procedure 9, Physical Surveillance

- **Approval and coordination**
  - **Approval: AFOSI/CC or delegee**
  - **Coordination**
    - **In the United States**
      - No coordination req'd for surveillance of active duty, on-base
      - FBI coord for off-base surveillance
      - FBI coord for surveillance on-base, non-active duty
    - **Outside the United States**
      - CIA coord for off-base surveillance
      - Consider with SOFA and foreign law/policy

Procedure 10, Undisclosed Participation (UDP)

- Scope: Governs the ***participation*** by an defense IC and anyone acting on behalf of an IC, e.g., sources, in any ***organization*** in the United States or any organization outside the United States that constitutes a U.S. person.
- Organization defined
  - An association of two or more individuals formed for any *lawful* purpose whose existence is formalized in some manner
  - Includes those that meet and communicate through the use of technologies
- Participation defined
  - When a person is tasked or asked to participate in an organization for the benefit of the DIC
  - Actions undertaken "for the benefit of" a DIC may include collecting information, identifying potential sources or contacts, or establishing or maintaining cover.

Procedure 10, Undisclosed Participation (UDP)

- **Exclusions**
  - Personal participation
  - Voluntarily provided information
  - Publicly available information on the Internet
    - Collection of publicly available information on the Internet in a way that does *not* require a person to provide identifying information (such as an email address) as a condition of access and does not involve communication with a human being
- **Approval level depends on the activity**
  - No specific level of approval
  - AFOSI/CC or delegee
  - AFOSI/CC or single delegee

Procedure 10, Undisclosed Participation (UDP)

- **Standards for review and approval:**
  - **The potential benefits to national security outweigh any adverse impact on civil liberties or privacy of U.S. persons;**
  - **The proposed UDP complies with the limitations on UDP; and**
  - **The proposed UDP is the least intrusive means feasible and conforms to the requirements of Procedure 2.**

Procedure 10, Undisclosed Participation (UDP)

- UDP requiring no specific level of approval
  - Education or training
  - Cover Activities: Participation in an organization solely for the purpose of obtaining or renewing membership status *in accordance with DoD cover policy*
  - Published or posted information: Participation in an organization whose membership is open to the public solely for the purpose of obtaining information published or posted by the organization or its members and generally available to members; must not involve elicitation.
  - Public forums: Employment affiliation not required and no elicitation of USPI; and
  - Foreign entity

Procedure 10, Undisclosed Participation (UDP)

- **UDP That May Be Approved by a Component Head or Delegee**
  - Non-U.S. persons as potential sources of assistance
  - Public forums: employment affiliation required or elicitation of USPI may be authorized
  - Cover activities beyond obtaining or renewing membership for the purpose of maintaining or enhancing cover
  - U.S. person organizations outside the United States involving participation from or about a non-U.S. person located outside the United States.

Procedure 10, Undisclosed Participation (UDP)

- **UDP That May Be Approved by a Component Head or a *Single* Delegee**
  - To conduct authorized CI activities not otherwise addressed in or outside the United States, after required coordination with the FBI or CIA.
  - To collect information inside the United States necessary to identify a U.S. person as a potential source of assistance to foreign intelligence or CI activities.
  - To collect information outside the United States necessary to assess a U.S. person as a potential source of assistance to foreign intelligence or CI activities.

THE AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

5 pages withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code (U.S.C.), Section 552 (FOIA)				Title 5, U.S.C. Section 552a (PA)	
☐	(b)(1)	☐	(b)(7)(D)	☐	(d)(5)
☐	(b)(2)	☐	(b)(7)(E)	☐	(j)(2)
☐	(b)(3)	☐	(b)(7)(F)	☐	(k)(1)
☐	(b)(4)	☐	(b)(8)	☐	(k)(2)
☒	(b)(5)	☐	(b)(9)	☐	(k)(3)
☐	(b)(6)	☐		☐	(k)(4)
☐	(b)(7)(A)	☐		☐	(k)(5)
☐	(b)(7)(B)	☐		☐	(k)(6)
☐	(b)(7)(C)	☐		☐	(k)(7)

☐ Documents originated with (an)other Government agency(ies). These documents were referred to that agency for review and direct response to you.

____ pages contain information furnished by (an)other Government agency(ies). You will be advised by AFOSI as to the releasability of this information following our consultation with the other agency(ies).

____ pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information:

Pages : 149, 152-155

Exemption (b)(5) protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency. Additionally, it protects deliberative process privilege."

HQ AFOSI/XIL FORM O-3, 19970701 (Word)

Topics Covered

- DoDM 5240.01 Overview
- DoDM 5240.01 Procedures
  - Proc 2, Collection
  - Proc 3, Retention
  - Proc 4, Dissemination
  - Proc 5, Electronic Surveillance
  - Proc 6, Concealed Monitor
  - Proc 7, Physical Search
  - Proc 8, Mail Search/Cover
  - Proc 9, Physical Surveillance
  - Proc 10, Undisclosed Participation
- JA Checklist

Call Your Attorney

Primary POC
(b)(6),(b)(7)(C) **J.D., LL.M.**
Chief, National Security Law
(b)(6),(b)(7)(C)

NIPR: (b)(6),(b)(7)(C) **@us.af.mil**
SIPR: (b)(6),(b)(7)(C) **civ@mail.smil.mil**
JWICS: (b)(6),(b)(7)(C) **@af.ic.gov**

Alternate POC
Maj (b)(6),(b)(7)(C)
Deputy SJA
(b)(6),(b)(7)(C)

NIPR: (b)(6),(b)(7)(C) **1@us.af.mil**
SIPR: (b)(6),(b)(7)(C) **10.mil@mail.smil.mil**
JWICS: (b)(6),(b)(7)(C) **@af.ic.gov**

OSI/JA Main Line
(b)(6),(b)(7)(C)

Page 173 of 3957

THE AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

5 pages withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code (U.S.C.), Section 552 (FOIA)				Title 5, U.S.C. Section 552a (PA)	
☐	(b)(1)	☐	(b)(7)(D)	☐	(d)(5)
☐	(b)(2)	☐	(b)(7)(E)	☐	(j)(2)
☐	(b)(3)	☐	(b)(7)(F)	☐	(k)(1)
☐	(b)(4)	☐	(b)(8)	☐	(k)(2)
☒	(b)(5)	☐	(b)(9)	☐	(k)(3)
☐	(b)(6)	☐		☐	(k)(4)
☐	(b)(7)(A)	☐		☐	(k)(5)
☐	(b)(7)(B)	☐		☐	(k)(6)
☐	(b)(7)(C)	☐		☐	(k)(7)

☐ Documents originated with (an)other Government agency(ies). These documents were referred to that agency for review and direct response to you.

____ pages contain information furnished by (an)other Government agency(ies). You will be advised by AFOSI as to the releasability of this information following our consultation with the other agency(ies).

____ pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information:

Pages : 149, 152-155

Exemption (b)(5) protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency. Additionally, it protects deliberative process privilege."

HQ AFOSI/XIL FORM O-3, 19970701 (Word)

Scenario

- You are stationed in Los Angeles, CA and tasked to surveil a military member suspected of providing classified information to a foreign power. You observe the member meeting with a known Chinese IO, driving a black Jeep Wrangler. While observing the meet you see a second individual, an unknown white male, with closely shaven hair approach the vehicle. In your reporting of the event can you:
  - Identify the primary subject?
  - Identify the Jeep Wrangler?
  - Describe the second individual?
  - What is the assumption of citizenship on the second individual?

Scenario

- You are grabbing a pint at Murphy's pub. You run into an old co-worker who is now an FBI agent. He states he heard you are working on a big Ukrainian FIS case. He wants to know if you can share information with him.

- Can you??

AFOSI and NCIS

Legal Training for BCITP

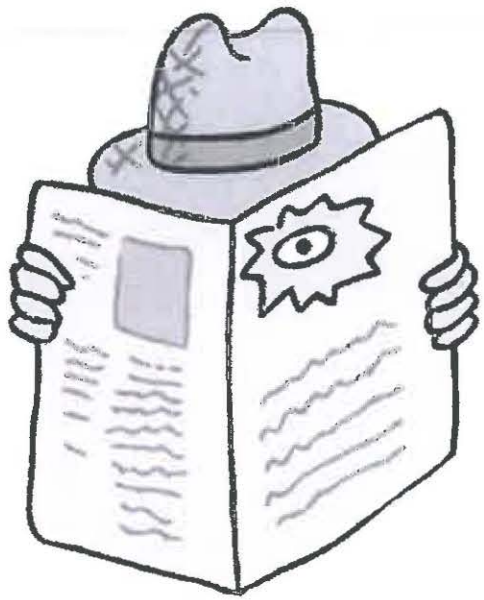
U.S. AIR FORCE

January 2017

Page 177 of 3957

Points of Contact

- **NCIS**
  - (b)(6),(b)(7)(C)
  -
- **AFOSI**
  - (b)(6),(b)(7)(C)
  -



Page 178 of 3957

Agenda

- Significance of Executive Order 12333
  - Key Sections
  - History
  - Today
- Counterintelligence v. Law Enforcement
  - Definition
  - Assigned Missions (E.O. 12333)
- CI Jurisdiction and UCMJ
  - Personal and Subject Matter
  - Article 31(b)

Other relevant provisions of EO 12333

- E.O. 1.4—Role of the IC
  - Collect and provide information needed by the President
  - Collect information on int'l terrorism, proliferation of WMD
  - Analyze, produce, and disseminate intelligence
  - Conduct research, development, and procurement of technical systems and devices for the IC
  - Protect the security of intel related activities, information, installations, property, and employees
- E.O. 1.10—Roles of the DoD
  - The Secretary of Defense shall "collect (including through clandestine means), analyze, produce, and disseminate information and intelligence in response to tasking by the DNI and to execute SecDef's responsibilities

Our Mission per the President, E.O. 12333

- **E.O. 12333, 1.7(f) Intelligence Community Elements: ARMY, NAVY, AIR FORCE, AND USMC.**

- **The Commanders and heads of the intelligence and counterintelligence elements *shall*:**

  (1) Collect (including through clandestine means), produce, analyze and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

  (2) Conduct counterintelligence activities;

  (3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

  (4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations

Counterintelligence Defined

Counterintelligence **means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of *foreign powers*, organizations, or persons, or their agents, or *international terrorist organizations* or activities.**

-- EO 12333, 3.5(a)

What does the threat look like?

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Page 183 of 3957

What are we up against?

Counterterrorism Defined

Counterterrorism is the activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals

-- Joint Publication 3-26 "Counterterrorism," 24 Oct 2014

- FBI is lead for all CT cases in the US

A Very Brief History . . .

- Spying is one of the oldest professions
  - General George Washington noted during the War of Independence "it was the British spies he feared the most."

- Today's laws and policies are the direct result of unfettered intelligence collection by DoD, FBI and CIA in the 1960s and 1970s.
  - Physical surveillance of public figures involved with the anti-Vietnam war and civil rights protests, e.g., MLK
  - Mail openings
  - Break-ins of the offices, vehicles and houses of U.S. persons
  - Undisclosed participation on university campuses

Unfettered Intelligence Collection

In September 1963, Attorney General Robert Kennedy gave permission to the FBI to break into Dr. Martin Luther King's home and install listening Devices.

The result?

- The Church and Pike congressional committees found the IC lacked policy on how to conduct it's mission in regards to U.S. persons
  - Recommended "reining" in Executive Branch powers in using intelligence elements against U.S. persons
  - Created the Permanent Select Committee on Intelligence (Senate) and the Congressional Committee on Intelligence
  - The Foreign Intelligence Surveillance Act was enacted in 1978

- Before Congress passed legislation to correct this deficiency, E.O. 11905 was signed, which was later replaced by E.O. 12333 (standing E.O. on Intelligence Oversight)

Current Concerns

- Continued desire of the U.S. government to ensure Intelligence Community personnel do not engage in activities which are illegal or that violate the rights of U.S. or other persons
  - Patriot Act renewal (renamed USA Freedom Act)
    - "The legislation we're considering proposes major changes to some of our nation's most fundamental and necessary counter-terrorism tools." Senate Majority Leader Mitch McConnell, R-Kent
  - DoDM 5240.01, 18 August 2016 -- NEW

- Areas of concern for the intelligence community:
  - Bulk data collection and databases
  - Insider Threat
    - Security Screening / Network Monitoring / Cyber activities
    - Mission Creep
  - Use of UAVs
  - The Internet
  - Others?

CI and LE Authorities

CI	LE
US Constitution Executive Order 12333 DoDM 5240.01 (Procs 1-10) DoD 5240.1-R (Procs 11-15) FISA (50 U.S.C. § § 1801 et seq) (National Security/Bank Letters) - 18 U.S.C. § 2709 (FBI only) - 15 U.S.C. § 1681v (DoD) - 12 U.S.C. § 3414 (FBI/DoD) - 50 U.S.C. § 3162 (FBI/DoD-travel records also available)	US Constitution DoDD 5200.27 - (U.S. Person) DoDI O-5505.09 - (Intercept Program) 18 U.S.C. § § 2701-2711 (ECPA-Electronic Communications Privacy Act) 18 U.S.C. § § 3121-27 (Pen/Trap Statute) 18 U.S.C. § § 2510-2522 (Wiretap Statute)

CI and Criminal Investigations

- Sister Services are inherently different (due to make-up and missions)
  - Army CI: Conducted solely by Intel professionals (No LE authority)
  - Navy CI: Conducted solely by NCIS Agents (dual CI/LE authorities)
  - AF CI: Conducted solely by AFOSI Agents (dual CI/LE authorities)
- USD(I) Policy controls CI investigations to include use of physical surveillance and other specialized collection techniques

Practice Points

- A CI investigation may transition to more LE methodology and techniques once charges are identified

- The approval authorities for some specialized collection techniques are lower for LE cases (physical surveillance and mail covers) and vice versa (oral wire intercepts)

Who can we investigate?

DoD CI Investigative Jurisdiction (of the Person)

CONUS

- Active Duty Military
- Retired Military, Active or Inactive Reserve, Member of National Guard if suspected offense occurred when subject was in Title 10 status

OCONUS

- AD and DoD civilians and dependents
- DoD contractors or family members (Coor'd with CIA/FBI)
- Retired personnel and other foreign nationals (Coor'd with FBI/CIA)

What can we investigate?

DoD CI Investigative Jurisdiction (subject matter)

- CI Investigative Jurisdiction (Subject Matter)
- Espionage, Treason, Spying, Subversion, Sedition
- FIS directed sabotage
- CI aspects of terrorism
- CI aspects of assassination or incapacitation of personnel
- Suicide/ AWOL of personnel with access/ clearance
- CI aspects of polygraph exams/ refusals
- CI aspects of unofficial travel or foreign contacts
- CI aspects of Insider Threat

Article 31(b), UCMJ

- Article 31(b) advice sounds a lot like Miranda except the military suspect is told what crime(s) they are suspected of committing.
- Also, military members receive the warnings, not only when they're in custody, but anytime they're officially questioned by someone who believes they have committed a criminal offense.
- Article 31(b) advice is an attempt to dispel the inherent compulsion a service member might feel to answer questions during interrogations by military superiors.

Taking a Moment....

Page 196 of 3957

Agenda, Part 2

- E.O. 12333
- DoDM 5240.01
  - Definitions (USPI, collection, retention and dissemination)
  - Procedure 2
  - Procedure 3
  - Procedure 4
  - Scenarios

Part II of EO 12333

"[T]o provide for the effective conduct of intelligence activities and the protection of constitutional rights...." -- EO 12333, Preamble

EO 12333, section 2.3

- Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and *approved by the Attorney General*, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director.

Who is a US Person?

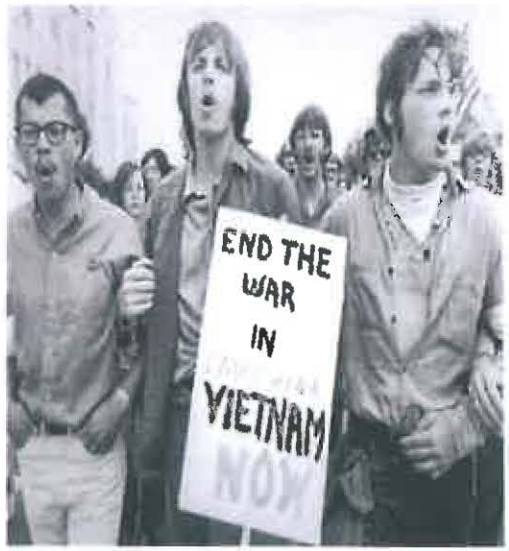
- US citizen
- Lawful permanent resident alien
- Unincorporated association substantially composed of US citizens or permanent resident aliens
- Corporation incorporated in the US, except for a corporation directed and controlled by a foreign government
- **NOTE:** A person or organization outside the US shall be presumed not to be a USP *unless specific information* to the contrary is obtained
- **Foreign national married to a U.S. servicemember?**

What is U.S. Person Information (USPI)?

- Information that is reasonably likely to identify one or more specific U.S. persons.
- May require a case-by-case assessment by a trained intelligence professional.
- May include names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone number, and Internet Protocol address info.
- Does not include:
  - A reference to a product by brand or manufacturer's name in a descriptive sense, e.g., Boeing 737

Basic Principles

- The rules permit CI investigations & operations targeting US persons, but must follow specific procedures
  - Do not infringe the constitutional rights of US persons
  - Protect privacy rights of persons entitled to protection
    - Rights to which a person is entitled depends on status and location
  - Perform a lawfully assigned function
  - Employ least intrusive techniques
    - If conducted in the US or directed against a US person
  - Comply with regulatory requirements
    - Review and approval requirements



Okay, but how can we do it?

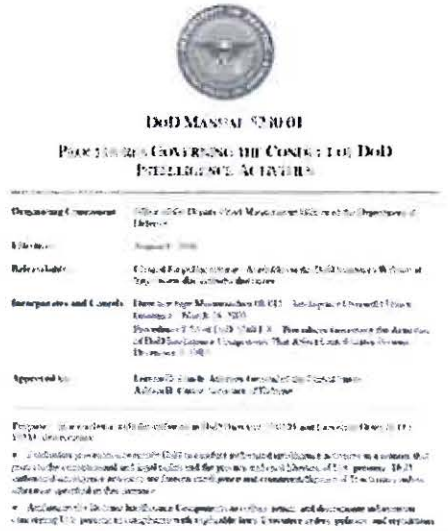
- DoDM 5240.01 and DoD 5240.1-R apply to activities of DoD Intelligence Components

  DoDM 5240.01 (8 Aug 2016)

  - Procedures 2 - 4: Authority to collect, retain, and disseminate United States person information (USPI)
  - Procedures 5 - 10: Guidance for *specialized* techniques to collect foreign intelligence and counterintelligence

  DoD 5240.01-R (7 Dec 1982)

  - Procedures 11 - 15 govern other aspects of DoD intel activities, including the oversight of such activities.



DoD MANUAL 5240.01

PROCEDURES GOVERNING THE CONDUCT OF DoD INTELLIGENCE ACTIVITIES

Procedure 2, Collection of USPERS Info

- Rule 1: You may intentionally collect USPI only if the information sought is *reasonably believed* to be *necessary* for the performance of an authorized intelligence mission or function, and if the USPI falls within one of the 13 categories

- Collection = Information is collected when it is *received* whether or not it is retained for intelligence or other purposes.
  - Regardless of when you use it
  - Computers can collect
  - Intel is collected only once

- Must use LEAST INTRUSIVE MEANS as are practicable when collecting USPI

Procedure 2, Reasonable Belief

- When the facts and circumstances are such that a reasonable person would hold the belief.
- Must rest on facts and circumstances that can be articulated
- Hunches or intuitions are not sufficient.
- Can be based on experience, training, and knowledge of foreign intelligence or CI activities as applied to particular facts and circumstances.

Procedure 2, 13 Collection Categories

1. Publicly Available
2. Consent
3. Foreign Intelligence (FI)
4. Counterintelligence (CI)
5. Threats to Safety
6. Protection of Sources/Methods
7. Current, Former, or Potential Sources
8. Persons in Contact With Sources or Potential Sources
9. Personnel Security
10. Physical Security
11. Communications Security
12. Overhead and Airborne Reconnaissance
13. Administrative Purposes

Procedure 2, 13 Collection Categories

1. **Publicly Available**
   - Not the same as OSINT

2. **Consent**
   - Implied consent: The legal advisor will determine whether a notice or policy is adequate and lawful, before the Component takes or refrains from taking action on the basis of implied consent.

3. **Foreign Intelligence**
   - (a) An individual reasonably believed to be an officer or employee of, or otherwise acting on behalf of, a foreign power;
   - (b) An organization or group reasonably believed to be directly or indirectly owned or controlled by, or acting on behalf of, a foreign power;
   - (c) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist or international narcotics activities;
   - (d) An individual, organization, or group who is a target, hostage, or victim of an international terrorist or international narcotics organization.

Procedure 2, 13 Collection Categories

4. Counterintelligence

- The information is *reasonably believed* to constitute CI and the U.S. person is one of the following:

(a) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in espionage, other intelligence activities, sabotage, or assassination on behalf of a *foreign* power, organization, or person, or on behalf of an agent of a *foreign* power, organization, or person;

(b) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist activities;

(c) An individual, organization, or group reasonably believed to be acting for, or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States; or

(d) An individual, organization, or group *in contact with a person described above* for the purpose of identifying such individual, organization, or group and assessing any relationship with the person described therein.

Procedure 2, 13 Collection Categories

5. Threats to Safety

- Information needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations, if:
  - (a) The threat has a *foreign* connection;
  - (b) Component head or delegee has determined that a person's life or physical safety is *reasonably believed* to be in imminent danger; *or*
  - (c) The information is needed to maintain maritime or aeronautical safety of navigation.

6. Protection of Intelligence Sources, Methods, and Activities

- The information is about U.S. persons who have access to, had access to, will have access to, or are otherwise in possession of information that reveals foreign intelligence or CI sources, methods, or activities, when collection is reasonably believed necessary to protect against the unauthorized disclosure of such information.

Procedure 2, 13 Collection Categories

7. Current, Former, or Potential Sources of Assistance

- The information is about those who are or have been sources of information or assistance, or are reasonably believed to be potential sources of information or assistance, to intelligence activities for the purpose of assessing their suitability or credibility.

8. Persons in Contact with Sources or Potential Sources

- The information is about persons in contact with sources or potential sources, for the purpose of assessing the suitability or credibility of such sources or potential sources.

9. Personnel Security

- The information is arising from a lawful personnel security investigation.

10. Physical Security

- The information is about U.S. persons reasonably believed to have a *foreign* connection and who pose a threat to the physical security of DoD personnel, installations, operations, or visitors
- Must have or be supporting an authorized physical security mission and must be able to articulate a reasonable belief in both the foreign connection of the U.S. persons who are collection targets and the physical security threat they pose

Procedure 2, 13 Collection Categories

11. Communications Security Investigation

- The information is arising from a lawful communications security investigation

12. Overhead and Airborne Reconnaissance

- May intentionally collect imagery that contains USPI provided that the collection is ***not*** directed at a specific U.S. person or, if the collection is directed at a specific U.S. person, the collection falls in one of the other 12 categories
- Includes information obtained from unmanned aircraft systems

13. Administrative Purposes

Procedure 2, Least Intrusive Means

- **Least Intrusive Means**
  - Use the least intrusive collection techniques feasible within the United States or when directed against a U.S. person abroad.
    - Publicly available sources or with the consent of the person concerned
    - Cooperating sources
    - Techniques that do not require a judicial warrant or AG approval
    - Techniques that do require a judicial warrant or AG approval

Procedure 2, Other

- Special Circumstances Collection – BIG DATA
  - Defense Intelligence Components ***will*** consider whether collection opportunities raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information

- Amount of Information Collected
  - In collecting non-publicly available USPI, to the extent ***practicable***, collect no more information than is reasonably necessary

Threshold Questions

- Are we collecting?
- Does the collection concern USPI?
- Does the collection fall within assigned mission/ function?
- Does the information collected fall within one of the 13 permissible categories?
- Are you using the least intrusive method?

- Consider the following collection "formula":

Mission + Reasonable Basis + Procedure = Collection

Procedure 3, Retention

- Permanent retention standard
  - Retention is reasonably believed to be necessary for the performance of an authorized intelligence mission; and
  - The information was lawfully collected or disseminated to the Component
    - Meets one of the 13 collection categories; or
    - Is necessary to understand or assess CI, e.g., information about a U.S. person that provides important background or context for CI.

Page 215 of 3957

Procedure 3, Retention

- Three primary evaluation periods to determine permanent retention of USPI
  - Promptly
  - Five (5) years
  - Twenty-five (25) years

- Intentional Collection of USPI
  - Must be evaluated promptly; and
  - If *necessary*, may retain the information for evaluation for up to 5 years, subject to extension

Page 216 of 3957

Procedure 3, Retention

- **Incidental Collection of USPI**
  - Defined: collection of USPI that is not deliberately sought, but is nonetheless collected
  - *Person in the United States,* may retain all of the incidentally collected information for evaluation for up to 5 years, unless extended
  - *Person outside the United States, may* retain all of the incidentally collected information for evaluation for up to 25 years

- **Voluntarily Provided USPI**
  - About a U.S. person, evaluate the information promptly, up to 5 years, unless extended.
  - About a non-U.S. person, evaluation for up to 25 years

Page 217 of 3957

Procedure 3, Retention

- **Unintelligible information**
  - The time periods begin when the information is processed into intelligible form
  - Includes information that a Component cannot decrypt or understand in the original format.
  - To the extent practicable, unintelligible information will be processed into an intelligible form.
  - Text in a foreign language is considered intelligible

- **Deletion of information**
  - Unless the standards for permanent retention are met, ***must*** delete all USPI from the Component's automated systems of records

Page 218 of 3957

Procedure 4, Dissemination

- We may disseminate USPI based upon the following criteria:
  - Any person or entity: Information is publicly available or U.S. person has consented to the dissemination.
  - Other intelligence community elements
  - Other DoD elements; federal government entities; state, local, tribal, or territorial governments: recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.
  - Foreign governments or international organizations
    - Recipient is reasonably believed to have a need to receive such information for its lawful missions or functions; and
    - Disclosure is consistent with applicable international agreements and foreign disclosure policy
  - Protective Purposes: Necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security

Page 219 of 3957

Questions on Procedures 2 – 4?

BREAK TIME

Page 220 of 3957

Agenda, Part 3

- Special Collection Procedures
  - Procedure 5 – Electronic Surveillance
  - Procedure 6 – Concealed Monitoring
  - Procedure 7 – Physical Search
  - Procedure 8 – Mail Covers
  - Procedure 9 – Physical Surveillance
  - Procedure 10 – Undisclosed Participation

Procedure 5, Electronic Surveillance

- Implements FISA and E.O. 12333
- Defined
  - The installation or use of any monitoring device in the United States where a person has a reasonable expectation of privacy, as determined by the legal advisor, and
  - A warrant would be required for law enforcement purposes.
- Fourth Amendment
  - All electronic surveillance must comply with the Fourth Amendment
  - The legal advisor is required to assess the reasonableness of collection, retention, and dissemination

Page 222 of 3957

Reasonable Expectation of Privacy

- Reasonable expectation of privacy (REP)
  - Can a person have a REP in a government office?
  - REP if a person has a private office with locked door?
  - Does a person in a public street ordinarily have a REP?
  - A person in their vehicle on public roads? A private garage?
- Generally, no expectation of privacy in . . .
  - Bank records (NSL)
  - Public activities
  - Garbage left at the curb, abandoned property
  - Handwriting
  - Smell of luggage
- Legal advisor needs the facts from the field re: REP

Page 223 of 3957

Procedure 5, Electronic Surveillance

- In the United States:
  - Attorney General or the Foreign Intelligence Surveillance Court (FISC) may authorize, except for emergency situations
  - May only conduct such surveillance if both:
    - A significant purpose of the electronic surveillance is to obtain foreign intelligence information; and
    - There is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power

Page 224 of 3957

Procedure 5, Electronic Surveillance

- Outside the United States:
  - U.S. person
    - Governed by FISA and E.O. 12333; or
    - Approval under exigent circumstances exception
  - Non-U.S. person: governed by Title I or Section 702
- Emergency situations: Attorney General approval

- Technical Surveillance Countermeasures (TSCM)
  - Applies to the use of electronic equipment and specialized techniques to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance

Page 225 of 3957

FISA

- Ensure you are written into the FISA request:
  - Make sure your personnel are authorized, within the request to receive FISA info, and that your equipment is authorized to be used as part of FISA collection.
- Dissemination of FISA derived information must include the caveat that use in any criminal proceeding requires prior approval from the AG.

DEPARTMENT OF JUSTICE

Procedure 6, Concealed Monitoring

- Defined as the following:
  - Hidden electronic, optical, or mechanical devices,
  - to monitor a particular person or a group of persons,
  - without consent,
  - in a surreptitious manner,
  - over a period of time, and
  - no reasonable expectation of privacy

- Examples
  - Video monitoring or sound recording of a subject in a place where he or she has no reasonable expectation of privacy if conducted over a period of time
  - Taking one photograph of a subject would not qualify

Procedure 6, Concealed Monitoring

- Scope: Proc 6 applies to the following:
  - Any person inside the United States, and
  - Any U.S. person outside the United States
- With the appropriate approval and coordination, we may conduct concealed monitoring . . .
  - In the United States
    - On DoD facilities
    - Outside DoD facilities after coordination with the FBI
  - Outside the United States
    - On DoD facilities
    - Outside DoD facilities must be coordinated with the CIA, and appropriate host country officials in accordance with any applicable SOFA or other international agreement

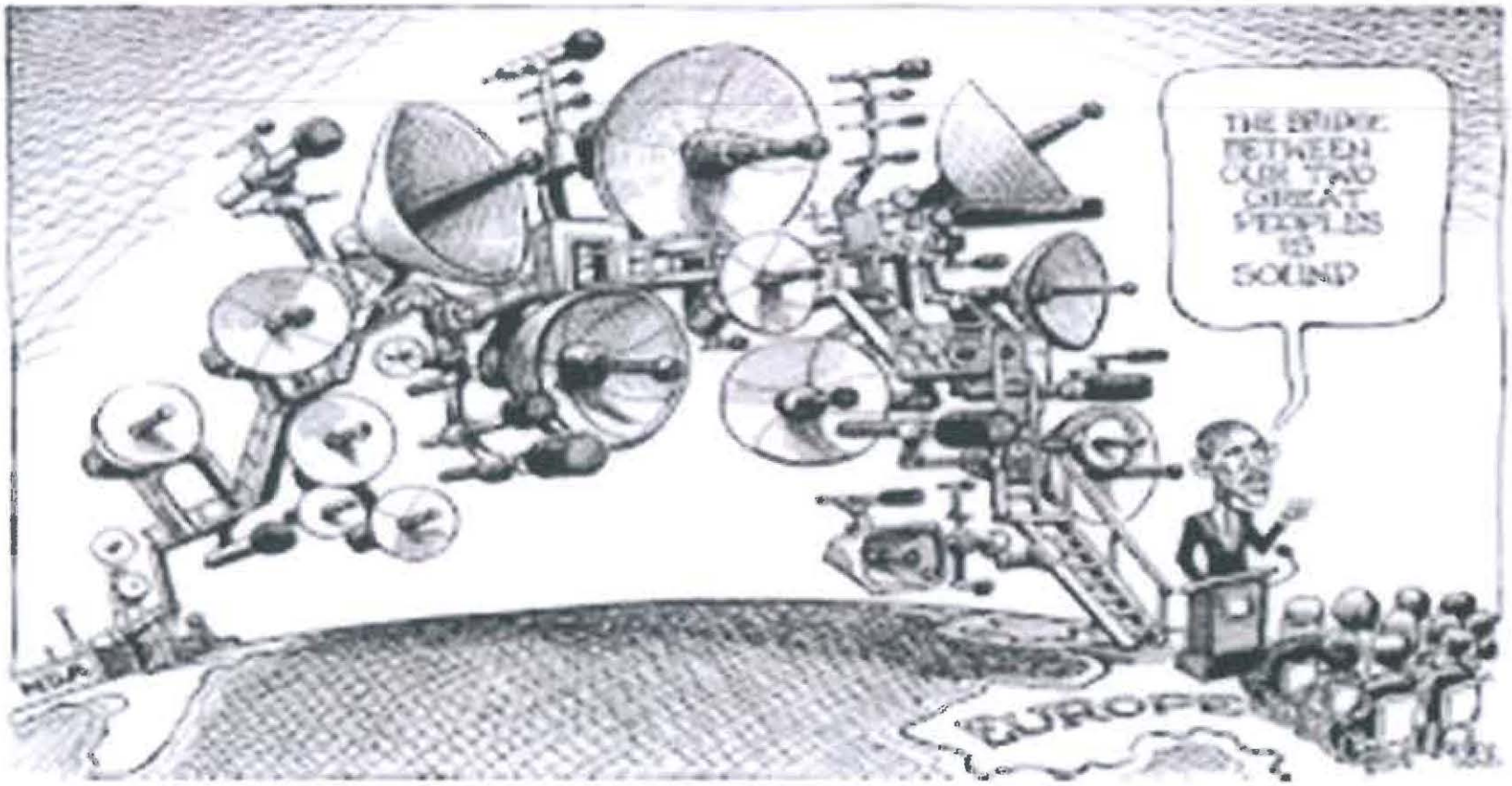
Page 228 of 3957

Procedure 6, Concealed Monitoring

- Approval: Component head or delegee
- Component legal is required to determine whether the following criteria have been met:
  - There is no reasonable expectation of privacy;
  - Such monitoring is necessary to conduct an assigned CI function;
  - A trespass will not be necessary to effect the monitoring; and
  - The monitoring is not subject to Procedure 5
- For more on trespass, see U.S. v. Jones, Sup. Ct. (2012)
  - Physical attachment of GPS tracking device on vehicle to monitor its movement is a trespass/search under Fourth Amendment

Page 229 of 3957

Taking a Moment...



Page 230 of 3957

Procedure 7, Physical Searches

- Scope: Applies to *nonconsensual* physical searches in the United States *and* of U.S. persons/property outside the United States
- Defined: Any intrusion on a person or property that would require a *warrant* for law enforcement purposes
- Does *not* include examinations of the following:
  - Areas that are in plain view and visible to the unaided eye if there is no physical trespass;
  - Publicly available information;
  - Abandoned property in a public place;
  - Items where we have consent; and
  - Government property pursuant to Military Rule of Evidence 314(d)

Page 231 of 3957

Procedure 7, Physical Searches

- **Approval Required**
  - Search of active duty: Attorney General or Foreign Intelligence Surveillance Court
  - Search of other persons inside the United States
    - We may NOT conduct searches of other persons in the U.S.
    - We may request the FBI to conduct such searches
  - Other U.S. persons outside the United States
    - The search is for an authorized CI purpose;
    - The search is appropriately coordinated with the CIA; and
    - The FISC or the Attorney General has authorized the search.
    - Who may request: SecDef, DSD, USD(I); SecAF; USecAF; DIRNSA/CHCSS; Director, DIA; Director, NGA; or Director, NRO

Page 232 of 3957

Procedure 8, Mail Searches and Cover

- **Mail Searches**
  - See Procedure 7

- **Mail cover, e.g., examination of envelope**
  - In U.S. postal service channels, request the USPS IAW 39 CFR 233.3(e)(2)
  - In foreign postal channels, may request a mail cover for mail that is to or from a U.S. person consistent foreign law and any applicable SOFA

Page 233 of 3957

Procedure 8, Mail Searches and Cover

- Any National Security mail cover request must be approved personally by the head of the law enforcement agency or intelligence component requesting the cover or the one designee at the agency's headquarters
- Original signed copy is forwarded to Chief Postal Inspector
- Postal has cleared facilities, request/justification must be specific to case details

Procedure 9, Physical Surveillance

- **Who can we surveil in the United States:**
  - Military service members;
  - Present or former military or civilian employees of a DIC;
  - Present or former contractors of a DIC;
  - Present or former employees of such a contractor;
  - Applicants for such employment or contracting;
  - Non-U.S. persons; and
  - Other persons, "when detailed to the FBI or when operating under FBI authorities."

Page 235 of 3957

Procedure 9, Physical Surveillance

- **Scope**
  - Any person inside the United States or any U.S. person outside the United States
  - Applies to any devices used to observe the subject of the surveillance (not Procedure 6)

- **Defined**
  - Deliberate and continuous observation of a person, and
  - Where the person has no reasonable expectation of privacy
  - Does <u>not</u> apply to surveillance detection or counter surveillance used to detect and elude foreign physical surveillance

Page 236 of 3957

DoD Intelligence Components

- NSA
- DIA
- The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
- The Assistant Chief of Staff for Intelligence, Army General Staff.
- The Office of Naval Intelligence.
- The Assistant Chief of Staff, Intelligence, U. S. Air Force.
- The Army Intelligence and Security Command.
- The Naval Intelligence Command.
- The Naval Security Group Command.
- The Director of Intelligence, U.S. Marine Corps.
- The Air Force Intelligence Service.
- The Electronic Security Command, U.S. Air Force.
- The counterintelligence elements of the Naval Investigative Service.
- The counterintelligence elements of the Air Force Office of Special Investigations.
- The 650th Military Intelligence Group, SHAPE.
- Other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of E.O. 12333 (reference (a)), applies, provided that the heads of such organizations, staffs, and offices shall not be considered as heads of DoD intelligence components for purposes of this Regulation.

Procedure 9, Physical Surveillance

- **Approval and coordination**
  - **Approval: Component head or delegee**
  - **Coordination**
    - **In the United States**
      - No coord req'd for on-base surveillance of active duty
      - FBI coord for all off-base surveillance
      - FBI coord for on-base surveillance of non-active duty
    - **Outside the United States**
      - CIA for off-base surveillance
      - Consider with SOFA and foreign law/policy

Procedure 10, Undisclosed Participation

- Scope: Governs the participation by DICs and anyone acting on behalf of a DIC, e.g., sources, in any organization in the United States or any organization outside the United States that constitutes a U.S. person.
- Organization defined
  - An association of two or more individuals formed for any lawful purpose whose existence is formalized in some manner
  - Includes those that meet and communicate through the use of technologies
- Participation defined
  - When a person is tasked or asked to participate in an organization for the benefit of the DIC
  - Actions undertaken "for the benefit of" a DIC may include collecting information, identifying potential sources or contacts, or establishing or maintaining cover.

Page 239 of 3957

Procedure 10, Undisclosed Participation

- Exclusions
  - Personal participation
  - Voluntarily provided information
  - Publicly available information on the Internet
    - Collection of publicly available information on the Internet in a way that does not require a person to provide identifying information (such as an email address) as a condition of access and does not involve communication with a human being

- Approval level depends on the activity—see below
  - No specific level of approval (NOT no approval)
  - Component head or delegee
  - Component head or single delegee

Page 240 of 3957

Procedure 10, Undisclosed Participation

- UDP requiring no specific level of approval
  - Education or training
  - Cover Activities: Participation in an organization solely for the purpose of obtaining or renewing membership status *in accordance with DoD cover policy*
  - Published or posted information: Participation in an organization whose membership is open to the public solely for the purpose of obtaining information published or posted by the organization or its members and generally available to members; must not involve elicitation.
  - Public forums: Employment affiliation not req'd and no elicitation of USPI; and
  - Foreign entity: Participation in an organization that is an entity openly acknowledged by a foreign government to be directed or operated by that foreign government or is reasonably believed to be acting on behalf of a foreign power, and the organization is reasonably believed to consist primarily of individuals who are non-U.S. persons.

Page 241 of 3957

Procedure 10, Undisclosed Participation

- UDP That May Be Approved by a component head or delegee
  - Non-U.S. persons as potential sources of assistance
  - Public forums: employment affiliation required or elicitation of USPI may be authorized
  - Cover activities: beyond obtaining or renewing membership for the purpose of maintaining or enhancing cover
  - U.S. person organizations outside the United States: involving participation from or about a non-U.S. person located outside the United States

Procedure 10, Undisclosed Participation

- **UDP That May Be Approved by a Defense Intelligence Component Head or a Single Delegee**
  - To conduct authorized CI activities not otherwise addressed in or outside the United States, after required coordination with the FBI or CIA.
  - To collect information inside the United States necessary to identify a U.S. person as a potential source of assistance to foreign intelligence or CI activities.
  - To collect information outside the United States necessary to assess a U.S. person as a potential source of assistance to foreign intelligence or CI activities

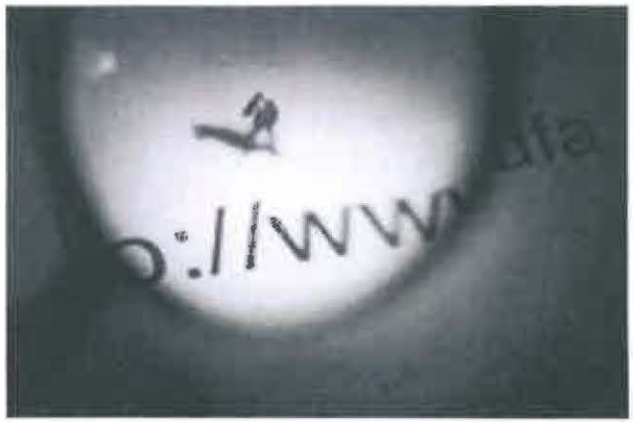
Page 243 of 3957

Procedure 10, Undisclosed Participation

- **Standards for review and approval: approving official must make the following determinations:**
  - **The potential benefits to national security outweigh any adverse impact on civil liberties or privacy of U.S. persons**
  - **The proposed UDP complies with the limitations on UDP; and**
  - **The proposed UDP is the least intrusive means feasible and conforms to the requirements of Procedure 2**

UDP Online/ Social Networking Sites

- Undisclosed Participation is applicable in the CYBER world…
- Is the website an organization/USP? Look to facts:
  - Primarily US users
  - Location of the server
  - Incorporation
  - Website content
  - Language used
  - Richard Shriffin memo
- Other matters
  - Cover Plan?
  - De-confliction?



Take a Moment . . .
(for our LE friends)

Page 246 of 3957

Agenda, Part 4

- Additional Legal Authorities / Special Collection
  - Bank and National Security Letters
    - Right to Financial Privacy Act (12 USC §3401)
    - Fair Credit Reporting Act (15 USC §1681(v))
    - Requests by Authorized Investigative Agencies (50 §USC 3162)
    - FBI Request for Telephone Toll and Transactional Records (18 USC §2709)
  - DoD IG Subpoena
  - Electronic Communications Privacy Act (ECPA), 18 USC §2701
  - Computer Trespasser Exception, 18 USC §2511(2)(i)

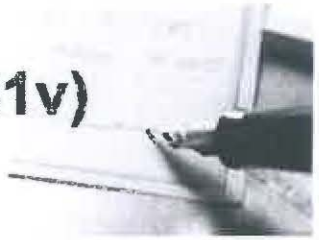
Page 247 of 3957

National Security Letters (NSLs)

- Several Federal statutes authorize intelligence officials to request certain business record information in connection with national security investigations.
- Prospects of continued NSL use is dimming
- What Congress gives, Congress can take away, but for now…..

Summary: Types of NSLs

- Financial Information - Bank Letter (12 USC 3414)
  - Non-compulsory for DoD
    - FBI has authority to compel per para (a)(5)(A)
- Credit Reporting Agency Letter (15 USC 1681v)
  - Compulsory
  - International terrorism only
- Security Clearance Investigations (50 USC 3162)
  - Requires consent; check SF 86 Paperwork!
  - Gets you Bank Records, Credit Reports and Travel Records
  - Compulsory
- Telephone and Toll Records/ISP (18 USC 2709)
  - Available only to the FBI



NSL - Bank Letter, 12 USC § 3414

- **What type of records?**
  - Any record held by a financial institution pertaining to a customer's relationship with the financial institution
  - Customer need not be the target of the investigation
  - Financial institutions broadly defined

NSL - Bank Letter, 12 USC § 3414

From whom can we request?

- Bank
- Savings bank card issuer
- Industrial loan company
- Trust company
- Savings association
- Building and loan, or homestead association (including cooperative banks)
- Credit union
- Consumer finance institution
- Broker registered w/ SEC

- Pawn broker
- Insurance Company
- U.S. Postal Service
- Dealer in jewels and precious stones
- Travel Agency
- Vehicle sales
- Casinos
- Persons involved w/ real estate closings

NSL - Credit Reporting Agency, 15 USC §1681v

- What type of records?
  - Customer credit reports and all other customer records
- Who can we compel to provide?
  - Consumer Reporting Agencies

EQUIFAX
experian
TransUnion

- When?
  - Must be related to International Terrorism

NSL - Security Clearance Investigations, 50 USC § 3162

- What type of records?
  - Financial records
  - Records pertaining to travel outside the U.S.

- Who can we request from?
  - Financial Institutions
  - Credit reporting agencies
  - Commercial entities within the U.S. with records refl travel outside the U.S.

NSL - Security Clearance Investigations, 50 USC § 3162

- TARGET
  - Executive Branch Employee
  - Who as *a condition of access to classified information*
  - Provided consent (during background investigation)
  - for a period of not more than 3 years thereafter to financial and travel records;

AND

Reasonable grounds to believe that the target

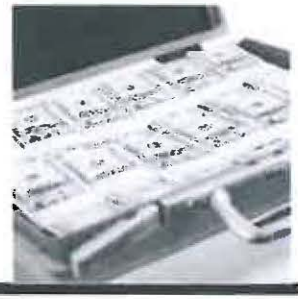
- is or may be disclosing classified info in an unauthorized manner to a foreign power or agent of a foreign power

Or

- has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other info;

Or

- had the capability and opportunity to disclose classified info which is known to have been lost or compromised to a foreign power or agent of a foreign power



NSL Summary Chart

Profile of the Current NSL Statutes

NSL Statute	18 U.S.C. 2709	12 U.S.C. 3414	15 U.S.C. 1681u	15 U.S.C. 1681v	50 U.S.C. 3162
Addressee	communications providers	financial institutions	consumer credit agencies	consumer credit agencies	financial institutions, consumer credit agencies, travel agencies
Certifying officials	senior FBI officials and SACs	senior FBI officials and SACs; or supervisory official of a rank designated by the head of the investigating agency	senior FBI officials and SACs	supervisory official of an agency investigating, conducting intelligence activities relating to or analyzing int'l terrorism	senior officials no lower than Ass't Secretary or Ass't Director of agency w/ employees w/ access to classified material
Information covered	identified customer's name, address, length of service, and billing info	identified customer financial records	identified consumer's name, address, former address, place and former place of employment	consumer report and all other information in a consumer's file	all financial information and foreign travel records relating to consenting employee
Standard/ purpose	relevant to an investigation to protect against int'l terrorism or clandestine intelligence activities	sought for foreign counterintelligence purposes to protect against int'l terrorism or clandestine intelligence activities	sought for an investigation to protect against int'l terrorism or clandestine intelligence activities	necessary for the agency's investigation, activities, or analysis of int'l terrorism	necessary to conduct a law enforcement investigation, CI inquiry or security determination

DoD IG Subpoena

- DoD IG Subpoenas may be used to Support Non-Fraud related investigations when
  - There is sufficient DoD nexus to the crime at issue to warrant the DoD IG's involvement in the investigation
    - Meaning (1) Agency must have investigative authority for the crime under investigation and (2) if the investigation is being conducted jointly the DoD entity must be designated the "lead investigative organization" and
  - The particular crime at issue of such a nature and/or such concern to DoD as to warrant the DoD IG's involvement in the investigation
    - Terrorism, Espionage, Agent for Foreign Government, Spies, Aiding the enemy are among the 25 delineated crimes

DoD IG Subpoena

- Documents and instructions available on DoD IG Website at

http://www.dodig.mil/Programs/Subpoena/subpoena.html

Page 257 of 3957

Mechanisms for Acquiring ISP data

- Request FBI pursue an NSL for Telephone Toll and Transactional Records, IAW 18 USC 2709
  - This option is NOT available to DoD entities in unilateral cases
  - Provides Subscriber Data and toll billing records, along with electronic comm transactional records

- 18 USC 2703 offers several mechanisms that a government entity may use to compel disclosure

Electronic Communications Privacy Act (ECPA)

- BLUF: USGOV can't access emails, data logs or subscriber data with nothing in hand
- ECPA governs information stored on Public Internet Service Providers (ISPs) and on Public Networks
  - Fewer requirements for private networks, such as DoD's
  - Plus, we obtain consent through Banner/User Agreement/IA Training
- General rule for ECPA: it is unlawful to access, obtain, alter or prevent access to wire or electronic communications while in storage by a provider of such communications services

ECPA Summary Chart

Page 260 of 3957

Preservation Letters

- If contemplating action under ECPA the first step is to PRESERVE the stored comms/data
- Requirement to preserve records or evidence in the ISP's possession pending the issuance of court order or other process for 90 days (additional 90 day extension is available) per 18 USC 2703(f)
- How to identify the ISP POC:
  - http://www.copyright.gov/onlinesp/list/a_agents.html (Service Provider's agents for notification of claims of copyright infringement)
  - http://www.search.org/resources/isp-list/

Computer Trespasser Exception, 18 USC §2511(2)(i)

- **Live monitoring of Internet/network communication is lawful provided the four (4) criteria are met:**
  - **1. The owner or operator of the protected computer must authorize the interception of a trespasser's communications.**
  - **2. The person intercepting the communication must be lawfully engaged in an ongoing investigation.**
  - **3. The person intercepting the communication must have reasonable grounds to believe that the contents of the communications to be intercepted will be relevant to the ongoing investigation.**
  - **4. The monitoring must be configured so that it only intercepts the trespasser's communications.**

Taking a moment...

Page 263 of 3957

Agenda

- Material Support to Terrorism (MST) Statutes (18 USC §§ 2339A and 2339B)
- Protection of Defense Information
  - 18 USC §793 - 18 USC §798
  - 18 U.S.C. §1924
  - Classification Reviews and CIPA
- Sanctions
  - TWEA and IEEPA (Dept of Treasury)
- Export Control
  - International Traffic in Arms Regulations (Dept of State)
  - Office of Foreign Assets and Control (Dept of Commerce)

Material Support to Terrorists (MST) Statutes

- "Material support" includes almost any kind of support for blacklisted groups; including humanitarian aid, training, expert advice, "services" in almost any form, and political advocacy.
  - Intent to further the illegal activities of the terrorist organization (presumption that any contribution to a terrorist organization furthers or facilitates criminal activity)

- 18 USC § 2339A Providing material support to terrorists
- 18 U.S.C. § 2339B Providing material support to designated foreign terrorist organizations

MST Applicability to You

- The term "whoever" within the statute and legislative history includes "government actors"
  - Ensure you and your assets are covered!
  - This can be a timely approval process so plan accordingly

- Each Agency has its own
  - Approval policy
    - Lethal Aide
  - Coordination with DOJ

Protection of Defense Information (18 USC 793-798)

- It all started with the Espionage Act of 1917
  - It originally prohibited any attempt to interfere with military operations, to support U.S. enemies during wartime, to promote insubordination in the military, or to interfere with military recruitment.
  - Passed along with the Trading with the Enemy Act
  - Espionage Act was based on the Defense Secrets Act of 1911, especially the notions of obtaining or delivering information relating to "national defense" to a person who was not "entitled to have it"

Page 267 of 3957

Statutes

- 18 USC § 793 - Gathering, transmitting or losing defense information
- 18 USC § 794 - Gathering or delivering defense information to aid foreign government
- 18 USC § 795 - Photographing and sketching defense installations
- 18 USC § 796 - Use of aircraft for photographing defense installations
- 18 USC § 797 - Publication and sale of photographs of defense installations
- 18 USC § 798 - Disclosure of classified information

Use of Classified Information in Court

- For these types of cases you will need the compromised information reviewed for an evaluation of harm to national defense if released and approval for use in charging/ trial
  - This will be a timely and occasionally an "emotional" experience
  - Prior to 2015, DoJ was requiring SECRET or above to charge
- Classified Information Protection Act (CIPA) and MRE Rule 505 provide for protection of the classified information during court proceedings
- False Flag Operations

Sanctions and Export Controls

- The principal statutes underpinning U.S. sanctions and embargos are administered by the Department of the Treasury:
  - The Trading With the Enemy Act (TWEA)
  - International Emergency Economic Powers Act (IEEPA)

These sanctions are further codified by:

- Office of Foreign Assets and Control (Department of Commerce)
- Arms Export Control Act via International Traffic in Arms Regulations (Department of State)

Sanctions: IEEPA (50 USC §§1701-1707)

- Authorizes the POTUS to regulate commerce with certain persons/countries after declaring a national emergency in response to an unusual and extraordinary threat from a foreign source.
  - Country or designated nationals list
  - Non-Proliferation Sanctions
  - Counter Terrorism Sanctions
  - Counter Narcotic Sanctions
  - Transnational Criminal Orgs

- Administered by Dep't of Treasury
- Restrictions apply to all U.S. persons and entities…

Sanctions: Office of Foreign Assets and Control (OFAC)

- OFAC administers a number of different sanctions programs. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals
- OFAC oversees, imposes penalties pursuant to, and grants licenses to permit activities covered by U.S. sanctions.
- Fines for violations: $50K to $100K and imprisonment from 10 to 30 yrs for willful violations.

OFAC Licenses

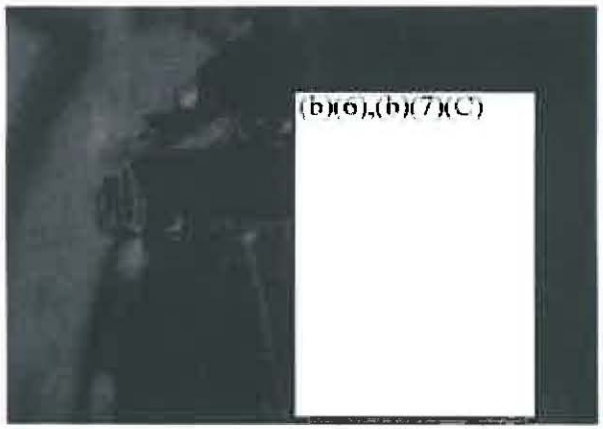
- There are two types of licenses:
  - A general license authorizes a particular type of transaction for a class of persons without the need to apply for a license.
  - A specific license is a written document issued by OFAC to a particular person or entity, authorizing a particular transaction in response to a written license application.
- Persons engaging in transactions pursuant to general or specific licenses must make sure that all conditions of the licenses are strictly observed.

Arms Export Control Act (Inter'l Traffic in Arms Regs)

- Administered by the Department of State
- 22 USC §2778 of the Arms Export Control Act (AECA) provides the authority to control the export of defense articles and services
- Executive Order 11958, as amended, delegated this statutory authority to the Secretary of State.
- International Traffic in Arms Regs (ITAR) implements this authority

ITAR (22 USC §2778)

- All U.S. manufacturers, exporters, and brokers of defense articles, defense services, or related technical data, as defined on the USML, are required to register with U.S. Department of State
- A foreign person is any person who is not a lawful permanent resident of the U.S. and includes foreign governments and organizations



ITAR Exceptions

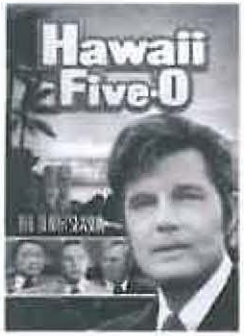
- ITAR does not apply to information related to general scientific, mathematical or engineering principles that is commonly taught in schools and colleges or information that is (legitimately) in the public domain
- Each agency has own procedures and approvals for dealing with ITAR controlled items.

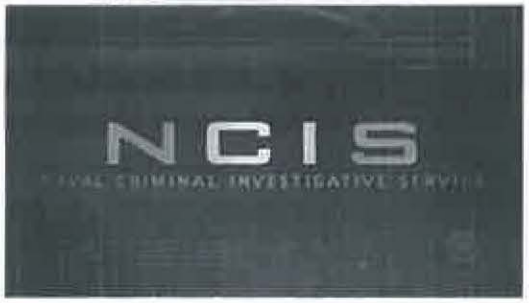
One last chance to meet your attorneys!

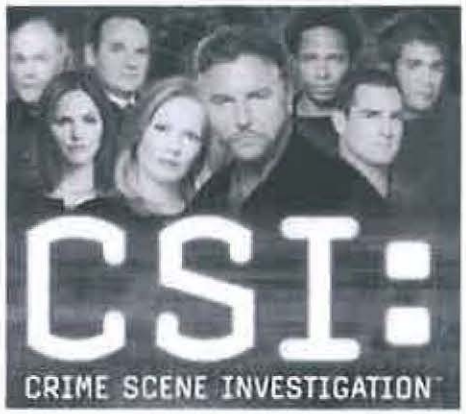
- **NCIS**
  - (b)(6),(b)(7)(C)
  -
- **AFOSI**
  - (b)(6),(b)(7)(C)
  -

Questions?

MARINES
THE FEW THE PROUD







GPS Trackers and Transponders

- U.S. v. Jones, January 2012 Supreme Court Ruling
- Physical attachment of GPS tracking device to monitor a vehicle is a trespass/ search
- Result for DoD?
  - Must use FISA or Procedure 7 –
  - Physical search authority
  - You will need to be able to
  - provide probable cause…

Cognitive-Emotional Conflict

Adversary Will and Social Resilience

By Linton Wells II

Today's information sharing tools let adversaries interfere more directly than ever with a targeted nation's political processes and the minds of its citizens.[1] Operating effectively in such "cognitive-emotional conflict" requires that information-based capabilities be employed and countered in agile, integrated ways across the military, government, and society.[2] Coherent narratives tied to strategy and backed by actions are important.[3] Technical cyberspace activities need to be well-coordinated with content-based approaches like military information operations, government-wide messaging, and intelligence gathering (including all forms of security).[4] Even more important is to build a society's resilience against persistent, disruptive, or disinformation campaigns that aim to undermine citizen confidence and core beliefs.[5]

The need for effective messaging is nothing new—targeting the minds of opposing leaders and the morale of their forces has been central to warfare from time immemorial. Historically, galvanizing public opinion in democracies usually has taken dramatic acts, from the Boston Massacre, to Pearl Harbor, to 9/11. Less dramatically, waning public opinion led President Bush to the Surge in Iraq, and President Obama to adjust his approach in Afghanistan. Activists today, however, have much more direct access to growing numbers of citizens, either to advocate for positions, muddy the waters of public opinion with alternative facts and fake news, or leak secrets to wide audiences. Empowered individuals and small groups can leverage media to enhance their impact by ensuring their asymmetric actions against people, societal structures, or military forces are much more widely disseminated. Some information activities will involve cyberspace operations, while some will involve more traditional information means. In any case, government communication tools such as press releases, white papers, web posts, or even leadership speeches rarely are effective counters to these information flows, especially when poorly coordinated.

The U.S. military and intelligence communities are starting to integrate their capabilities better, but implementing whole-of-government approaches is proving much harder owing to diverse interests, capabilities, and understandings of the information environment. Strengthening society's overall resilience to such campaigns is

Dr. Linton Wells II is a Visiting Distinguished Research Fellow at National Defense University. A retired U.S. Navy officer with more than five decades of public service, Dr. Wells served as Deputy Under Secretary of Defense and twice as Principal Deputy Assistant Secretary of Defense.

Page 280 of 3957

even more difficult, and also more important. A variety of reasons, from lack of trust to lack of capability, make it hard for most Western governments to craft and promote effective resilience campaigns. That said, transparency ultimately is a powerful asset, and where checks and balances, horizontal information flows, and citizen engagement exists, societies can adapt and become more resilient to cognitive-emotional attacks. However, the Strategic Multi-Layer Assessment (SMA) and others are doing important work on fake news inoculation and enhancing population resilience, as well as the use of neuroscience to help understand subconscious decisionmaking.[6] Positive steps to reframe and refocus arguments can be used to counter disinformation campaign tactics.[7]

The Continuum of Conflict

Where does cognitive-emotional conflict fit into the broader continuum of conflict that exists today? First one must define the continuum. Strategist Frank Hoffman at National Defense University defines this as measures ranging from "short of armed conflict" to "major theater war."[8] The spectrum includes an "unconventional and special warfare" category that cuts across the entire continuum of violence.[9] Most of the conflicts today fall into the blue and green zones identified in Figure 1.

Measures Short of Armed Conflict

A proposed definition is the employment of covert or illegal activities that are below the threshold of violence. This includes disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of jurisprudence, and financial corruption as part of an integrated design to achieve strategic advantage.[10]

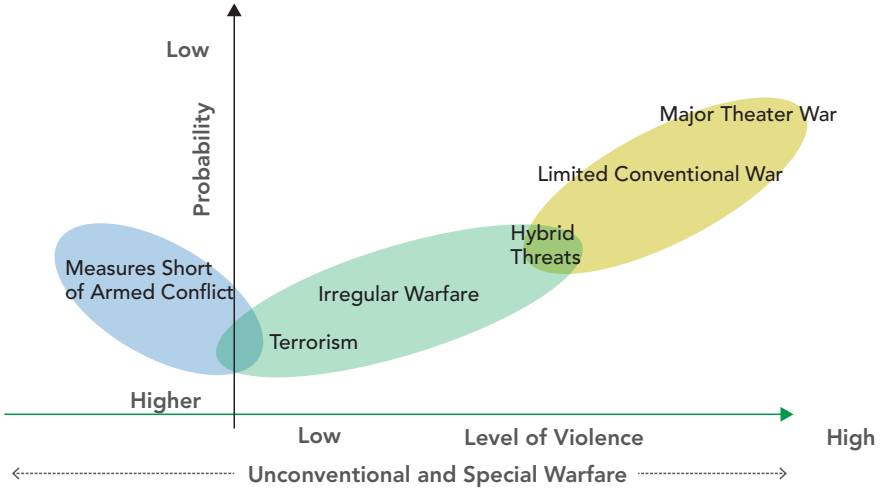
Irregular Warfare and Terrorism

Existing U.S. doctrine defines irregular warfare as a "violent struggle among state and non-state actors for legitimacy and influence over the relevant populations."[11] Irregular warfare is characterized by indirect and asymmetric approaches that avoid direct and risky confrontations with strong forces.[12] Irregular warfare may include criminal activity and/or terrorism.

Hybrid Threats

Hoffman defines this group as the "tailored violent application of advanced conventional military

FIGURE 1: Continuum of Conflict.



capabilities with irregular tactics, or combination of forces during armed conflict."[13]

Theories of Conflict and Resilience

War is "an act of force to compel the enemy to do your will"—fair enough, but a complementary formulation is "… supreme excellence [in war] consists in breaking the enemy's resistance without fighting."[14] Within the continuum of conflict, breaking the resistance of *both* civilian and military adversaries without fighting major wars is an increasingly common objective.

Key arguments in this area were introduced by John Arquilla and David Ronfeldt in their 1993 article "Cyberwar is Coming!"[15] that first introduced the concept of "cyberwar"—"the idea that the vulnerability of communications could cripple an advanced army" by "disrupting, if not destroying, information and communication systems…on which an adversary relies in order to *know itself*…"[16] Cyberwar has proven hard to define, and is not included in the official U.S. military lexicon, but "cyberspace operations" are, and they are associated with powerful technical components, usually considered to be offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and computer network exploitation (CNE).[17] Such operations can impact most conflicts, but often they have been treated as technical capabilities injected from a parallel, networked universe, rather than integrated as part of an overall campaign. However, Arquilla's and Ronfeldt's seminal 1993 article not only discussed how the information age is altering the nature of all conflict, but also introduced the concept of "netwar" in which actors seek to "disrupt, damage, or modify what a target population knows or thinks it knows about the world around it."[18] Today cyberspace operations closely relate to cyberwar with potential impacts on military systems, critical infrastructures, etc., while netwar is increasingly relevant to the cognitive and emotional disruption of societies.[19]

Worldwide, hundreds of billions of dollars are spent to defeat enemies on high-intensity battlefields. Such capabilities are necessary, but insufficient. A variety of cognitive-emotional campaigns are underway, from sustained efforts to undermine respect for liberal democratic values, to initiatives to establish new geopolitical "facts" in East Asian waters. Those suggest that the center of gravity for at least some conflicts is shifting away from military forces toward the political processes, thought leaders, and social media of the targeted populations. Rather than inciting a population to take a particular action, as the leak of the Zimmerman telegram did in accelerating the U.S. entry into World War I, campaigns today often seek to fragment citizen opinions and disrupt belief systems. The ultimate resilience of a nation or an alliance lies in the minds of its citizens who today are under persistent pressure.

There are many definitions of resilience, the best of which include proactive pre-crisis preparations and risk mitigation, effective incident management, and leveraging whatever shocks occur to build back better, as probability scholar Nassim Taleb advocates in his work, *Anti-Fragile: Things That Gain From Disorder.*[20] The Rockefeller Foundation defines resilience as:

> *The capacity of individuals, communities and systems to survive, adapt, and grow in the face of stress and shocks, and even transform when conditions require it. Building resilience is about making people, communities and systems better prepared to withstand catastrophic events—both natural and manmade—and able to bounce back more quickly and emerge stronger from these shocks and stresses.*[21]

The summary of resilience should therefore move from "bounce back" to "be prepared to bounce forward better."[22] How to strengthen the resilience of societies deserves more attention in conflict studies.

Cognitive-Emotional Conflict

Continued, long-term campaigns of disruption, perception management, and deception sow confusion and undercut values and convictions.[23] These campaigns are but one element of cognitive-emotional conflict. Many of their components are not new. They involve violence and the threat of violence, integrating kinetic and non-kinetic elements in ways that would be fully understood by Sun Tzu, Clausewitz, or John Boyd.

The American way of war historically has favored kinetic approaches in environments that clearly distinguish between combat and non-combat, where "one side distinctively wins while the other distinctively loses."[24] Violent action and its connection to policy have long been at the heart of Western military thought, but there also are complementary strategies. Sun Tzu did not clearly delineate between a state of peace and war, though violence and the threat of violence were part of his conception of statesmanship.[25] He did emphasize the importance of deception, perhaps since it helped the leader to "flow" between various states of conflict. Twentieth century military strategist John Boyd later addressed both the offensive and defensive sides of cognitive approaches, noting that strategy should "magnify and augment our inner spirit and strength" while swaying the uncommitted. It should also "isolate adversaries from their allies…[and from] one another, in order to magnify their internal friction, produce paralysis, bring about their collapse…so that they can no longer inhibit our vitality and growth."[26]

Information-based acts in cognitive conflict draw on many tools to "confuse, befuddle, discourage, confound, depress, deny, destroy, degrade, disrupt, usurp, corrupt, deter/dissuade, disconnect, cost-impose, dispose, convey weakness or worse, engender fear (or respect), herd/vector in desired direction and generally negatively impact on victims'/adversaries' ability to see, know, understand, command/control/access his own means, decide, act and be confident of his/her posture, processes or destiny… [These] actions will likely be applied around critical times."[27] Clearly they have been employed before in high-intensity wars (the deception operations surrounding Normandy), other armed conflicts (direct adversary messaging to populations during the Vietnam War and the First Intifada), and in measures short of armed conflict (propaganda and false news to undermine the legitimacy of governments or belief systems).

What is new today is the ease by which modern communications allow adversaries to bypass military forces, borders, and alliances to magnify their voices in the minds of our people, our adversaries, the uncommitted, and our allies.[28] Since experiencing disappointing results in Chechnya in the 1990s the Russians have been refining their "information-psychological" capabilities, which approximate the goals of netwar.[29] Parts of China's "three [unconventional] warfares" relate to efforts to implement "political work."[30] As future cyberspace activities evolve to destroy physical systems more effectively or disrupt essential services, they provide other ways to undercut the confidence of people in their governments.

There is an ample theoretical basis, and a range of operational capabilities, to support a portfolio of cognitive-emotional strategies, from offensive ones to influence opponents, to persuasive ones to encourage neutrality, to defensive ones to build cohesion. This is broader than a cognitive-emotional campaign in the military sense since key parts fall outside military control. Cognitive-emotional conflict is:

> *A struggle to affect the thoughts and values of people at all levels of an opponent's organization and society, using technical and other informational means, while preserving the resilience of one's own organizations and society, and attracting the uncommitted.*

Within this struggle of understanding an adversary's conscious and unconscious perceptions is the recognition that the process of creating actions to shape perceptions will be iterative. The next step is creating and highlighting mismatches in perceptions and using them as weaponized information to target the mind of the adversary and related populations.[31] Since it is impossible to understand perfectly how an adversary's perceptions can be shaped, messages will need to be tested continuously for effectiveness and adapted. Cognitive-emotional conflict thus extends across the entire continuum of conflict, as shown in Figure 2.

U.S. Advantages and Disadvantages in Cognitive-Emotional Conflict

Daunting as the military challenges may be, there are two greater problems: first, how to address coordination beyond the Department of Defense (DOD) in a whole-of-government framework? And then, how to move beyond government to achieve the kind of "whole-of-society" resilience that the nation, and its alliance partners, will need to face the coming cognitive-emotional challenges? The United States starts with a number of advantages, but also serious weaknesses.

U.S. Advantages in Cognitive-Emotional Conflict

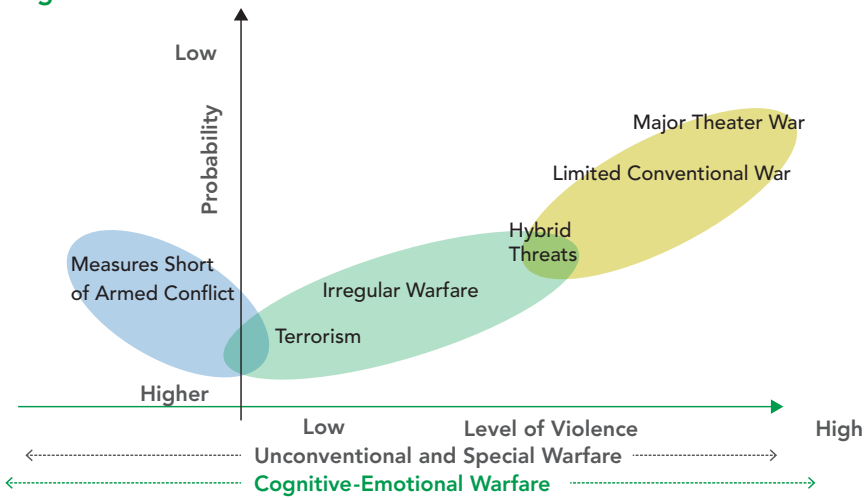
Military/Government Levels

DOD and the Intelligence Community (IC) have exceptional technical cyber capabilities across the full range of OCO, DCO, and CNE as well as many of the non-cyber disciplines, to include electronic warfare, operational deception, space, and command and control. Additionally, Special Operations Forces and parts of the cyber community can adapt quickly to emerging technology and changing circumstances. The U.S. hacking community also is more integrated into the cybersecurity community than in many other countries, partnering through programs like "bugs for bounty" and hackathons.

National Levels

Our diverse population and relatively open system is able to adapt in complex, uncertain environments. Many studies suggest that closed systems begin to lose their adaptability under adversity, and eventually come to be at risk of survival. Such closure can occur either through top down direction (such as isolating a national internet), or a self-selecting series of actions, such as choosing only reinforcing information sources (echo chambers) that limit understanding of a rapidly evolving environment.

FIGURE 2: Cognitive-Emotional Conflict Extends Across the Entire Continuum of Conflict.



Former Dean of Princeton's Woodrow Wilson School of Public and International Affairs, Anne Marie Slaughter, observed in 2009 that the United States ought to have significant advantages in a networked world that derive from the heterogeneity of its population, its geographic location, a horizontal social structure, and a culture of entrepreneurship and innovation.[32]

> *In a networked world, the United States has the potential to be the most connected country…If it pursues the right policies, the United States has the capacity and the cultural capital to reinvent itself.*

The United States possesses the checks and balances, diversity, and feedback loops, and is resilient enough to absorb lessons, learn from them, and adapt. A key is to recognize that "the antidote to netwar poison is active transparency," however painful and disruptive that may be to implement.[33]

U.S. Disadvantages in Cognitive Conflict

The exceptional increases anticipated in science and technology capabilities during the next 15 years will have social impacts as well as operational and strategic ones. Many technology fields such as biotech, robotics, information, nanotech, energy, and additive manufacturing are rapidly changing in parallel. These issues affect the winners and losers in society, the way nations interact, and the way our children think. They raise questions for policymakers, ambassadors, commanders, not just technical specialists. Technological changes, and their interactions, need to be considered as strategic variables in national security planning, but they rarely are today.[34]

Military/Government Levels

The United States and its allies, are not organized, trained, and equipped to be agile and effective in cognitive-emotional conflicts today.[35] U.S. military strengths and doctrine have been aligned more with conventional kinetic conflict than with nuanced cognitive-emotional approaches. Achieving integrated effects at strategic, operational, and even tactical levels is complicated by the way the U.S. now separates cyberspace operations, military information support operations (MISO), intelligence, civil affairs, and related fields into discrete disciplines with distinctive organizations, personnel systems, and operational concepts.[36] Though they often are intended to be mutually supporting, campaigns in each of these areas now may not interact as much as they should to produce integrated effects. Often they are executed at very different levels of classification by skilled operators who are doing their best, but who may be largely unaware of each other's needs and accomplishments.

The problem is compounded by how critical information flows increasingly are outside the government's control—for example, products of geographic information systems (GIS) from sources like commercial satellite imagery and unmanned systems—aerial, ground, and underwater. These are augmented by an explosion of new sensors, from smart phones to augmented reality devices, to the Internet of Things. Finally there is the volume, velocity, veracity, and value of information (IV4) produced by the 24/7 news cycle, amplified and accelerated by social media.

National Level

Most Americans do not recognize the threats posed by cognitive-emotional conflicts and weaponized information. Despite the nation's diversity, most Americans are poorly equipped, through language skills or cultural awareness, to engage deeply in foreign cultures.[37] This can make it hard to recognize that different nation states have different views of concepts such as soft power.[38] For example, Russia thinks of soft power as everything short of outright war (deception, fake news, etc.), while the United States

often views soft power as something that attracts people to American ideals.[39] Such differences make it hard to project, or counter, narratives effectively in foreign environments; particularly given how the United States has cognitive-emotional conflict needs that extend globally, but few of our allies can execute cognitive campaigns beyond regional levels.

The United States thus far has given insufficient attention to crafting and disseminating compelling narratives that shape perceptions. We have allowed our once exceptional capabilities for cognitive-emotional conflict—e.g. in the information campaigns of World War II and the activities of organizations like the U.S. Information Agency during the Cold War—to atrophy, and we lack a consistent national narrative to tell our story. Additionally, U.S. practitioners are bound by asymmetric legal, moral, and ethical constraints that often keep them from being agile enough to compete effectively with skilled adversaries in the realm of social media. This admittedly is a complex problem for any open, democratic society that does not perceive an existential threat.[40]

Consider how Russia's state-owned news outlets routinely deliver government-sponsored messages that are increasingly being accepted as unbiased.[41] And al-Qaeda in Iraq did not need to match U.S. armor or firepower. It only needed to record improvised explosive device (IED) attacks for broadcast to the world. It is much easier to kill one American and broadcast the video to millions than it is to try to kill ten thousand Americans in a combined arms maneuver campaign. Effective cognitive-emotional conflict amplifies small events to create effects in the adversary's mind. Daesh has leveraged these techniques through social media and has broadened its appeal to new regions such as Southeast Asia much more rapidly than expected.[42]

U.S. practitioners of cognitive-emotional conflict need excellent situational awareness, supported by securely networked systems and processes with information flowing as freely as possible, even while trying to disrupt and isolate adversary equivalents. The stovepipes among U.S. tools for cognitive-emotional conflict may be understandable, but they cannot deliver integrated effects. Other nations have fewer artificial restrictions. For example, the Russians, like the Soviets before them, do not separate the intelligence, operations, and communications functions, but rather refer to a more integrated "radio-electronic struggle," which avoids many of the inefficiencies caused by divisions among personnel structures, doctrine, management, etc. These are part of whole-of-government approaches.

Improving the Odds of Success in Cognitive-Emotional Conflict

Some suggest that we are reaching the end of the post–World War II international security structure, pressured by the challenges of a risen China, the resurgence of Russia, worldwide migration, and terrorism, and the various national and transnational responses.[43] The emerging structure is not yet clear, but cognitive and emotional elements certainly will be part of any follow-on conflicts. This section addresses the military, whole-of government, and societal actions that could help prepare for cognitive-emotional conflict in our changing world.

Information as a Joint Warfare Function

In July 2017, Chairman of the Joint Chiefs of Staff, General Joseph F. Dunford, Jr., approved the designation of information as the seventh joint warfare function.[44] This designation of information as the seventh joint warfare function opens up possibilities for coordination that are just now beginning to be examined. A strategy for "Operations in the Information Environment" (OIE) was issued almost one year prior, so there is a basis for considering the closer integration of cyber and content along the full spectrum of doctrine, organization, training, material, logistics, personnel, and facilities—better known as DOTMLPF. Other information-based

components that could benefit from closer integration include but are not limited to:

- strategic communications;
- electronic warfare, to include an electromagnetic pulse (EMP) attack;
- kinetic and non-kinetic operations;
- space and counter-space operations;
- operational security (OPSEC);
- military information support operations (MISO), a.k.a. PSYOPS;
- covert action/propaganda;
- controlled and uncontrolled leaks.[45]

These activities involve different skill sets, agencies, armed services, and even organizational cultures, and should include the Intelligence Community. Half steps are unlikely to be effective but, at the same time, trying to eat the whole elephant at once is likely to be overwhelming. First steps should focus on cross-cutting approaches to a few problems to maximize prospects for near-term successes. On the personnel side, recognize that not everyone will be able to perform well in this environment. Train and educate as broadly as possible, but focus on building a core team of exceptional practitioners.

Already the U.S. Navy has combined its intelligence (N2) and communications (N6) functions into an Information Warfare corps. Could/should similar functions be included by other armed services to improve integration and agility? Ironically, the potential split of U.S. Cyber Command from the National Security Agency may complicate these efforts to breakdown stovepipes.[46]

Alternatively, some have suggested that a new "Joint Concept for Cognitive-Emotional Warfare" be developed to give the idea of cognitive-emotional conflict a larger role in the training, budgetary, and force structure processes. Given the ongoing developments, this probably is premature. The other activities should be allowed to mature.

Reshaping the Broader U.S. Government for Cognitive-Emotional Conflict

The nation needs to convey, by all possible means, the narratives it seeks to represent it. Diplomacy—especially public diplomacy—is on the front line of this campaign, supported by aid programs, and the myriad of other messages the United States projects on a daily basis. Executive Branch departments other than Defense and State have important roles to play, as does industry.

The Department of Homeland Security (DHS), for example, is responsible for protecting the .gov domain and critical infrastructure. DHS has well-defined, whole-of-government management structures in-place for steady state and incident response activities.[47] These structures require collaboration with the private sector through mechanisms such as Information Sharing and Analysis Centers (ISACs) and Organizations (ISAOs), and response to a cyber incident could well be an important part of a cognitive conflict campaign.

Communications need to be aligned with strategy, which must be supported by both narrative and action.[48] Distorted information in a disinformation campaign can be reframed, refocusing can counter distraction, reaffirmation can offset dismissive efforts, and reassurance can address information intended to dismay.

Coordinating these activities is likely to be difficult, given the lack of an agreed U.S. national narrative at present, but it must be tried. Democracies have the added challenge of using information legally and ethically within severe constraints, which often are strained in cognitive-emotional conflict. Decisionmakers have no right to be wrong.

Increasing National Resilience against Cognitive-Emotional Conflict

Government action alone is unlikely to resolve key societal issues, given countervailing moral, legal, and ethical interpretations, as well as suspicions

of the government in many quarters. For example, legal and privacy concerns are critical elements of a democratic society, and they need thorough vetting, even though this may impede rapid action on cybersecurity issues. Impassioned policy discussions over security and privacy have existed since the beginning of the internet, and doubtless will continue in new directions as technology continues to evolve. No one side has all the answers, but the debates are essential, and are a far better approach than top down unitary, directed solutions.

Singapore has postulated a "total defense" concept involving military, civil, economic, social, and psychological components.[49] It recognizes citizen participation as essential as connectivity increases and infrastructures become more interdependent. Signs like "our diversity is our strength" are omnipresent across Singapore. Not every nation can match the tight integration of Singapore's population and their general trust in government. However, as noted earlier, nations that have strong systems of checks and balances, feedback loops, and open information flows have great sources of resilience. These should be nurtured, for they are the basis by which the nation can absorb cognitive-emotional attacks and adjust, over time, to the cognitive-emotional campaigns against them.

At the same time, serious research is needed into the basis of, and limits to, societal resilience in a networked world, especially in democracies. For example, what will be the likely impacts on resilience of disruptions of services through cyberattacks on infrastructures? What differentiates a spirited divergence of views from unbridgeable divisions of worldview? In some cases, neuroscience may be able to provide insights.[50] As these are being worked out, the critical importance of transparency remains. The adjustments are not likely to be quick, smooth, or painless, but they must happen, and represent one of the nation's greatest strengths in cognitive-emotional conflict.

Parting Thoughts

Today's environment is particularly conducive to cognitive-emotional conflicts, owing to the rise of cyber interconnectedness and the range and reach of information sharing tools. There are billions of netizens and billions more will connect during the next few years. This level of connectedness accelerates change and can disrupt many of the policy formulation mechanisms that are legacies of the industrial age, "When decision-makers had time to study a specific issue and develop the necessary response or appropriate regulatory framework."[51] Cognitive-emotional conflict thrives in this dynamic, interconnected environment, and the "weaponization of information" is one way that it can challenge the established order. Actions, both violent and non-violent, can be tailored for nearly instant network dissemination. The nimble player who can shape perceptions generally wins against slow and methodical one.

Success in these sorts of contests requires the nimble, nuanced, and harmonized use, not only of all aspects of national power, but also of non-state and transnational instruments.[52] Strategy, narrative, and actions need to be aligned. Cyberspace operations need to be integrated with "other information-based attacks, defenses, or exploitations as a means for conveying influence, signaling, messaging, or executing strategic communications based on the information-based content itself."[53] All must be supported by intelligence attuned to each area. Decisionmakers and their staffs will need near-real-time situational awareness, yet with options that provide time for reflection. Parts of an engagement will proceed at machine speed with people "on-the-loop," rather than "in-the-loop," while other aspects will require nuanced cultural understanding, sophisticated narratives, and human contact.[54] Throughout, citizens must be informed in credible ways, amidst myriad countervailing information flows, many of them ill-informed at

best, and malicious at worst. Conspiracy theories abound, amplified by information "echo chambers."[55] No organization today—government or civilian—is prepared to deal with all these forces effectively in real-time. PRISM

Notes

[1] This paper represents my personal views and does not reflect the opinions of National Defense University or the U.S. Government. It would not have been completed without major contributions by Maj Phillip Lere, USAF. Dr. Frank Hoffman, Dr. T.X. Hammes, and ADM William O. Studeman, USN (ret.), and Dr. Rebecca Goolsby provided invaluable insights. Any errors are my own.

[2] Cognitive processes involve the acquisition and understanding of knowledge which, while important, are not sufficient to address the full scope of emotions targeted by today's information and disinformation campaigns.

[3] Mark Laity, Director of Strategic Communications at NATO's Allied Command Operations (ACO) repeatedly made this point to a roundtable of senior Southeastern European (SEE) leaders on September 27, 2017.

[4] Cognitive-emotional conflict is defined later in this article. Information Operations are defined in U.S. Joint Publication (JP) 3–13 as "the integrated employment, during military operations, of IRCs [information related capabilities] in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own." JP–3-13, November 27, 2012 incorporating Change 1, November 20, 2014, ix. This definition makes it clear that IO primarily applies to military operations, although the "in concert with other lines of effort" could tie into "whole-of-government," or even "whole-of-society" conflicts. For more information see <http://dtic.mil/doctrine/new_pubs/jp3_13.pdf>. RAND notes IO and IW "… also known as influence operations, includes the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent." For more information see <https://www.rand.org/topics/information-operations.html>.

[5] Resilience is defined later in this article.

[6] From the SMA description: "The Strategic Multi-Layer Assessment (SMA) provides planning support to Commands with complex operational imperatives requiring multi-agency, multi-disciplinary solutions that are NOT within core Service/Agency competency. Solutions and participants are sought across USG and beyond. SMA is accepted and synchronized by the Joint Staff/J-39 Deputy Director for Global Operations (DDGO) and executed by the Deputy Assistant Secretary of Defense (DASD) for Emerging Challenges and Prototyping (EC&P).

See, for example SMA Panel Discussion: Fake News Inoculation and Enhanced Population Resilience, a Department of State Perspective; Booklet July 6, 2017.

Page 289 of 3957

[7] Dr. Rebecca Goolsby proposes four "Rs" (reframe, refocus, reaffirm and reassure) to counter the four "D"s of disinformation campaigns (distort, distract, dismiss, dismay). Presentation to a roundtable of senior Southeastern European (SEE) leaders on September 26, 2017.

[8] F.G. Hoffman, Exploring a Continuum of Contemporary Conflict, December 2016, unpublished.

[9] Unconventional warfare (UW) is defined by U.S. doctrine as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow an occupying power or government by operating through or with an underground, auxiliary, and guerrilla force in a denied area." JP 3–14, *Unconventional Warfare*, September 2015. This mode of conflict is usually done covertly, with low signatures and limited footprint, and conducted primarily by Special Operations forces.

[10] Hoffman, working definition. In his formulation, "Measures Short of Armed Conflict" include so-called "gray zone" operations, which now are not clearly defined in doctrine. That said, others have provided working definitions of "gray zone activity" as "an adversary's purposeful use of single of multiple elements of power to achieve security objectives by way of activities that are typically ambiguous or cloud attribution, and exceed the threshold of ordinary competition, yet intentionally fall below the level of open warfare." U.S. Strategic Multi-Level Assessment (SMA) Gray Zone Effort Update, February 2017, 1. Special Operations Command (SOCOM) has used "Competition Short of Armed Conflict" (CSAC) in lieu of MSAC, ibid, 3.

[11] First established in the Joint Staff (J7) *Irregular Warfare Joint Operating Concept*, version 1.0, Washington D.C., September 11, 2007.

[12] Irregular Warfare often is abbreviated IW, which is confusing in the context of this paper with Information Warfare. Accordingly, "IW" in this paper only refers to Information Warfare.

[13] Hoffman, 19.

[14] Carl Von. Clausewitz, *On War*, translated by Michael Howard and Peter Paret, Princeton University Press,1976, 75. Sun Tsu *The Art of War*, translated by Lionel Giles, Amazon Classics, 2017, available at <https://www.amazon.com/Art-War-AmazonClassics-Sun-Tzu/dp/1542047528/ref=sr_1_3?s=books&ie=UTF8&qid=1502664791&sr=1-3&keywords=art+of+war>. This is a more nuanced formulation than what is sometimes translated as to "defeat an enemy without fighting is the acme of skill."

[15] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy*, Volume 12, Number 2 (1993): 144¬46. Precise definition is used by Arquilla in his interview with FRONTLINE on March 4, 2003, available at < http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>.

[16] Ibid,146.

[17] *Cyber Operations*, JP3–12(R), February 5, 2013,vii and I–3.

[18] Cited in Robert Brose. "Cyber War, Netwar, and the Future of Cyberdefense" DNI, 2012 available at <https://www.dni.gov/files/documents/atf/Cyber%20War%20Netwar%20and%20the%20Future%20of%20Cyberdefense_Header.pdf>, 2-3, et. seq.(emphasis supplied).

[19] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy*, Vol 12, No 2 (1993), 144. Cited in Robert Brose. "Cyber War, Netwar, and the Future of Cyberdefense," 2012, available at <https://www.dni.gov/files/documents/atf/Cyber%20War%20Netwar%20and%20the%20Future%20of%20Cyberdefense_Header.pdf>, 2–3, et. seq.

[20] Nassim Taleb, *Anti-Fragile: Things That Gain from Disorder*, 2014, available at <https://www.amazon.com/dp/B0083DJWGO/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1>.

[21] Rockerfeller Foundation, "Valuing the Resilience Dividend: A New Way Forward," available at <https://www.rockefellerfoundation.org/our-work/topics/resilience/>.

[22] I am indebted to Dr. Dane Egli for his insights about this formulation.

[23] A speaker in Singapore recently referred to this as "slow burn" threats that erode public unity and confidence: Lin Qinghui briefing at the Asia-Pacific Programme for Senior Military Officers (APPSMO), Singapore, August 8, 2017.

[24] CAPT Phil Kapusta, USN, in SMA "Panel Discussion on the Gray Zone in support of USSOCOM," April 27, 2017, 4.

[25] Michael I. Handel, *Masters of War: Classical Strategic Thought*. London: Routledge, 3rd edition, 2000.

[26] Frans Osinga, Science, *Strategy and War: the Strategic Theory of John Boyd*. London: Routledge, 2007, 213.

[27] ADM William O. Studeman, USN (ret.) "Tutorial on Managing the Overlap Between and Alignment of Cyber, Information Warfare/Conflict/Operations and Intelligence (including all forms of security)," February 2017. Critical times include elections, preparation for military operations, during campaigns to build public support, etc.

[28] Osinga op. cit.

[29] Brose, op. cit., 10–11. The complement of "Information-Psychological" capabilities is "Information-Technical" efforts, which equate more to cyberwar.

[30] *Ibid*, 18–23.

Page 291 of 3957

[31] Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," testimony before the Senate Armed Services Committee, Subcommittee on Cybersecurity on April 27, 2017, available at <https://www.armed-services.senate.gov/imo/media/doc/Waltzman_04-27-17.pdf>. Osinga, op. cit., 217.

[32] Anne-Marie Slaughter, "America's Edge: Power in the Networked Century," *Foreign Affairs*, January/February, 2009. Looking back, many aspects of this article now seem optimistic, but the points about the strengths the United States can derive from its diversity and networking seem valid.

[33] Brose, *op. cit*., 28.

[34] James Kadtke and Linton Wells II, "Technology Is a Strategic National Security Component," *Signal* Magazine, January 2015, available at <http://www.afcea.org/content/?q=node/13831>.

[35] Linton Wells II, "Prepared for Battle, But Not Prepared for War," *Proceedings*, (U.S. Naval Institute Press: November 2017).

[36] Military information support operations— Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. Also called MISO. (JP 3–13.2), available at <http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf>.

[37] This extends beyond inabilities to speak foreign languages or unfamiliarity with the norms of other cultures. Richard E. Nisbett, in *The Geography of Thought: How Asians and Westerners Think Differently...and Why*, 2004, examines differences in basic thought processes between US/European and East Asian societies. During a recent Compexity Workshop in Singapore, Dr. Cheong Siew An, in a presentation entitled "Complex Narratives and Identities," noted the difficulty in aligning cultural narratives with historical facts.

[38] Brose, *op. cit*.,15.

[39] Joseph S. Nye, Jr., *Soft Power: The Means To Success In World Politics*, New York: Public Affairs, 2009.

[40] See, for example, CAPT Wayne Porter, TEDx talk "A National Strategic Narrative & Role of American Communities." May 18, 2014, available at <https://www.youtube.com/watch?v=BWO8JJcqrVs>and the broader, website available at <http://nationalstrategicnarrative.org/>.

[41] See, for example: Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*, Public Affairs, 2014; see also "Russia and the Menace of Unreality," *The Atlantic*, September 9, 2014, available at <http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/>, accessed December 30, 2016.

[42] Jerard, "Índomitable Hydra," *op. cit.*

[43] Views expressed at Singapore's International Risk Assessment Horizon Scanning Symposium (IRAHSS), July 18–19, 2017.

[44] The U.S. military traditionally has recognized six warfare functions: Command and Control (C2), Intelligence, Fires, Movement and Maneuver, Protection, and Sustainment. A review of the National Military Strategy (NMS) this year led to an annex on "*Shaping the Joint Force*" that directed the joint force to "treat information as a joint function." Change 1 to Joint Publication 1, *Doctrine for the Armed Forces of the United States*, dated July 12, 2017, established information as the seventh joint function, available at <http://dtic.mil/doctrine/new_pubs/jp1_ch1.pdf>.

[45] Studeman, *op. cit.*

[46] Patrick Tucker, "What the Announced NSA/Cyber Command Split Means," *Defense One*, August 18, 2017, available at <http://www.defenseone.com/technology/2017/08/what-announced-nsa-cyber-command-split-means/140362/>.Based on other reporting, it is not clear the NSA/Cyber Command split has been finalized.

[47] See, for example, Linton Wells II, Motohiro Tsuchiya, and Riley Repko, Improving Cybersecurity Cooperation between the Governments of the United States and Japan <https://spfusa.org/wp-content/uploads/2017/02/Improved-Cybersecurity-cooperation.pdf>, 4–9.

[48] Laity , *op. cit.*

[49] Lin Qinghui briefing at Asia-Pacific Programme for Senior Military Officers (APPSMO), *op. cit*.

[50] SMA, "Leveraging Neuroscience for Understanding the Cognitive Battlefeld," August 2017.

[51] These conflicts are shaped by diverse, dynamic forces, from accelerating technological change, to the Fourth Industrial Revolution as postulated by Dr. Klaus Schwab of the World Economic Forum in: Klaus Schwab, "The Fourth Industrial Revolution: What it Means, How to Respond," January 14, 2016, available at <http://www.weforum.org/agenda/2016/01/>, accessed February 16, 2016. Many of these issues are beyond the scope of the Defense Department's role, but there are steps that DOD can take to help the nation deal with them.

[52] The rapid spread of jihadist ideologies in Southeast Asia during 2015–17 shows an exceptionally nimble, nuanced and integrated use of non-state and trans-national instruments. See Jolene Jerard, "Indomitable Hydra: Transnational Terrorist Threat," presented at the Military Studies Programme Seminar 2017 at the S. Rajaratnam School of International Studies

Page 291 of 3957

(RSIS), Nanyang Technological University, Singapore, August 11, 2017.

[53] Studeman, *op. cit.*

[54] "Man-in-the-loop" refers to situations where people make the key decisions. "Man-on-the-loop" recognizes that some aspects of modern warfare, notable machine-to-machine computer operations move too quickly for people to be engaged at every step and so the person ON the loop must pre-delegate certain ranges of action to the autonomous subsystems when certain criteria are met. This is equivalent to delegating authority under "rules of engagement."

[55] Information flows that reinforce each other to support a particular point of view, or world view, form an "echo chamber."

2021 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Combatting Targeted Disinformation Campaigns

A whole-of-society issue

Part Two

August 2021

2021 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Combatting Targeted Disinformation Campaigns

A whole-of-society issue

Part Two

August 2021

United States

DISCLAIMER STATEMENT: This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.

Acknowledgments

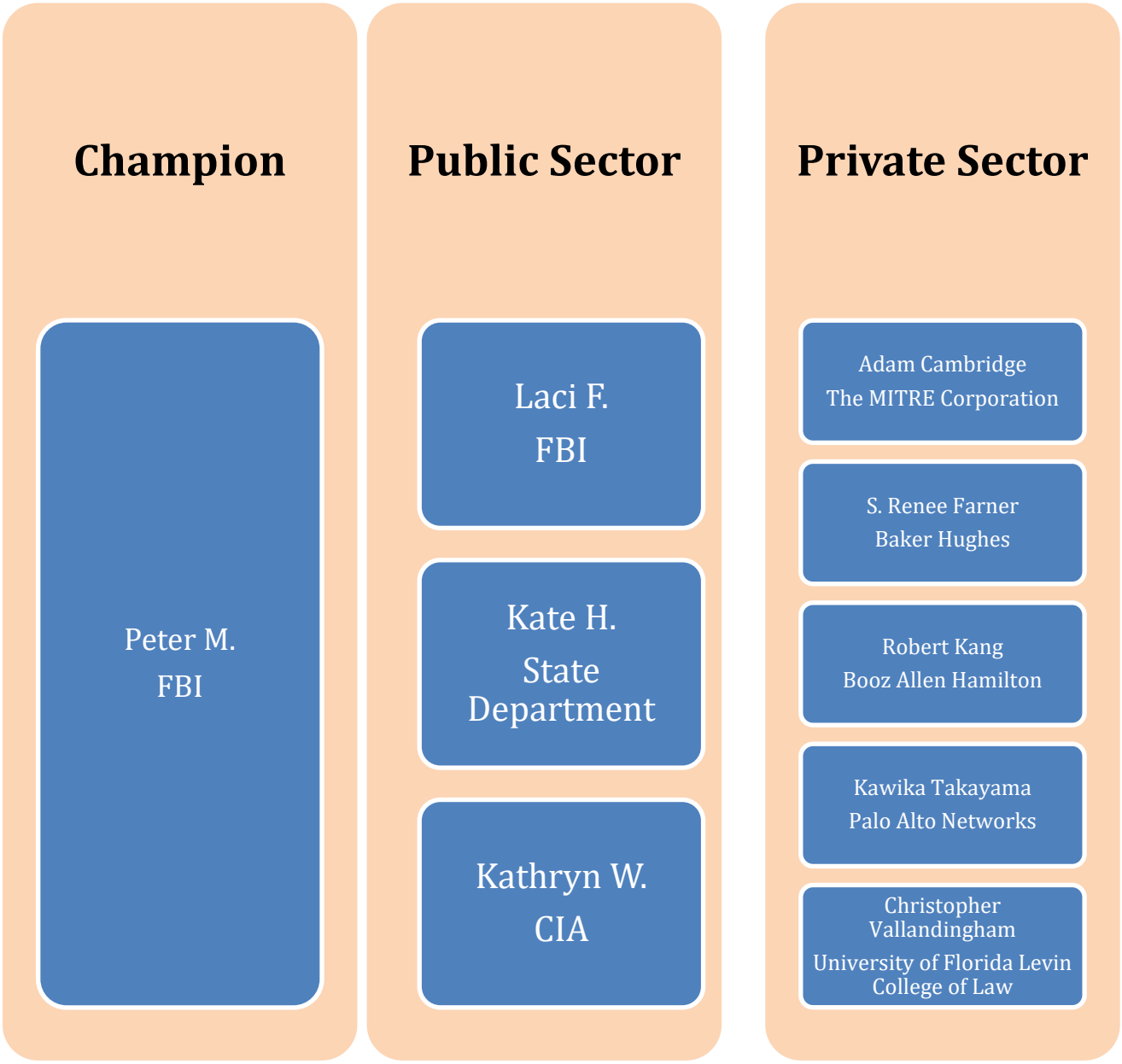
We would like to thank all who contributed to this research amid the unprecedented challenge of the COVID-19 pandemic. This project would not be possible without the assistance of the Office of the Director of National Intelligence and the Department of Homeland Security, who provided us the opportunity to work together on a very important and pressing topic.

We are grateful to the individuals from academia, private sector companies, and think tanks who joined us in our weekly teleconferences to lend their insights on the vexing topic of disinformation campaigns. Their input provided invaluable guidance on lines of inquiry and potential criteria for evaluating the effectiveness of different approaches to countering disinformation campaigns.

We would like to extend a special thank you to Peter M., Team Champion, whose patience and wisdom help guidance us through both years of our project.

We would like to acknowledge the Team members listed below for their contributions on this project and report. We are deeply indebted to Peter Thielen from Booz Allen Hamilton for helping the team to develop a graphic on how to spot dis/misinformation and bringing our vision to fruition and Hale Vallandingham for her assistance with graphics and formatting.

Team Members



Scope

This paper was produced by the Combatting Targeted Disinformation Campaigns team under the auspices of the Public-Private Analytic Exchange Program – an initiative of the Office of Director of National Intelligence and managed by the Department of Homeland Security. The paper was based on open-source research and interviews with subject matter experts. All judgments and assessments are based solely on unclassified sources, are the product of joint private sector and U.S. government efforts, and do not necessarily represent the judgments and assessments of the employers of the Team members.

Offensive and defensive cyber operations conducted by the U.S. government against foreign threat actors are beyond the scope of this paper.

Executive Summary

Recent events have demonstrated that targeted disinformation campaigns can have consequences that impact the lives and safety of information consumers. On social media platforms and in messaging apps, disinformation spread like a virus, infecting information consumers with contempt for democratic norms and intolerance of the views and actions of others. These events have highlighted the deep political and social divisions within the United States. Disinformation helped to ignite long-simmering anger, frustration, and resentment, resulting, at times, in acts of violence and other unlawful behavior.

All information consumers are vulnerable to being deceived by imposters, charlatans, hucksters, con men, and self-proclaimed experts. But ideological rigidity and intolerance of opposing views make information consumers especially vulnerable to such deception. In polarized environments, threat actors find ample opportunity to spread disinformation. Their voices are amplified by disgruntled audiences willing and sometimes eager to spread messages of discord.

Figure 1 Disinformation (obtained from Defense.Info).

In 2019, the Combatting Targeted Disinformation Campaigns team submitted the first of a two-part report on targeted disinformation campaigns.[1] In the first report, we provided

[1] 2019 Public-Private Analytic Exchange Program, Department of Homeland Security, *Combatting Targeted Disinformation Campaigns: A whole-of-society issue*, PDF file, October 2019, https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf (Accessed August 24, 2021).

a broad overview of targeted disinformation campaigns, described how disinformation enters the information ecosystem, how threat actors exploit modern technology, and how information consumers wittingly or unwittingly contribute to the spread of disinformation. We then suggested ways to counter these campaigns. We concluded that, to combat these campaigns, a comprehensive solution involving many sectors of society and lines of efforts was required.

In our second paper, we expand on two themes explored in the first paper: 1) how to stem the supply of disinformation; and 2) how to reduce the demand for disinformation. In this paper, we recommend approaches that impact both supply and demand. None of these approaches are new; nor are they decisive by themselves. When combined and implemented consistently, the sum is greater than the parts.

Figure 2 Dilok Klaisataporn, Shutterstock.

Disinformation should not be viewed as a problem to be solved, but as a condition to be treated. There is no cure. However, preventative and alleviatory measures can be taken.

Recommendations

Source attribution	•Identification of sources of disinformation, when feasible. We believe that threat actors should not be permitted to hide behind the veil of anonymity and identifying them by name gives information consumers important information as they evaluate the truthfulness of the information.
Exposure of imposters	•Exposure of imposters who use false persona and fake credentials to dupe information consumers online. If possible, we believe that uncovering imposters should be done without revealing personally identifiable information about the person.
User control over content	•Greater control by information consumers over the sources of information that appear in their content feeds on social media platforms. We believe that giving information consumers greater control may help to limit the creation of echo chambers.
Fact checking	•Access to content alerts which identify information that is factually incorrect, fraudulent, misleading, or satirical. We believe that such alerts should be politically neutral and based on clear definitions of the categories used.
Psychology of disinformation	•Making information consumers aware of how they process online information and how their online activities facilitate disinformation campaigns will help them make better decisions regarding this information.
Media literacy	•Information consumers who understand how to evaluate the impact of social media and other modern forms of communication on their ability to assess the trustworthiness of information will be more resilient to disinformation.

Page 300 of 3957

Table of Contents

Acknowledgments 2
Team Members 3
Scope 4
Executive Summary 5
Recommendations 7
1. Disinformation Campaigns Are National Security Threats 10
2. Reducing the Supply of Disinformation 13
2.1. Source Attribution and Anonymity 15
2.1.1. Identifying Foreign Actors 15
2.1.2. Identifying Domestic Actors 18
2.1.3. Uncovering Imposters 21
2.2. Social Media Algorithms & Fact-Checking 23
2.2.1. Social Media Algorithms 23
2.2.2. Fact-checking 25
3. The Demand for Disinformation 30
3.1. Cognitive Bias 32
Confirmation bias 32
Belief bias 33
Bandwagon effect 33
3.2. Emotional reactions to disinformation 35
3.3. The Psychology Behind Sharing Information Online 36
4. Media Literacy and Critical Thinking Skills 38
Conclusion 43

Figures

Figure 1 Disinformation (obtained from Defense.Info). 5
Figure 2 Dilok Klaisataporn, Shutterstock. 6
Figure 3 Jimmy Margulies via AP (from ABC news). 10
Figure 4 Divided country (obtained from News Bharati). 11
Figure 5 Source: The MITRE Corporation. 14
Figure 6 State-affiliated media account labels (obtained from Twitter). 17

Page 301 of 3957

Figure 7 OpenAI, GPT-3. 18
Figure 8 Pandemic Profiteers, Center for Countering Digital Hate. 19
Figure 9 Fake identities, (obtained from Wonder How To). 21
Figure 10 Misinformation, (obtained from Agility PR Solutions). 23
Figure 11 A simple algorithm. 25
Figure 12 Reuters. 26
Figure 13 International Fact Checking Code of Principles, IFCN. 27
Figure 14 The Fact Checking Process, (obtained from PesaCheck). 28
Figure 15 Comforting Lies vs. Unpleasant Truths (obtained from News Literacy Matters). 31
Figure 16 Tunnel Vision (obtained from Aftercare.com). 32
Figure 17 See hear speak no evil cartoon (obtained from VectorStock). 33
Figure 18 Blind Leading the Blind (obtained from Conversion Uplift). 33
Figure 19 Cognitive Bias, Raconteur. 34
Figure 20 Angry Comments on Social Media (obtained from ISM Works). 35
Figure 21 Eric Allie/Cagle Cartoons. 37
Figure 22 IREX Media Literacy Training Manual. 39
Figure 23 Critical Thinking Diagram (obtained from Tycoonstory). 40
Figure 24 SMART Graphic | Source: Combatting Targeted Disinformation Campaigns Team 2021 42

1. Disinformation Campaigns Are National Security Threats

Disinformation campaigns are threats to national security because they have a corrosive impact on democratic institutions and civil society in the United States. A healthy democracy depends on well-informed citizens, the competition of ideas, and the willingness to compromise. Disinformation campaigns undermine all three.

Disinformation campaigns have contributed measurably to divisions within U.S. society. Threat actors take advantage of these divisions and harness the power of social media platforms to spread disinformation to large audiences. At times, these disinformation campaigns influence the real-world behavior of information consumers. For example, disinformation about the 2020 presidential elections impacted the lead-up to the events of January 6, 2021 in Washington, D.C. Furthermore, disinformation about the COVID-19 vaccination program has undermined efforts to curb the virus and its variants. Disinformation also weakens international alliances and undermines U.S. attempts to project soft power abroad.

Figure 3 Jimmy Margulies via AP (from ABC news).

Figure 4 Divided country (obtained from News Bharati).

The launch of Sputnik I in 1957 sent shockwaves through the U.S. government. Fearing that the Soviet Union was surpassing the United States in technological and military prowess, the U.S. government responded by investing heavily in human capital and the development of technology. Experts identified weaknesses in educational institutions from primary to graduate levels, insufficient investment in basic and applied research, and governmental bureaucracies ill-adapted to guide the changes deemed necessary to respond to the threat. Major sectors of society contributed to a whole-of-society response to the perceived threat. A similar response is needed today for disinformation campaigns. However, the divisions in our society hinder such a coordinated response.

> *Perhaps because the disinformation crisis has descended upon us so suddenly, and because it reinforces our increasing political polarization, we've tended to regard it as inevitable and unavoidable—a fact of digital life. But we do have options, and if we come together to exercise them, we could make a meaningful difference.*
>
> *Glenn Gerstell, former NSA General Counsel*

In Finland, information literacy forms part of the national curriculum for primary and secondary schools. In math courses, instructors show students how statistics can be manipulated for the purposes of misleading others. In art classes, students learn how images can be altered to change their meaning. In language classes, students are exposed to different ways words can be used to mislead. And finally, students learn in history classes about past propaganda campaigns.

In Malaysia, the Communication and Multimedia Ministry launched an information verification portal called "sebenarnya.my." The public can use this portal to request that the Ministry verify information found online.

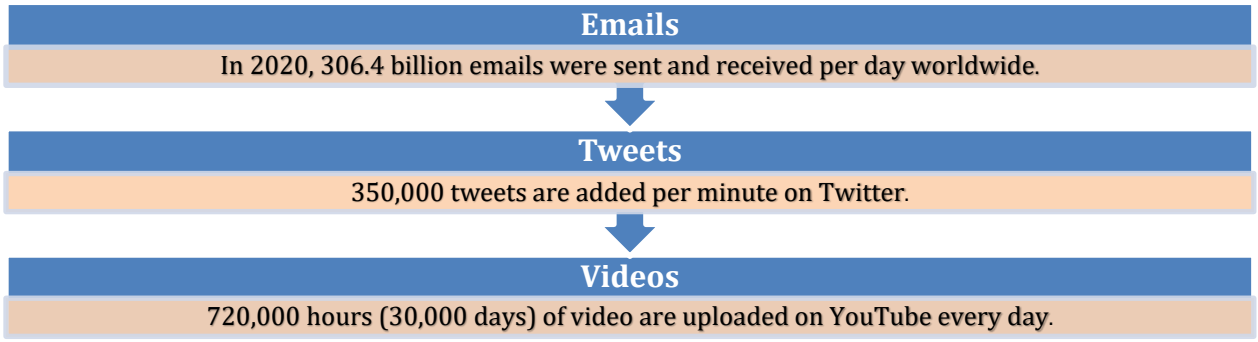
Germany introduced the "Act to Improve Enforcement of the Law in Social Networks" in 2017. This bill requires social media companies with over two million users in Germany to enforce 21 statutes in the German criminal code related to hate speech on their platforms. Platforms must review and delete unlawful content within 24 hours of receiving a complaint or be fined up to 50 million EUR.

Efforts of other countries: Finland [2]; Malaysia[3]; Germany[4]

[2] Jon Henley, "How Finland Starts Its Fight against Fake News in Primary Schools," *The Guardian*, last modified January 29, 2020, https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news (accessed August 24, 2021).
[3] Fairuz Mohd Shahar, "Communications Ministry launches sebenarnya.my to quash fake news, information", New Straits Times, last modified March 14, 2017, https://www.nst.com.my/news/2017/03/220604/communications-ministry-launches-sebenarnyamy-quash-fake-news-information (accessed August 24, 2021).
[4] Nina Jankowicz and Shannon Pierson, "Freedom and Fakes: A Comparative Exploration of Countering Disinformation and Protecting Free Expression", PDF file, Wilson Center, December 2020, https://acrosskarman.wilsoncenter.org/sites/default/files/media/uploads/documents/WWICS%20STIP%20Freedom%20and%20Fakes%20A%20Comparative%20Exploration%20of%20Countering%20Disinformation%20and%20Protecting%20Free%20Expression.pdf (accessed August 24, 2021).

2. Reducing the Supply of Disinformation

Methods exist which can help slow, but not eliminate, the supply of disinformation. The challenge is breathtaking. The global information ecosystem enables the creation and distribution of information on an enormous scale.



The global dissemination of information: Emails; [5] Tweets;[6] YouTube.[7]

In this section, we conclude that technological and non-technological solutions exist that can reduce the likelihood that disinformation will course through the information ecosystem and negatively impact the target audience. These methods include source attribution, fact-checking, and greater user control over algorithms used by social media platforms.

[5]Joseph Johnson, "Number of sent and received e-mails per day worldwide from 2017 to 2025", last modified April 7, 2021, https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide (accessed August 24, 2021).
[6] "Twitter Usage Statistics," https://www.internetlivestats.com/twitter-statistics. (accessed August 24, 2021).
[7] Maryam Mohsin, "10 YouTube Stats Every Marketer Should Know in 2021" (Infographic), last modified January 25, 2021, https://www.oberlo.com/blog/youtube-statistics (accessed August 24, 2021).

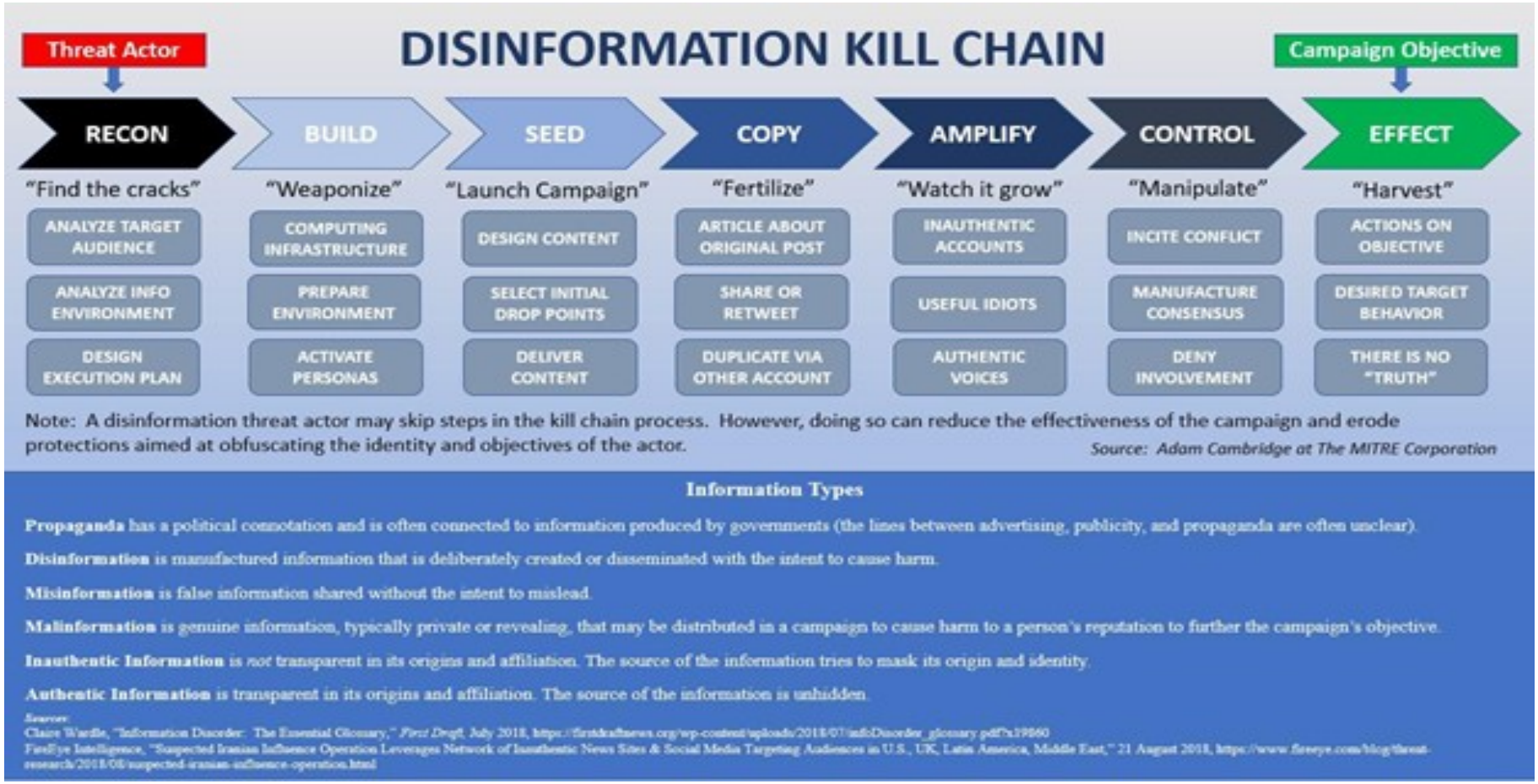


Figure 5 Source: The MITRE Corporation.

2.1. Source Attribution and Anonymity

Providing information about the threat actors responsible for disinformation campaigns can help slow the spread of disinformation since the source of information influences how information consumers evaluate the truthfulness of the information and the decision to later share the information. This method is called source attribution. Source attribution can be conducted in a manner that safeguards the constitutional and statutory rights of U.S. citizens to privacy and the freedom of speech.

In the United States, anonymity has long been considered a necessary component of the freedom of speech. However, anonymity on the Internet is a mixed bag. It not only promotes the discussion of sensitive topics, but also facilitates uncivil behavior and the spread of disinformation. In the next two sections, we consider source attribution of both foreign and domestic threat actors.

2.1.1. Identifying Foreign Actors

"Naming and shaming" is an approach to countering disinformation in which threat actors behind disinformation campaigns are publicly identified. When threat actors use fake personas to deceive, information consumers may decide to disregard the threat actor and the disinformation associated with that threat actor when the deception is uncovered. Once a threat actor is publicly identified, they will be shamed into altering course.

> Our deeply-felt national scruples about misidentifying a fake account or inadvertently silencing someone, however briefly, create a welcoming environment for malign groups who masquerade as Americans or who game algorithms….When tech platforms or regulators strive to take meaningful action to suppress abuse of their platforms and our American polity, there are waves of outrage over censorship. We have conversations about whether or not bots have the right to free speech, we respect the privacy of fake people..
>
> New Knowledge, ***The Tactics & Tropes of the Internet Research Agency***

Private companies have publicly attributed malicious cyber incidents to foreign state actors.[8] The benefits of doing so are usually short-lived since the threat actor will likely change tactics in response. These companies have stated several reasons for engaging in this activity, including supporting internal government discussions by allowing employees not possessing the appropriate security clearances to view information that would likely be classified if provided by the federal government, providing corroborating information for other information gathered by the federal government, and underscoring to the public the reach of the cyber incident.[9]

One method of disseminating this information is through source alerts. Researchers at Harvard University tested whether source alerts help to reduce the likelihood that

[8] Sasha Romanosky and Benjamin Boudreaux, "Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government", PDF file, Rand, January 2019, https://www.cs.dartmouth.edu/~ccpalmer/teaching/cs55/Resources/Papers/RAND_WR1267.pdf (accessed August 24, 2021).
[9] Ibid., 17-20.

information consumers will believe or share political messages. Limiting the study to foreign sources of information and two social media platforms (Twitter and Facebook), the researchers explored whether general ("foreign government") and specific ("Russian government") source alerts did have such an effect.[10] In assessing how the participants in the study viewed the truthfulness of the information, the researchers found that the effects were more significant for specific source alerts than for general ones. Exposure to specific source alerts reduced the probability that the participants would find the disinformation truthful. General and specific source alerts reduced the tendency to "like" or share the disinformation on Twitter only.

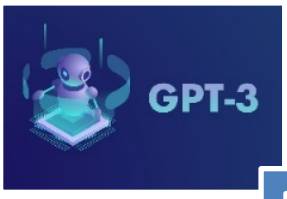
Figure 6 State-affiliated media account labels (obtained from Twitter)

FireEye, CrowdStrike, Dell SecureWorks, and Cisco Talos have publicly identified foreign threat actors.[11] In recent years, both Facebook and Twitter have increased the use of specific source alerts and have tied disinformation campaigns to foreign actors such as the Iran Broadcasting Company and the Royal Thai Military.[12]

[10] Jason Roos Arnold et al., "Source alerts can reduce the harms of foreign disinformation", PDF file, *Harvard Kennedy School Misinformation Review*, May 2021, https://misinforeview.hks.harvard.edu/wp-content/uploads/2021/05/arnold_source_alerts_foreign_disinformation_20210510.pdf (accessed August 24, 2021).

[11] Romanosky and Boudreaux, "Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government." 6.

[12] Josh A. Goldstein and Shelby Grossman, "How disinformation evolved in 2020", Tech Stream, Brookings, last modified January 4, 2021, https://www.brookings.edu/techstream/how-disinformation-evolved-in-2020 (accessed August 24, 2021).



Developed by OpenAI, GPT-3 uses neural networks and machine learning to generate automated text in response to prompts from humans. These texts are difficult to differentiate from those written by humans.

Figure 7 OpenAI, GPT-3.

There are risks associated with source attribution. Such source attribution invites blowback from these threat actors and may undermine ongoing federal law enforcement, intelligence, and diplomatic efforts.

The evidence that such naming "shames" foreign actors into modifying their behavior is thin.[13] However, identifying specific foreign threat actors behind disinformation campaigns gives information consumers the opportunity to evaluate the information with this source attribution in mind and therefore we recommend such attribution when circumstances allow.

❖ Recommendation 1: Identify Foreign Sources of Disinformation

2.1.2. Identifying Domestic Actors

Since the 2016 U.S. presidential election and the emergence of the COVID-19 pandemic, the focus on disinformation campaigns has shifted from foreign

[13] Jack Snyder, "Backlash against naming and shaming: The politics of status and emotion", *The British Journal of Politics and International Relations* 22, no 4 (2020): 644-653.

threat actors to domestic ones.[14] On balance, disinformation campaigns originating from domestic actors are more enduring and damaging than those originating from foreign actors.[15] But, when domestic actors are involved, even if co-opted by foreign actors, the factors that bear on the decision to identify domestic actors differ in important ways from those that apply to foreign actors.

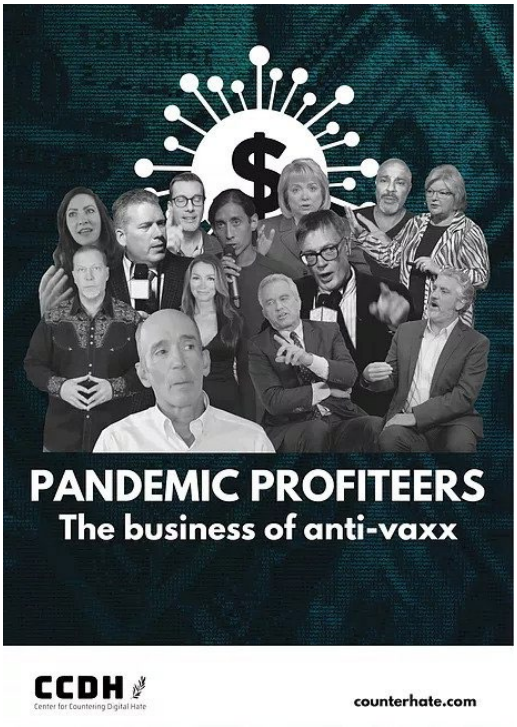


Figure 8 Pandemic Profiteers, Center for Countering Digital Hate.

Both private and public entities have legal obligations to protect information they collect about information consumers. This obligation depends on the type of information collected and how it was collected. Private entities generally have no legal obligation to protect information about information consumers with whom they have no fiduciary relationship, provided the information was gathered through licit means. Therefore, these private entities are free to publish this information when it suits their purpose. For example, in a report published in March 2021, the Center for Countering Digital Hate named twelve information consumers responsible for 73% of anti-COVID-19 vaccine content online.[16]

[14] Larry Luxner, "Ahead of the 2020 US elections, the disinformation threat is more domestic than foreign", Atlantic Council, last modified September 23, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/ahead-of-the-2020-us-elections-the-disinformation-threat-is-more-domestic-than-foreign (accessed August 24, 2021).
[15] Richard Stengel, "Domestic Disinformation Is a Greater Menace Than Foreign Disinformation", *Time*, last modified June 26, 2020, https://time.com/5860215/domestic-disinformation-growing-menace-america (accessed August 24, 2021).
[16] Center for Countering Digital Hate, "The Disinformation Dozen: Why Platforms Must Act on Twelve Leading Online Anti-Vaxxers", PDF file, March 24, 2021, https://252f2edd-1c8b-49f5-9bb2-cb57bb47e4ba.filesusr.com/ugd/f4d9b9_b7cedc0553604720b7137f8663366ee5.pdf. (accessed August 24, 2021).

The report included the name, photo, and screenshots of posts on Facebook and Twitter of each individual. The New York Times later published a more detailed article on the person listed in the report as the greatest offender.[17]

Whether the identification of domestic threat actors by private entities helps to stem the spread of disinformation is unclear. While naming and shaming may be superficially appealing as a method of exacting a price from those who peddle in disinformation, such naming and shaming might make matters worse by provoking a fierce backlash from those sympathetic to the views of the information consumers identified. In the end, this further entrenches both sides in their respective ideological positions.[18] Since polarization is a primary reason for the success of disinformation campaigns, attempting to counter these campaigns with methods which may generate even more polarization seems questionable. Also, revealing the identities of domestic threat actors and other personally identifiable information can render these information consumers vulnerable to harassment or more egregious forms of retaliation.[19] We do not condone harassment and vigilantism as means of responding to domestic threat actors.

Absent suspicion of criminal activity or a legitimate government purpose pursuant to clear legal authority, government monitoring of the opinions and activities of U.S. persons is problematic. Although federal and state law penalize false statements in judicial proceedings and official documents and information consumers may be liable for words

[17] Sheera Frankel, "The Most Influential Spreader of Coronavirus Misinformation Online", *N.Y. Times*, last modified July 24, 2021, https://www.nytimes.com/2021/07/24/technology/joseph-mercola-coronavirus-misinformation-online.html (accessed July 30, 2021).
[18] Ibid.
[19] Kim Zetter, "Cyberbullying Suicide Stokes the Internet Rage Machine", *Wired*, last modified November 21, 2007, https://www.wired.com/2007/11/cyberbullying-suicide-stokes-the-internet-fury-machine (accessed August 24, 2021).

that incite violence, defraud, or defame, disinformation, much less misinformation, is not illegal in most cases.

2.1.3. Uncovering Imposters

An alternative to naming specific domestic threat actors is to alert information consumers to those threat actors who assume fake persona or claim to have credentials which they do not have. The status of the threat actor plays an important role in influencing the perceived trustworthiness of that threat actor.[20] Someone who claims to be an epidemiologist will likely be viewed as more reliable on the topic of coronaviruses than a person who claims to be a bus driver.

Information consumers who assume fake personas or claim fake credentials to deceive others for illegitimate purposes have no moral or legal standing for protection for their fraud, which is a form of disinformation. Revealing that credentials are fake can be accomplished without identifying the threat actor by name or by other information which can be tied to a specific person.

Figure 9 Fake identities, (obtained from Wonder How To).

[20] Edward L. Glaeser, "Measuring Trust", PDF file, *The Quarterly Journal of Economics*, (August 2000): 811-846. https://scholar.harvard.edu/files/laibson/files/measuring_trust.pdf (accessed August 24, 2021).

Threat actors who spread disinformation often seem to act with impunity, facing few negative consequences for the harm that they cause. In some circles, their disinformation may enhance their status and generate lucrative opportunities for them due to the attention that they draw. Legal actions against threat actors are available, but limited in number, and invariably costly and time-consuming. In a deeply divided society, shunning and ostracism no longer have the practical import they may have had in earlier generations. The lack of perceived consequences encourages threat actors to continue their activities. We acknowledge the challenges in today's environment and believe that punitive measures are less effective than measures which provide information about the threat actors upon which information consumers can make better informed decisions.

❖ Recommendation 2: Uncover Imposters

2.2. Social Media Algorithms & Fact-Checking

Challenging disinformation by fact-checking the information and making the results of this fact-checking publicly available is an important method of combatting disinformation campaigns. Disinformation which spreads unchecked through the information ecosystem will ultimately end up in the content feeds of social media platforms. Algorithms determine much of the content which ends up in these feeds. By allowing information consumers more control over these algorithms and the sources which these algorithms utilize, information consumers may have a greater ability to exclude known sources of disinformation.

Figure 10 Misinformation, (obtained from Agility PR Solutions).

2.2.1. Social Media Algorithms

Social media companies use algorithms to sort, index, prioritize, and sometimes suppress the content generated by users of their platforms. These companies can manipulate these algorithms to enhance the profitability of their platforms by attempting to keep users engaged on their platforms as much as possible through attention-grabbing features such as likes, comments, streaks, and recommended posts and people to follow. User activities are recorded, quantified, and used to tailor the user's experience while on the social media platform. On the one hand, algorithms simply give

the user more of what the user's activity on the platform seems to indicate the user wants. On the other hand, these same algorithms potentially create polarizing echo chambers by excluding contrary views.

In April 2021, the United States House of Representatives Subcommittee on Privacy, Technology, and the Law, a subcommittee of the Committee on the Judiciary, met to discuss the impact of algorithms.[21] Several panelists warned of the dangers of algorithms and broadly echoed the sentiments of others who claim that algorithms affect how we see the world[22], erode our ability to freely make choices[23], inherently create polarization[24], and create dangerous feedback loops[25]. The panelists offered solutions ranging from robust federal oversight to a new digital infrastructure which avoids the many problems created by social media platforms in their current forms.

Algorithms influence decision-making in many sectors of society from determining insurance rates to assessing the volatility of stock prices on Wall Street. Algorithms require data to function, which comes in the form of user input on social media platforms.

---

[21] *Algorithms and amplification: How Social Media Platforms' Design Choices Shape Our Discourse and Our Minds,* 117th Congress, Subcommittee on Privacy, Technology, and the Law, Committee on the Judiciary, U.S. Senate, April 27, 2021, https://www.judiciary.senate.gov/meetings/algorithms-and-amplification-how-social-media-platforms-design-choices-shape-our-discourse-and-our-minds (accessed August 24, 2021).

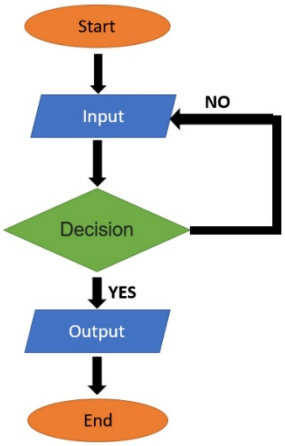
[22] Joanna Stern, "Social-Media Algorithms Rule How We See the World. Good Luck Trying to Stop Them, *Wall Street Journal*, last modified January 17, 2021, https://www.wsj.com/articles/social-media-algorithms-rule-how-we-see-the-world-good-luck-trying-to-stop-them-11610884800 (accessed August 2, 2021).

[23] Lewis Mitchell and James Bagrow, "Do social media algorithms erode our ability to makes decision freely? The jury is out", last modified October 11, 2020, https://theconversation.com/do-social-media-algorithms-erode-our-ability-to-make-decisions-freely-the-jury-is-out-140729 (accessed August 3, 2021).

[24] Charles Johnston, "How Social Media Platforms Inherently Create Polarization", *Psychology Today*, last modified November 29, 2020, https://www.psychologytoday.com/us/blog/cultural-psychiatry/202011/how-social-media-algorithms-inherently-create-polarization (accessed August 3, 2021).

[25] Ben Dickson, "What makes AI algorithms dangerous?", *TechTalks*, last modified June 10, 2020, https://bdtechtalks.com/2020/06/10/ai-weapons-of-math-destruction (accessed August 3, 2021).

Input into algorithms helps to determine the output of these algorithms. Social media platforms ultimately determine what content the algorithms feed into the content streams of users. By providing control of the data that the algorithm uses, platforms may help to ensure users have control over their individual experiences on the platform. Regular reminders to review the information that the algorithms use and make adjustments, if necessary, can help keep users engaged in the process of determining the content that shows up in their content feeds.



❖ Recommendation 3: Grant Users More Control over Content Feeds

2.2.2. Fact-checking

In general, publishers of information have an ethical, legal, and fiduciary responsibility to ensure that they publish information that is accurate. When mistakes are uncovered, publishers can retract articles and posts, send amended versions, and publicly announce the course of action taken to remedy the situation. Notable exceptions are media sites whose content is for satirical purposes or entertainment shows that generate fake news for comic effect. Social media companies are not publishers in the traditional sense of the word. These companies provide platforms where users of these platforms can add content. The user-driven content on these

platforms does not imply that the social media companies endorse the content. While these companies usually grant users the ability to moderate content on the pages and groups formed by the users themselves, content is not first subject to pre-approval by the social media companies prior to posting.

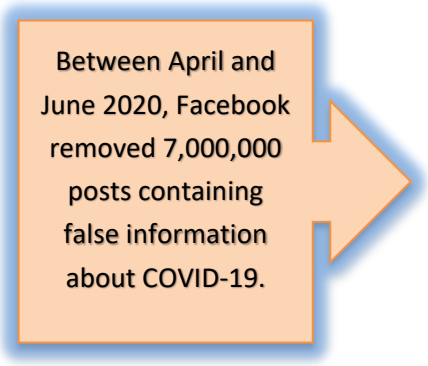


Figure 12 Reuters.

Social media companies arguably play an outsized role in providing access to news and providing a means to share news and other types of information. The power to determine what content is permissible on a social media platform and what is not is a power that social media companies should exercise with great discretion. These determinations should be made based on impartial and easily understood guidelines. Alerting users to the accuracy of information appearing in content feeds plays a useful role in encouraging users to make informed decisions.

Social media platforms, third-party entities, and users themselves can play a role in fact-checking information. If information is determined to be false, the information can be labeled as such, deleted, or supplemented by facts. To minimize the politicization of the process of removing or correcting disinformation, clear distinctions should be drawn between fact-checking, content moderation, and what constitutes improper censorship.

The goal of fact-checking is not to promote or suppress points of view, but to make sure that the information presented can be supported by verifiable information. We urge all fact-checkers to adhere to the principles identified below:

Figure 13 International Fact Checking Code of Principles, IFCN.

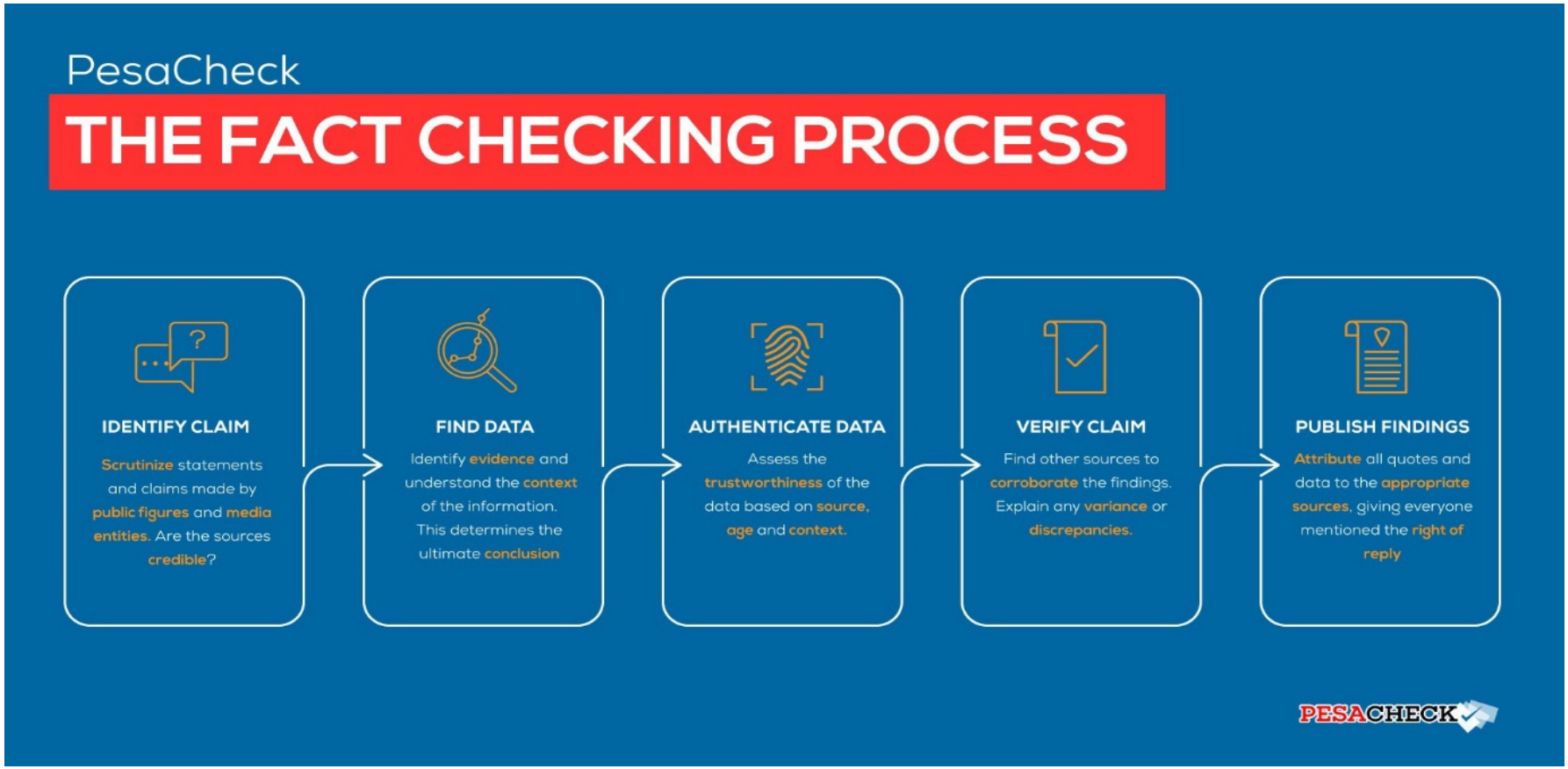
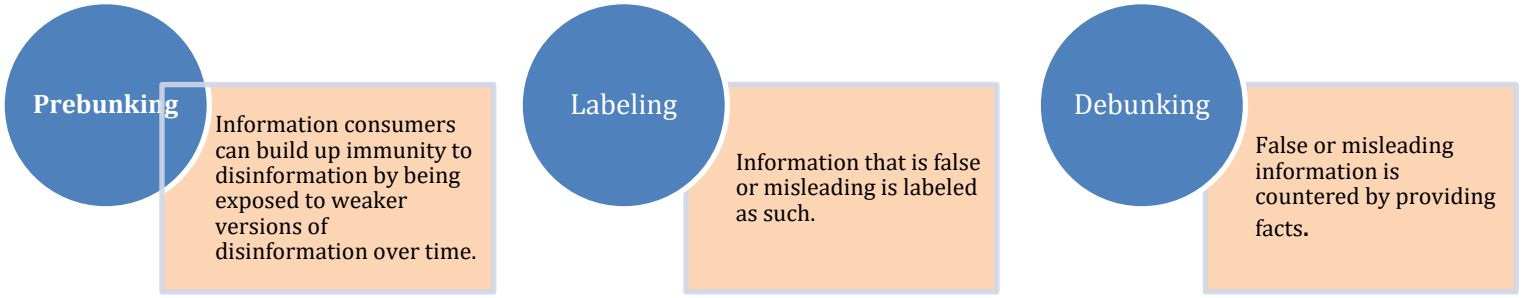


Figure 14 The Fact Checking Process, (obtained from PesaCheck).

Page 321 of 3957

There are different methods of notifying readers that information has been fact-checked, but found to be unverifiable or false.



Researchers have found that the timing of fact-checks provided to readers makes a difference.[26] In one study, participants were exposed to 18 true headlines and 18 false headlines with true and false tags before (prebunking), during (labeling), and after (debunking) reading the headlines. The participants rated the accuracy of each headline. A week later, the participants were asked again to rate the accuracy of each headline. In comparison to prebunking and labeling, debunking had the greatest impact on their ability to discern the truthfulness of the headlines.

More research needs to be conducted into the efficacy of one method versus another, particularly on a longer time scale. However, having accurate information does not necessarily lead to a change in belief.[27] Some researchers maintain that the effect is

[26] Nadia M. Brashier et al., "Timing matters when correcting fake news", *PNAS* 118, no 5 (2021): e2020043118. https://doi.org/10.1073/pnas.2020043118 (accessed August 24, 2021).
[27] Oscar Barrera et al., "Facts, alternative facts, and fact checking in times of post-truth politics", *Journal of Public Economics* 182, (2020). https://doi.org/10.1016/j.jpubeco.2019.104123 (accessed August 24, 2021).

weak.[28] Overall, the impact of fact-checking alone is limited.[29] The ability to spread disinformation far outpaces the ability to fact-check. Therefore, fact checkers need to prioritize where they can best employ their resources. We conclude that challenging misinformation and disinformation online is preferable to allowing both to flow unchecked.

❖ Recommendation 4: Increase Fact-Checking Efforts

3. The Demand for Disinformation

Disinformation campaigns wreak havoc because information consumers consume the disinformation, share it with others, and act upon it. For a variety of psychological and social reasons, information consumers are tempted to believe disinformation without weighing whether the disinformation is supported by evidence or sound reasoning.

> *A cognitive bias is a systemic error in thinking that occurs when people are processing and interpreting information in the world around them and affects the decisions and judgments that they make.*
>
> *Kendra Cherry*

Understanding the influence of cognitive biases and why information consumers make different choices about what to believe and share

[28] Nathan Walter, et. al., "Fact-checking: A Meta-Analysis of What Works and for Whom", *Political Communication* 37, no 3 (2020): 350-375, DOI: 10.1080/10584609.2019.1668894 (accessed August 24, 2021).
[29] Andrew Tompkins, "Is fact-checking effective? A critical review of what works – and what doesn't", *DW AKADEMIE*, last modified December 10, 2020, https://www.dw.com/en/is-fact-checking-effective-a-critical-review-of-what-works-and-what-doesnt/a-55248257 (accessed August 2, 2021).

with others can help make them more resilient to threat actors who exploit the way information consumers think and interact with one another.

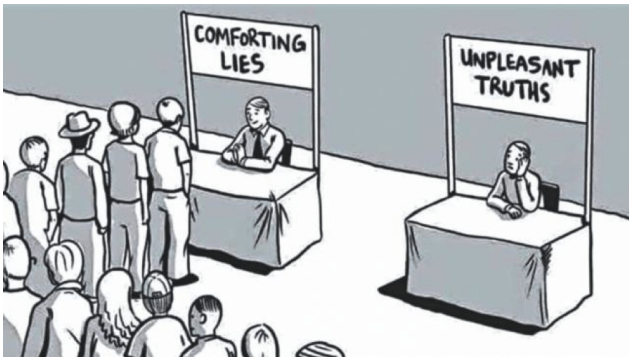


Figure 15 Comforting Lies vs. Unpleasant Truths (obtained from News Literacy Matters).

Threat actors are not alone in attempting to use the lessons of cognitive science and group psychology to their advantage. Governments, religious authorities, and retail advertisers have long taken advantage of psychological and social characteristics of information consumers to induce conformity, sell products, discourage harmful health habits, and otherwise steer thinking and behavior in a desired direction. Information consumers use reverse psychology or play on known weaknesses of others to achieve certain aims. Information consumers are not always aware of these efforts to manipulate them.

The information ecosystem has a profound impact on how we view the world. An information ecosystem contaminated by disinformation can influence people to think, feel, and behave in ways not informed by evidence, but by the duplicity of determined threat actors.

> An environment is, after all, a complex message system which imposes on human beings certain ways of thinking, feeling, and behaving. It structures what we can see and say and, therefore, do. It assigns roles to us and insists on our playing them. It specifies what we are permitted to do and what we are not.
>
> Neil Postman

In this section, we conclude that information consumers can become more resilient to disinformation online by understanding how their brains process information, improving

their ability to think critically, and becoming aware of how their online activity can facilitate the spread of disinformation.

3.1. Cognitive Bias

The mechanisms by which human brains process information make information consumers vulnerable to disinformation. For the human brain to process the enormous amounts of sensory input it receives; the brain has evolved mental shortcuts or "cognitive biases". However, these cognitive biases can undermine the ability to identify relevant facts, weigh the relevance of these facts, and form coherent courses of action based on these facts. Confirmation bias, belief bias, and the bandwagon effect are cognitive biases that are particularly relevant to understanding disinformation campaigns.

Confirmation bias

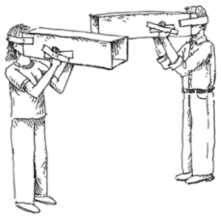


Figure 16 Tunnel Vision (obtained from Aftercare.com).

Information consumers who rely primarily on sources of information that conform to their ideological preferences are particularly vulnerable to disinformation. The design of online search engines, social media platforms, and smartphone applications, plus the availability of cable news programming catering to specific audiences, make it easy to screen information consumers from viewpoints that conflict with their ideological preferences.[30]

[30] Silvia Knobloch-Westwick and Steven B. Kleinman, "Preelection Selection Exposure: Confirmation Bias Versus Informational Utility", *Communication Research* 39, no. 2 (2012): 170-193. https://doi.org/10.1177%2F0093650211400597 (accessed August 24, 2021).

Belief bias

Figure 17 See hear speak no evil cartoon (obtained from VectorStock).

Information consumers tend to favor data and arguments which support their predetermined conclusions and view more harshly data and arguments which do not. While researching the spread of disinformation prior to the 2016 presidential election, researchers determined that whether a news item was accepted as true or rejected as false by information consumers strongly depended on how much it conformed to their belief system.[31]

Bandwagon effect

Figure 18 Blind Leading the Blind (obtained from Conversion Uplift).

Information consumers tend to adopt the beliefs that other people in their political and social networks have. Research has shown that exposure to pre-election polls increases the likelihood that voters will side with majority opinions.[32]

Cognitive biases facilitate analytical errors, lapses in judgment, faulty conclusions, hasty generalizations, and other defects in sound reasoning. Since cognitive biases are features of the human brain, learning how to minimize their impact by developing critical things skills is essential to building resilience to disinformation.[33]

---

[31] Giovanni Luca Ciampaglia and Filippo Menczer, "Misinformation and bias infect social media, both intentionally and accidentally", *The Conversation*, last modified June 20, 2018, https://theconversation.com/misinformation-and-biases-infect-ocial-media-both-intentionally-and-accidentally-97148 (accessed August 24, 2021).

[32] Mike Farjam, "The Bandwagon Effect in an Online Voting Experiment With Real World Political Organizations", PDF file, *International Journal of Public Opinion Research vol 33 (2)* (Summer 2021): 412-421. https://doi.org/10.1093/ijpor/edaa008 (accessed August 24, 2021).

[33] Paul Machete and Marita Turpin, "The Use of Critical Thinking to Identify Fake News: A Systematic Literature Review", PDF file, *IFIP International Federation for Information Processing*, (2020): 235-246. https://link.springer.com/content/pdf/10.1007%2F978-3-030-45002-1_20.pdf (accessed August 24, 2021).

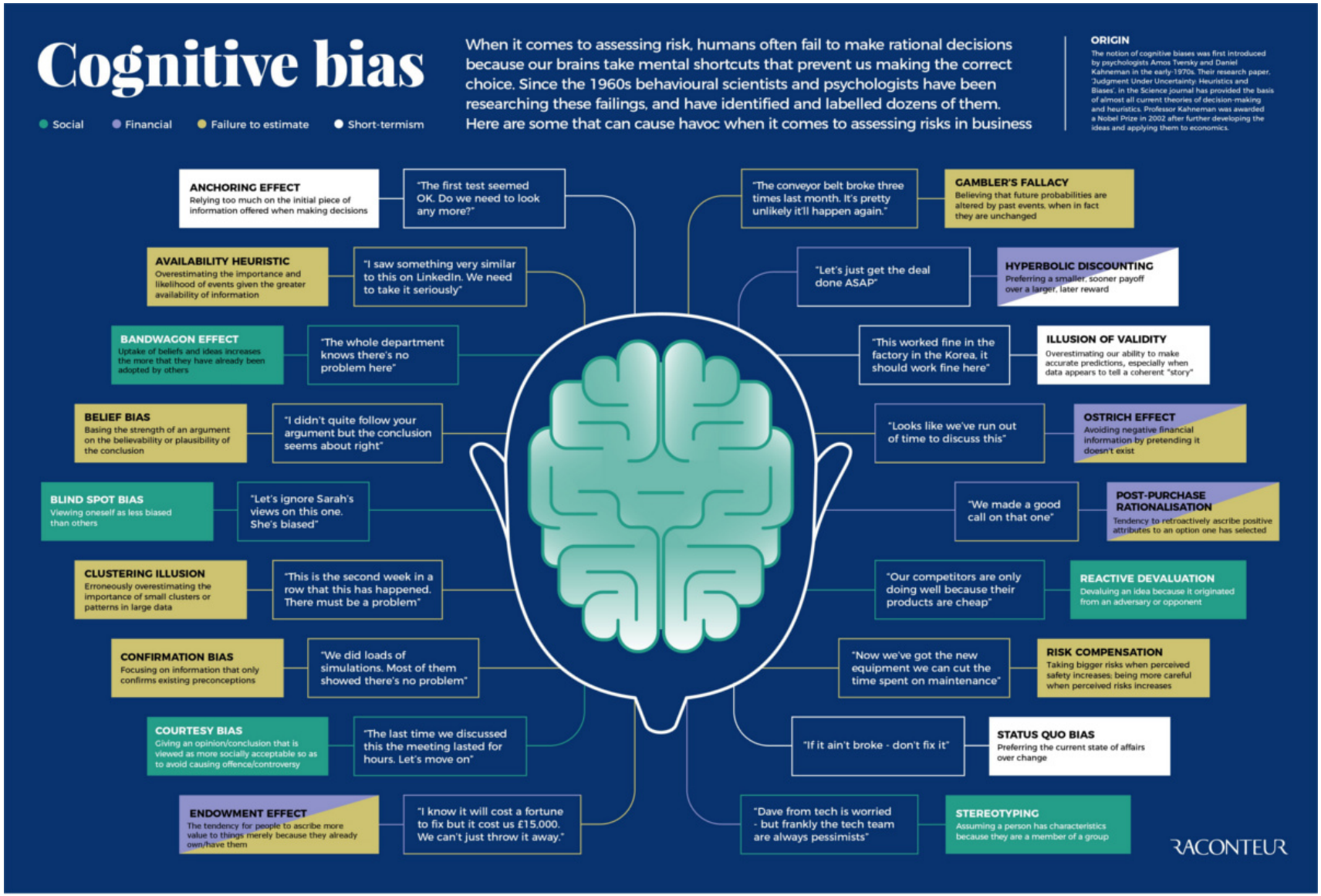


Figure 19 Cognitive Bias, Raconteur.

3.2. Emotional reactions to disinformation

Strong emotions influence the ability of information consumers to process information. Information that elicits strong emotions can overwhelm an individual's ability to think rationally and make prudent decisions. Strong emotions fuel "outrage culture" and lend their force to the incessant volleys of mutual recriminations which are commonplace on social media platforms. Threat actors start disinformation campaigns not to inform, but to agitate, provoke, incite, and inflame. By doing so, they render their audiences more receptive to the disinformation they wish to promote.

Figure 20 Angry Comments on Social Media (obtained from ISM Works).

The belief in the truthfulness of fake news is largely dependent on whether the information consumer relies primarily on reason or emotion to assess the information.[34] The more the information consumer relies on emotion, the more likely the information consumer is to believe in the fake news. Additionally, information consumers are more likely to share information if that information provokes emotional reactions.[35] Researchers determined that the ability to attract an information consumer's attention is key to whether the information consumer will later share this information. Information that does not elicit strong emotions is less

[34] Cameron Martel, Gordon Pennycock, and David G. Rand, "Reliance on emotion promotes belief in fake news", *Cognitive Research: Principles and Implications*. 5:47 (2020). https://doi.org/10.1186/s41235-020-00252-3 (accessed August 24, 2021).

[35] William J. Brady et al., "Emotion shapes the diffusion of moralized content in social networks", *PNAS* 114, no. 28 (2017): 7313-7318. Doi: 10.1073/pnas.1618923114 (accessed August 24, 2021).

likely to attract the attention of information consumers and therefore less likely to be shared.

The circumvention of thoughtful deliberation before acting, rather than the presence of strong emotions, is the key issue. Information consumers often make poor decisions in the heat of the moment, and when blinded by outrage or the desire for revenge. When information consumers encounter information online which elicits such reactions, these feelings should give the individual pause.

3.3. The Psychology Behind Sharing Information Online

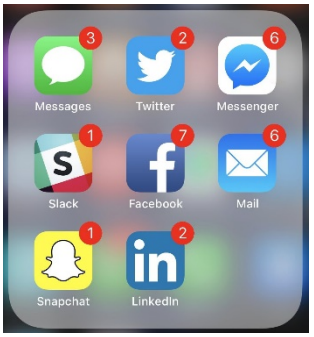
Information consumers who share disinformation help sustain disinformation campaigns and contribute to the rapid spread of disinformation through the information ecosystem. Research suggests that relatively few people intentionally share disinformation on social media.[36] Three main factors that drive the decision to share disinformation are consistency, consensus, and authority.[37] First, the disinformation is consistent with the beliefs that the information consumers already possess. Second, the information consumer believes that most people in his or her social group believe the disinformation. Third, the information consumer believes that the disinformation derives from an authoritative source.

[36] Tom Buchanon, "Why Do People Share Disinformation on Social Media?", PDF file, *Policy Brief*, September 2020, https://crestresearch.ac.uk/download/3040/20-017-03-disinformation-on-social-media.pdf (accessed August 24, 2021).

[37] Tom Buchanon, "Why Do People Spread Disinformation Online: The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation", *PLoS ONE* 15, no 10 (2020): e0239666. https://doi.org/10.1371/journal.pone.0239666 (accessed August 24, 2021).

Figure 21 Eric Allie/Cagle Cartoons.

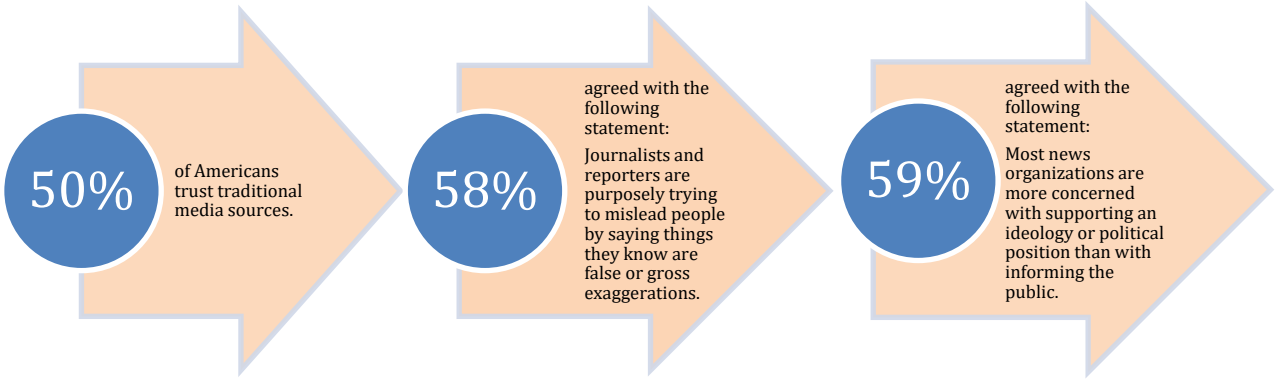
Other factors also play a role in the decision to share disinformation. Information consumers may share disinformation on social media platforms to demonstrate allegiance to a particular idea (similar to virtue signaling), to share novel information, or to draw attention to themselves to increase 'likes', 'views', or 'followers'. Political partisanship motivates information consumers to share disinformation when this disinformation can be used to counter the arguments of political opponents.[38]



Social media platforms have features that incentivize information consumers to share information. These features often have addictive qualities that make it difficult for information consumers to resist the temptation to share information, including disinformation, or to disengage from the platform entirely. Before sharing information online, we encourage information consumers to critically examine the information they wish to share and the motives they have for sharing it. Disinformation at rest is far less effective than disinformation in motion.

[38] Mathias Osmundsen et al, "Partisan Polarization is the Primary Psychological Motivation behind Political Fake News Sharing on Twitter," *American Political Science Review* 115, no 3, (2021): 1-17.

❖ **Recommendation 5: Teach Information Consumers about the cognitive and emotional impact of social media and online information**



Edelman Trust Barometer 2021.

4. Media Literacy and Critical Thinking Skills

Media literacy is the application of critical thinking skills to forms of information, whether print newspapers and magazines, along with their online counterparts, broadcasts on television and radio, online video or podcasts, and on social media platforms or messaging apps. Media literacy efforts typically involve training information consumers how to differentiate fact from opinion, how to assess sources of information, and how information can be manipulated to deceive the audience. Research suggests

that media literacy efforts can assist information consumers to distinguish real news from fake news.[39]

Other approaches include helping information consumers understand the cognitive and mental health impact of using social media and other digital sources of information and helping them negotiate the many hazards found online.[40] One researcher maintains that media literacy efforts should encompass not only traditional forms of media, but also the information that passes through their networks of online connections.[41] Using this approach, information consumers can more clearly appreciate their own roles in the dissemination of disinformation. An article, video, podcast, or photograph shared, a retweet, a like, a comment, a post to a listserv, all may have more impact than an individual might foresee.

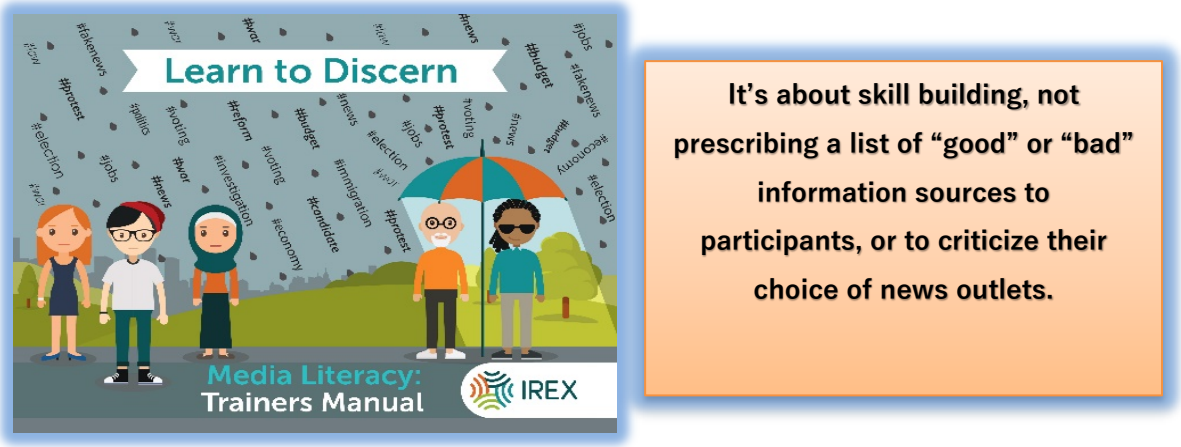


Figure 22 IREX Media Literacy Training Manual.

[39] Andrew Guess et al., "A digital media intervention increases discernment between mainstream and false news in the United States and India", PDF file, PNAS Vol. 117, no.27 (2020): 15536-15545. https://www.pnas.org/content/pnas/117/27/15536.full.pdf (accessed August 24, 2021).
[40] Amy Callahan, "Media Literacy Isn't Coming to Save Us (But We Can Make It Better)", *EdW*, last modified January 23, 2019, https://www.edweek.org/teaching-learning/opinion-media-literacy-isnt-coming-to-save-us-but-we-can-make-it-better/2019/01 (accessed August 24, 2021).
[41] Dana Boyd, "You Think You Want Media Literacy…Do You?," *Points: Data & Society*, last modified March 9, 2018, https://points.datasociety.net/you-think-you-want-media-literacy-do-you-7cad6af18ec2 (accessed August 24, 2021).

Educational institutions and non-governmental organizations provide resources on media literacy for use in formal and information educational settings, and self-paced learning. In 2019, the Digital Citizenship and Media Literacy Act was introduced in the U.S. Senate to assist with nationwide efforts, including the study of best practices in media literacy programs.[42]

Research indicates that many information consumers are not able to articulate the criteria by which they evaluate the trustworthiness of information and therefore are unable consistently to distinguish real news from fake news.[43] The development of critical thinking skills can help information consumers recognize faulty reasoning, weakly-

Figure 23 Critical Thinking Diagram (obtained from Tycoonstory).

[42] A Bill to promote digital citizenship and media literacy, S. 2240, 116th Congress, 1st Session. (2019).
[43] Blanca Puig, Paloma Blanco-Anaya, and Jorge J. Pérez-Maciera, "'Fake News' or Real Science? Critical Thinking to Assess Information on COVID-19", *Frontiers in Education*, last modified May 3, 2021, https://www.frontiersin.org/articles/10.3389/feduc.2021.646909/full (accessed August 24, 2021).

supported arguments, and disinformation. Teaching critical thinking skills as a separate course, as well as incorporating the application of critical thinking in all courses, leads to better outcomes than not providing a course focused exclusively on the teaching of critical thinking skills.[44] We encourage the development of critical thinking skills in both formal and informal educational settings.

❖ Recommendation 6: Teach Media Literacy and Critical Thinking Skills

We also suggest information consumers to utilize the SMART mnemonic and practices. Based on Aesop's The Tortoise and the Hare, the SMART graphic on the next page illustrates the need to take time to reflect on information to verify its truthfulness before dissemination to others. Proceeding slowly, but prudently, before acting on information is preferable to proceeding rapidly, but carelessly. The tortoise bypasses the hurdles that impede the search for the facts. Meanwhile, the hare falls headlong into the traps set by those who promote disinformation.

[44] Shane Horn and Koen Veermans, "Critical Thinking efficacy and transfer skills defend against 'fake news' at an international school in Finland," *Journal of Research in International Education*, 18, no. 1 (2019): 23-41. https://doi.org/10.1177%2F1475240919830003 (accessed August 24, 2021).

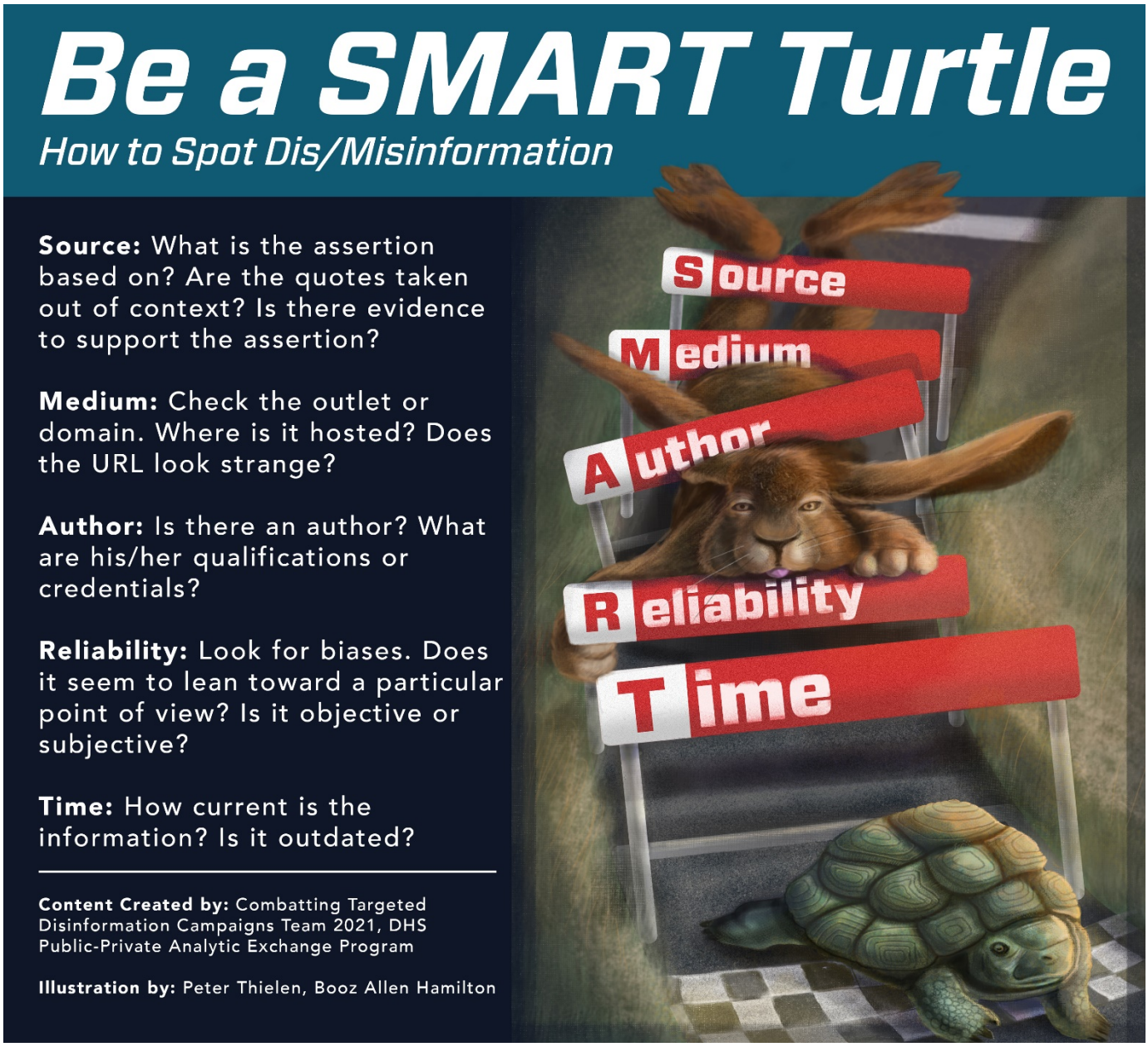


Figure 24 SMART Graphic | Source: Combatting Targeted Disinformation Campaigns Team 2021

Conclusion

It is extremely improbable that disinformation campaigns will disappear in the foreseeable future. Despite the increasing effectiveness of countermeasures, threat actors will always find avenues to spread their disinformation and will adopt new tactics as new forms of technology emerge. Compared to many legitimate forms of persuasion and influence, disinformation campaigns are inexpensive and frequently have few downsides for the threat actor. Threat actors take ready advantage of software and communication platforms that they did not develop and benefit from political and social conditions that they did not create.

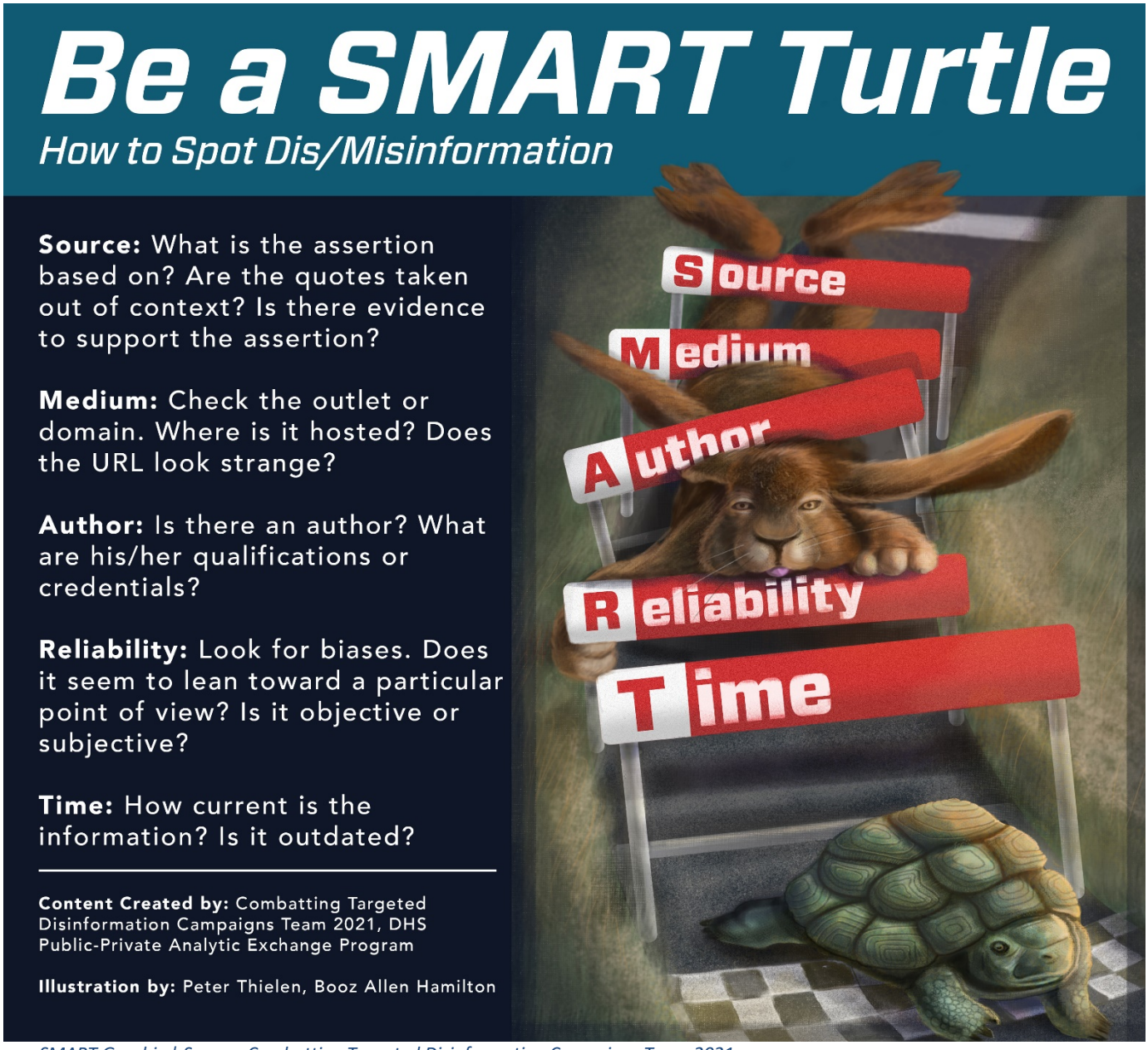
In this report, we concluded that disinformation campaigns are threats to national security because they undermine the well-being of our society. Though disinformation campaigns cannot be stopped fully, we believe that measures can be taken to impede these campaigns and reduce their impact. We believe that building the resilience of information consumers to disinformation will likely bear more fruit than focusing on technological solutions. To build such resilience, we believe that giving information consumers more tools with which they can verify the information they consume online, identify the threat actors behind disinformation campaigns, verify the claims of imposters hiding behind fake persona and credentials, and control their content feeds is essential.

The factors which make information consumers vulnerable to disinformation are rooted in human psychology, the divisions within our society, and the siloed nature of today's information ecosystem. As illustrated in the Disinformation Kill Chain, one result of

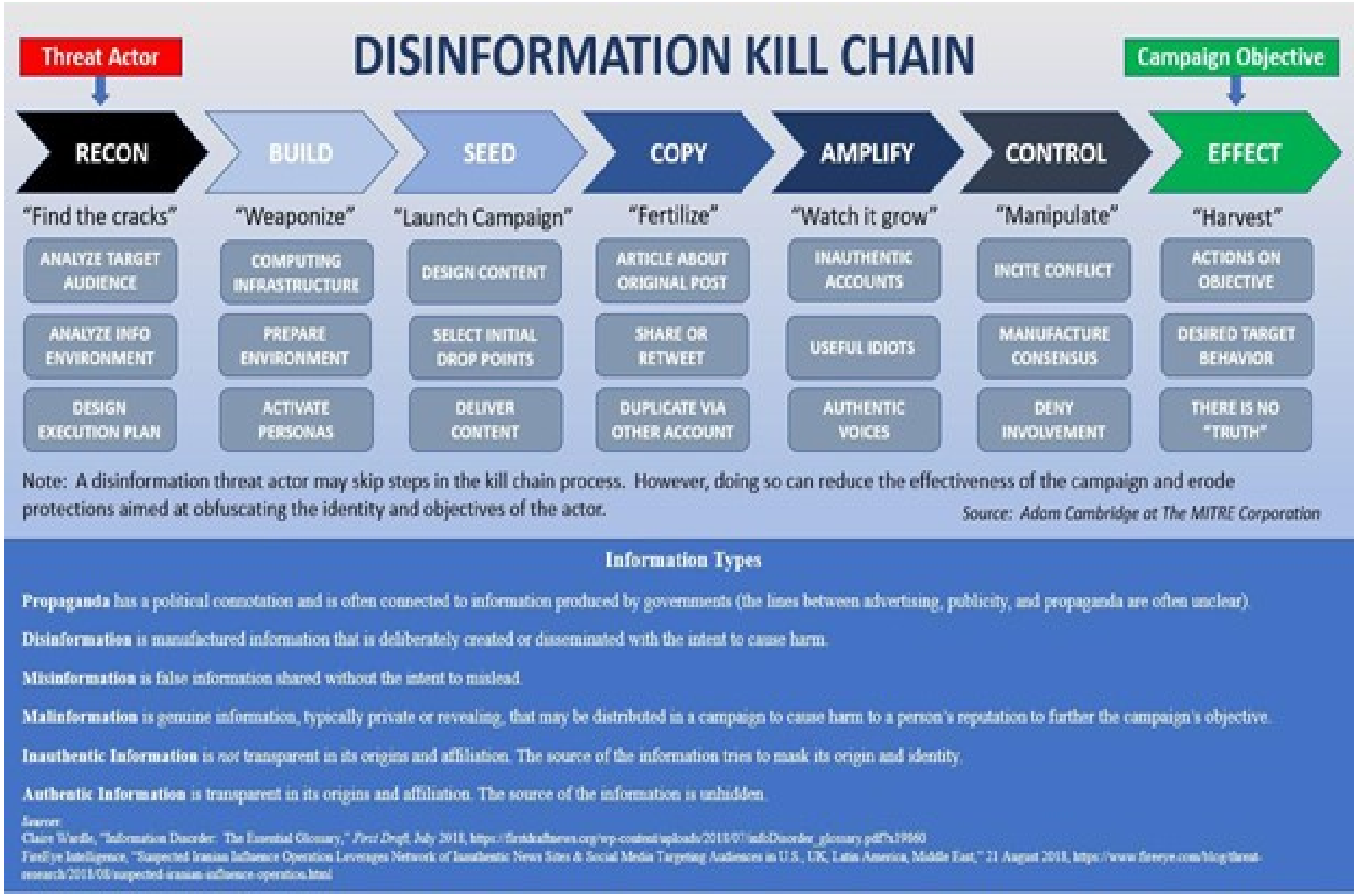
disinformation campaigns is that information consumers end up believing that truth no longer exists. Such a result demonstrates that supply and demand form a positive feedback loop. When information consumers lose the ability to distinguish fact from fiction, and become uninterested in doing so, demand for disinformation grows, which drives the supply of disinformation.

The prevalence of disinformation campaigns in our society is emblematic of the polarization of our society. Such polarization hampers a united response and even the ability to come to a common understanding of what a fact is, and what disinformation or misinformation are. Individual information consumers can build up their immunity to disinformation. But our society, as a whole, will not be able to build up its resilience until the larger problems that recent events have exposed are dealt with first.

Exhibits



SMART Graphic | Source: Combatting Targeted Disinformation Campaigns Team 2021.



Source: The MITRE Corporation.

DISCLAIMER STATEMENT: This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.

RAND ARROYO CENTER

Recent events in Crimea and the Donbass in eastern Ukraine have upended relations between Russia and the West, specifically the North Atlantic Treaty Organization (NATO) and the European Union (EU). Although Russia's actions in Ukraine were, for the most part, acts of outright aggression, Russia has been aiming to destabilize both its "near abroad"—the former Soviet states except for the Baltics—and wider Europe through the use of ambiguous "gray zone" tactics. These tactics include everything from propaganda and disinformation to election interference and the incitement of violence.

To better understand where there are vulnerabilities to Russian gray zone tactics in Europe and how to effectively counter them, the RAND Corporation ran a series of war games. These games comprised a Russian (Red) team, which was tasked with expanding its influence and undermining NATO unity, competing against a European (Green) team and a U.S. (Blue) team, which were aiming to defend their allies from Red's gray zone activities without provoking an outright war. In these games, the authors of this report observed patterns of behavior from the three teams that are broadly consistent with what has been observed in the real world. This report presents key insights from these games and from the research effort that informed them.

$19.00

ISBN-10 1-9774-0402-2
ISBN-13 978-1-9774-0402-2
51900
9 781977 404022

www.rand.org

RR-2791-A

Competing in the Gray Zone: DRussian Tactics and Western Responses

PETTYJOHN AND WASSER

RAND

RAND CORPORATION

STACIE L. PETTYJOHN, BECCA WASSER

Competing in the Gray Zone

Russian Tactics and Western Responses

Competing in the Gray Zone

Russian Tactics and Western Responses

STACIE L. PETTYJOHN, BECCA WASSER

Prepared for the United States Army
Approved for public release; distribution unlimited

RAND ARROYO CENTER

For more information on this publication, visit www.rand.org/t/RR2791

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-1-9774-0402-2

Published by the RAND Corporation, Santa Monica, Calif.
© Copyright 2019 RAND Corporation
RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Support RAND
Make a tax-deductible charitable contribution at
www.rand.org/giving/contribute

www.rand.org

Preface

This report documents research and analysis conducted as part of a project entitled *Gray Zone War Games*, sponsored by the Office of the Deputy Chief of Staff, G-3/5/7, U.S. Army. The purpose of the project was to develop an interrelated series of expert input, tabletop, and computer-assisted war games to simulate "gray zone" activities, or measures short of war, to support analysis of strategic and operational threats and opportunities, to inform indications and warning processes, and to support U.S., UK, and other NATO strategies and force development plans.

This research was conducted within RAND Arroyo Center's Strategy, Doctrine, and Resources Program. RAND Arroyo Center, part of the RAND Corporation, is a federally funded research and development center sponsored by the United States Army.

RAND operates under a "Federal-Wide Assurance" (FWA00003425) and complies with the *Code of Federal Regulations for the Protection of Human Subjects Under United States Law* (45 CFR 46), also known as "the Common Rule," as well as with the implementation guidance set forth in DoD Instruction 3216.02. As applicable, this compliance includes reviews and approvals by RAND's Institutional Review Board (the Human Subjects Protection Committee) and by the U.S. Army. The views of sources utilized in this study are solely their own and do not represent the official policy or position of DoD or the U.S. Government.

Page 344 of 3957

Contents

Preface iii
Figures and Table vii
Summary ix
Acknowledgments xiii
Abbreviations xv

CHAPTER ONE
Introduction 1

CHAPTER TWO
Methodology 5
Designing the Games 6

CHAPTER THREE
The Gray Zone Is More Usefully Conceptualized as a Type of Tactic, Rather Than an Operational Environment 9

CHAPTER FOUR
"Everyday" Gray Zone Actions Must Be Differentiated from More Aggressive, Focused Gray Zone Actions 21

CHAPTER FIVE
NATO and the EU Are Unlikely to Be Able to Compel Russia to Stop Using Nonviolent, Everyday Russian Gray Zone Tactics, but They Might Be Able to Deter Higher-Order Aggression 31

Page 346 of 3957

Page 347 of 3957

CHAPTER SIX
Vulnerability to Russian Gray Zone Tactics Varies Significantly Across Europe 35

CHAPTER SEVEN
Civilian Organizations, Rather Than the Military, Might Be Best Positioned to Counter Most Russian Gray Zone Tactics 43

CHAPTER EIGHT
The West Might Be Winning This Competition, but Does Not Recognize It 45

APPENDIX
Wargaming the Gray Zone 49

References 53

Page 347 of 3957

Figures and Table

Figures

2.1. Gray Zone Game Design Process 8
4.1. Types and Examples of Gray Zone Tactics 22
6.1. Intra-European Vulnerability to Russian Gray Zone Tactics ... 37
A.1. Gray Zone Timeline Board 51
A.2. Main Gray Zone Game Board 51

Table

3.1. Russian Gray Zone Tactics 14

Page 348 of 3957

Summary

Russia's 2014 offensives in the disputed regions of Crimea and the Donbass in Ukraine present a different challenge—an undeclared form of warfare that relied on a mixture of conventional and unconventional tools—from the one that the North Atlantic Treaty Organization (NATO) had prepared for during the Cold War. There have been many terms used to describe these unconventional Russian campaigns, including "gray zone conflict." This study was tasked with examining the "gray zone" in Europe, which is the expression we will use. We define gray zone tactics as *ambiguous* political, economic, informational, or military actions that primarily target domestic or international public opinion and are employed to advance a *revisionist* nation's interests without provoking outright war.

To better understand where there are vulnerabilities to these types of tactics and how to effectively counter them, we ran a series of war games to explore the issue of Russian gray zone aggression in Europe. These games comprised a Russian (Red) team, which was tasked with expanding its influence and undermining NATO unity, competing against a European (Green) team and a U.S. (Blue) team, which were aiming to defend their allies from Red's gray zone activities without provoking an outright war. In our games, we observed patterns of behavior from the three teams that are broadly consistent with what we have observed in the real world. This report presents the following key insights from these games and from the research effort that informed them:

Page 350 of 3957

- "Everyday" gray zone actions must be differentiated from more aggressive and focused gray zone actions. There are two variables, the target of the action and whether it involves outright violence or the threat of violence, that are important for understanding Russian gray zone tactics, because they imply different time horizons, objectives, and stakes. Many of the unconventional tactics that Russia uses to try to gain influence are routine, diffuse, and long-term, although others have very specific, short-term objectives. Russian gray zone tactics might also be nonviolent (e.g., propaganda and disinformation) or involve outright violence or the threat of violence (e.g., a planned coup in Montenegro).
- Based on the war games conducted to support this project, we observed that NATO and the European Union (EU) are unlikely to be able to compel Russia to stop using nonviolent Russian gray zone tactics, but they might be able to deter high-order aggression. There is much talk about "deterring" Russian gray zone aggression, but many of these discussions are based on a misunderstanding of the concept. Because Russia is already engaging in steady-state gray zone actions, NATO and the EU need to compel Russia to stop these activities, which is a much harder task than deterrence. Moreover, the characteristics of everyday gray zone tactics—they are largely nonmilitary, usually gradual, and difficult to decisively attribute—lower the stakes and make it difficult for the West to credibly threaten to punish Russia, even if the actions are conclusively traced back to Moscow. Outright Russian aggression with the aim of territorial expansion is an entirely different situation, and one that can be deterred by conventional means.
- Vulnerability to Russian gray zone tactics varies significantly across Europe. Russia's "near abroad"—defined as the countries around its border—is the most vulnerable region, followed by the Balkans. This is largely because of those countries' weak governmental institutions and historic, cultural, and linguistic ties to Russia. By contrast, the Baltic states are less susceptible to gray zone tactics because of their relatively good governance. Finally,

Western and Central Europe are least vulnerable to Russian gray zone actions.

- Civil organizations, rather than militaries, might be best positioned to counter Russian gray zone tactics. The vast majority of Russian gray zone tactics are not geared toward territorial gains, but instead are routine actions that seek to enhance Russia's influence through nonmilitary means. In short, this is primarily a social, political, and economic fight, not a military one, that is better waged by civilian agencies and nongovernmental organizations whose core competencies lay in these domains. The military plays an important but limited role in countering Russian gray zone activities by improving cyber defenses, enhancing intelligence and counterintelligence capabilities, and building partner special forces capacity.
- Our research suggests that the West is winning this competition but does not recognize it. Some seem to believe that, because the West cannot stop Russia from using everyday gray zone activities, it is therefore somehow losing, but this neglects the larger strategic situation. Russia's gray zone tactics will persist and should be countered by hardening Western societies against propaganda and attempts to undermine democracy. However, overreaction only serves Moscow's purposes. Strong civil societies and robust democratic institutions, rather than panic at "losing" or attempts to fight Russia blow-by-blow, are the West's best defenses against Russia's gray zone tactics. Russia's gray zone tactics signify its weakness, and the West's stronger political, cultural, and social systems will prevail over them if given the chance.

Acknowledgments

The authors would like to thank MG William Hix for the opportunity to examine an important question and MAJ Robert Kurtts for his guidance of the project. Our report was strengthened by reviews from Dara Massicot of the RAND Corporation and Michael Kofman of CNA, and we thank them for their helpful comments. We also thank the Latvian Ministry of Defense, Latvian President's Office, NATO Stratcom Centre of Excellence, Centre for East European Policy Studies, International Centre for Defence and Security, Estonian Ministry of Foreign Affairs, and Estonian National Security and Defence Coordination Unit for sharing with us their views of Russian gray zone tactics and European countermeasures.

At RAND, we thank our colleagues Jenny Oberholtzer, William Mackenzie, Stephanie Pezard, David Frelinger, David Shlapak, and Ben Connable for helping to develop and run the games, and Sally Sleeper and Jennifer Kavanagh for their guidance of the project. We also thank the players in the multiple games that we conducted at RAND for their participation and valuable insights.

Page 354 of 3957

Abbreviations

DDOS	distributed denial of service
DF	(Montenegrin) Democratic Front party
EU	European Union
FSB	Federal Security Service (Russia)
GRU	Main Directorate of the General Staff of the Russian Federation
MNA	Hungarian National Front
NATO	North Atlantic Treaty Organization
NGO	nongovernmental organization
RS	Republic of Srspka
SME	subject-matter expert

CHAPTER ONE

Introduction

In 2014, Russia's bloodless annexation of the Crimean Peninsula and its support of a separatist uprising in eastern Ukraine shattered the notion that Europe was peaceful and secure. It became clear that Russian President Vladimir Putin would use force to maintain Russia's influence in its "near abroad"—the former Soviet states except the Baltics—to undermine the North Atlantic Treaty Organization (NATO), divide Europe, and reduce U.S. dominance of the international order. Consequently, for the first time in several decades, NATO began to seriously grapple with how to deter and defeat aggression in its backyard. However, Russia's 2014 offensives seemed to present a different challenge—a covert form of warfare that relied on a mixture of conventional and unconventional tools—from the one that NATO had prepared for during the Cold War, one which the alliance was ill-prepared to counter. The Russian government did not officially acknowledge its offensives in Ukraine, which were characterized by the use of proxies, unmarked forces, disinformation, and cyberattacks, along with the use of conventional military forces. Together, these tactics were intended to create confusion and delay a response, allowing enough time for Russia to achieve its objective, thereby forcing its opponents to escalate the situation and mount an offensive to regain the lost territory. These tactics succeeded in paralyzing the Ukrainian government and multilateral European institutions during the Crimea operation, but did not achieve a commensurate level of success in eastern Ukraine because separatist operations in the Donbass (commonly defined as the Luhansk and Donetsk regions of Ukraine) were bogged down in a

Page 358 of 3957

Page 359 of 3957

bloody, inconclusive conflict with the Ukranian government. Although Russian conventional forces played decisive roles in both operations, many observers have focused on the unconventional tools that Russia used to mask the true nature of its actions and to bolster their efficacy. Russia has employed similar techniques—in particular the use of cyberattacks, propaganda, proxy forces, and disinformation—to try to create strife or to influence elections in Western democracies.

There have been many terms used to describe these unconventional Russian actions, including "gray zone conflict," "hybrid warfare," "nonlinear warfare," "ambiguous warfare," "indirect action," "asymmetric," and "political warfare."[1] We are not going to delve into the debates about the coherence or utility of these various terms.[2] Rather, this study was tasked with examining the gray zone in Europe,

---

[1] Joseph L. Votel, "Statement of General Joseph L. Votel, U.S. Army Commander, United States Special Operations Command Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities," March 18, 2015, p. 7; Van Jackson, "Tactics of Strategic Competition: Gray Zones, Redlines, and Conflicts Before War," *Naval War College Review*, Vol. 70, No. 3, Summer 2017; Mary E. Connell and Ryan Evans, *Russia's 'Ambiguous Warfare' and Implications for the U.S. Marine Corps*, Arlington, Va.: CNA, May 2015; Frank Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," in Dakota L. Wood, ed., *2016 Index of Military Strength: Assessing America's Ability to Provide for the Common Defense*, Washington, D.C.: Heritage Foundation, 2015; Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses*, Santa Monica, Calif.: RAND Corporation, RR-1577-AF, 2017; Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, blog post, July 6, 2014; Fletcher Schoen and Christopher Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Washington, D.C.: Institute for National Strategic Studies, June 2012, pp. 8–9; Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Carlisle, Pa.: Strategic Studies Institute and U.S. Army War College Press, December 2015.

[2] Adam Elkus, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense," *War on the Rocks*, December 15, 2015; Hal Brands, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, February 5, 2016; Hoffman, 2015; Nadia Schadlow, "The Problem with Hybrid Warfare," *War on the Rocks,* April 2, 2015; Frank Hoffman, "On Not-So-New Warfare: Political Warfare vs Hybrid Threats," *War on the Rocks,* July 28, 2014; Merle Maigre, *Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO*, German Marshall Fund of the United States, February 2015; Kristen Ven Bruusgaard, "Crimea and Russia's Strategic Overhaul," *Parameters*, Vol. 44, No. 3, Autumn 2014, p. 81; Mark Galeotti, "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's New Way of War?" *Small Wars and Insurgencies*, Vol. 27, No. 2, 2016.

Page 359 of 3957

Page 360 of 3957

which is the expression that we will use. We define *gray zone tactics* as ambiguous political, economic, informational, or military actions that primarily target domestic or international public opinion and are employed to advance a nation's interests while still aiming to avoid retaliation, escalation, or third-party intervention.[3]

The purpose of this report is to document the findings from a study of Russian gray zone tactics that included a series of war games along with in-depth research on the topic. Both forms of analysis contributed to the insights discussed later in this chapter.[4] The remainder of the report is organized as follows. Chapter Two details the methodology employed in this study. It is followed by chapters reporting the study's main insights, which include a framework to better understand Russian gray zone tactics. Finally, there is an appendix that provides more information about the war games.

---

[3] Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats,* Stockholm: Swedish Defence University, European Center of Excellence for Countering Hybrid Threats, May 9, 2018, p. 10; Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs*, Vol. 92, No. 1, 2016, pp. 178–179; Radin, 2017, p. 5; Christopher S. Chivvis, *Understanding Russian 'Hybrid Warfare' and What Can Be Done About It: Addendum*, testimony before the U.S. House of Representatives Armed Services Committee, Washington, D.C., March 22, 2017, p. 2.

[4] The interaction between the war games and research is discussed further in the methodology chapter.

Page 360 of 3957

CHAPTER TWO

Methodology

To study the dynamics of Russia's gray zone activities, we employed two methodologies in an iterative way. Our aim was to develop a framework that could be used to understand the variety of different Russian gray zone tactics in Europe and also to inform U.S. strategic planning. To develop this framework, we combined extensive historical research and a review of relevant literature (including strategic documents, interviews, and analysis by other scholars) with a series of war games intended to both inform the ongoing research and further test emerging insights.[1] The process was iterative in that we conducted both tasks simultaneously, with the research informing the games and the games informing the research. Both activities contributed equally to the final framework and key insights presented in this report.

The gaming and research efforts were integrated in several ways. We began by researching Russia's gray zone activities, but also began running open-ended and loosely structured games with expert players. These initial games helped us gain a better understanding of the nature of the competition and focused us on particular aspects of the problem that appeared most challenging to the United States and European partners. In other words, the early games were valuable in guiding our research, pointing us toward key questions—such as whether Russia's choice to employ certain types of gray zone tactics is dependent on location, timing, and context—and insights that warranted additional investigation, such as the dominant role of civilian organizations in

[1] We ran a matrix gray zone game three times, a semistructured gray zone game twice, and a structured gray zone game twice.

Page 362 of 3957

Page 363 of 3957

combatting Russian gray zone tactics. At times, the games pointed us toward interesting observations that we then investigated further through research, including in interviews with subject-matter experts (SMEs) and government officials in Europe. Although players occasionally made important decisions during game play, it was mostly the postgame deliberations where we collectively considered the pros and cons of various strategies, and the competition more broadly, that led us to new insights that are expounded on throughout this report. In the later stages of the research effort, semistructured and structured games also served as a platform for testing various hypotheses and insights. Again, although player moves and game outcomes were interesting, postgame discussions with players and research team members were equally important. In several cases, after testing a hypothesis in a game, we conducted additional research to refine or improve our understanding of key dynamics.[2]

The framework and insights presented in this report are a synthesis of our research and observations made during the games and postgame discussions. The report does not describe specific moves made by the players during these games or the outcomes of the games, which could be misleading, but instead focuses exclusively on the insights that emerged from our broader cycle of gaming and research.

Designing the Games

As mentioned previously, we developed and ran several types of games. The first gray zone games were matrix games that were largely free-form exercises where the players made arguments that were judged by umpires about what they could do and to what effect.[3] We then devel-

[2] An example of a hypothesis we tested in one of the structured games: Russia seeks to actively halt NATO enlargement in the Balkans.

[3] There are three types of strategy games discussed in this report: free-form games, matrix games, and structured games. Free-form games (also known as seminar-style games) have few rules or physical elements, and game outcomes are determined by expert adjudicators in an ad-hoc way. Matrix games are a specific type of argumentation-based free-form game, where the teams present reasons why they could or their adversary could not do something,

Page 363 of 3957

Page 364 of 3957

oped a semistructured game that provided the players with a menu of options, pieces, a board, and a partially specified set of adjudication rules. Finally, we constructed a fully structured game with detailed rules that guided what the players could do and the effect of their actions.[4] Our gray zone games were intended to serve as vehicles for the players to develop coherent strategies, explore the pros and cons of different decisions, and to have a robust discussion that helped them to identify which strategies are most likely to be effective in different situations and which strategies appear the most robust against a variety of possible futures.

All of our gray zone games comprised a Russian (Red) team, tasked with expanding its influence and undermining NATO unity, competing against a European (Green) team and a U.S. (Blue) team, aiming to defend their allies from Russia's gray zone activities without provoking an outright war.[5] The players in our games were RAND Corporation experts on Russian, European, and U.S. defense and intelligence policy, and they role-played the appropriate country which aligned with their expertise.

Creating these games was an iterative process that involved extensive research on the concept of the gray zone, Russia's unconventional tactics, counteractions to Russian measures, and their effectiveness (see Figure 2.1). In the course of our research, we consulted a wide variety of sources on Russia's gray zone tactics, including journal articles, think tank studies, government reports, and periodicals. We used this

---

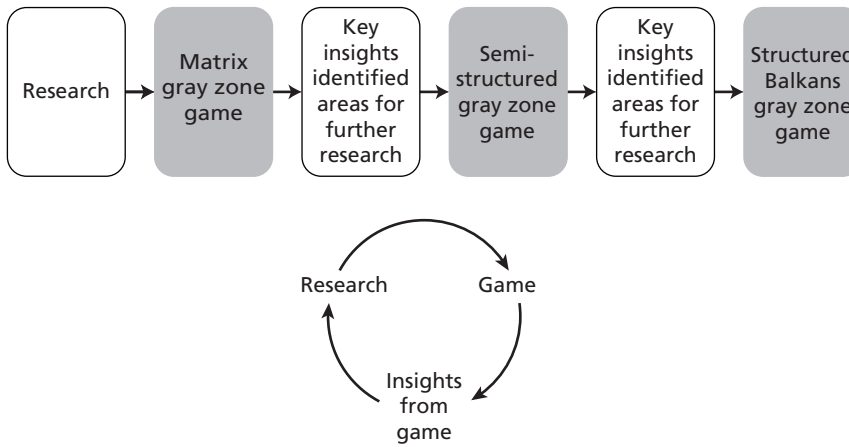
and then an adjudicator or umpire makes a final determination based on the net quality of the argumentation for and against an action. Structured games typically represent the phenomena with physical elements (e.g., cards and blocks) and have rules that determine game outcomes. For more on these see Becca Wasser, Jenny Oberholtzer, Stacie L. Pettyjohn, and William Mackenzie, *Gaming the Gray Zone: Observations from Designing a Structured Gray Zone Strategy Game*, Santa Monica, Calif.: RAND Corporation, RR-2915-A, 2019.

[4] John Curry and Tim Price, *Matrix Games for Modern Wargaming: Developments in Professional and Educational Wargames Innovations in Wargaming*, Vol. 2, Barking, UK: Lulu Press, Inc., August 2014; Warren Wiggins, *War Game Adjudication: Adjudication Styles*, Newport, R.I.: United States Naval War College, 2014.

[5] We follow the traditional wargaming practice of calling the U.S. team the "Blue team," U.S. allies the "Green team," and the adversary—in this instance, Russia—the "Red team."

Page 364 of 3957

Figure 2.1
Gray Zone Game Design Process



research to develop simple adjudication rule sets for the games; these rule sets distilled the existing empirical literature on individual gray zone tactics and countermeasures into a set of probability curves represented as a combat results table. These rules captured the central causal relationships of different phenomena but were simple enough that they allowed for relatively quick adjudication so that the game could be played in the course of a day. We do not claim that the rules or the underlying relationships are "correct;" rather, they are consistent with the literature and the understanding of these phenomena of the experts who played in our games, and offer a standard baseline for determining game outcomes.[6] A companion report, *Gaming the Gray Zone: Observations from Designing a Structured Gray Zone Strategy Game*, discusses the game design at greater length.

[6] In the structured Balkans gray zone game, game rules were printed on cards and therefore accessible to the players, who could understand what drove outcomes. The players could then argue with the adjudicators if they believed that the rules were wrong. When the adjudicator agreed that the rules did not accurately capture a dynamic in the game, they were modified in real time and the change was noted and incorporated into future iterations of the game.

CHAPTER THREE

The Gray Zone Is More Usefully Conceptualized as a Type of Tactic, Rather Than an Operational Environment

Because there is no commonly accepted definition of the "gray zone," we began by surveying the existing literature and cataloging different definitions, and then used our early games to crystalize our own thinking about the concept. Although many conceive of the gray zone as a phase of conflict, our postgame conversations led us to recast it as a type of tactic. Identifying the *gray zone* as a tactic—rather than a type of conflict or operating environment—is a new approach, but one that has greater analytic coherence and is more useful for crafting civilian and military strategies to counter gray zone activities.

Generally, there was agreement, both among game participants and during interviews conducted as part of the broader research project, that *ambiguity* is the defining characteristic of gray zone activities.[1] There might be ambiguity about who is responsible for the actions, as was the case initially in Crimea and the Donbass; ambiguity about the legality or veracity of the claims made, as is true for much of Russia's propaganda; or ambiguity about Russia's true aims, as is true with the unstated purpose of Russia's promotion of its culture and heritage.[2] Employed in the absence of conventional war, gray zone tactics are a

[1] David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone,'" *War on the Rocks,* May 19, 2015; Brands, 2016.

[2] Christopher Paul and Miriam Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It,* Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016.

Page 366 of 3957

Page 367 of 3957

covert subset of political warfare, which was defined by George Kennan as "employment of all the means at a nation's command, short of war, to achieve its national objectives."[3] Gray zone tactics exist beyond the realm of traditional statecraft and intelligence activities, but stop short of the use of conventional military power—although as *tactics*, they might still be employed even after a conflict has escalated to the conventional level, as we have seen in Ukraine, and just as propaganda and guerrilla warfare were elements of World War II.[4]

The murky nature of gray zone tactics is often identified as critical to their success because it prevents their target from quickly recognizing the threat or from rapidly gaining support from equally undecided external actors and institutions, reducing the likelihoods of rapid retaliation or escalation. This is particularly a concern for a large multilateral organization, such as NATO, where all members of the alliance need to agree to activate the collective security clause embodied in Article V, which in turn requires them to assist the party under attack.[5] Nevertheless, the veil of deniability is often quite thin, especially when Russia has employed belligerent and militarized gray zone tactics and trained observers were able to quickly see through it as was the case of the Russian invasion of the Donbass.[6]

We focus on gray zone *tactics* versus the gray zone as a distinct type or sphere of conflict. Many others conceptualize the gray zone as a separate form of warfare that falls somewhere in the middle of a spectrum between peace and conventional war.[7] This is in line with

---

[3] Overt political warfare or other white measures short of war are not a form of gray zone tactics. George Kennan, "George F. Kennan on Organizing Political Warfare [Redacted Version]," Wilson Center Digital Archive, April 30, 1948.

[4] Some, such as Mazarr and Lanoszka, define gray zone tactics as something only revisionist states—those that seek to alter the status quo—use, but in fact one could argue that covert actions, which the United States and other countries employ and have used extensively in the past, are a gray zone tactic.

[5] Mazarr, 2015, p. 39.

[6] Andrew Roth, "From Russia, 'Tourists' Stir the Protests," *New York Times,* March 3, 2014b; Andrew Higgins, Michael R. Gordon, and Andrew Kramer, "Photos Link Masked Men in East Ukraine to Russia," *New York Times*, April 20, 2014.

[7] Hoffman, 2015, p. 26; U.S. Special Operations Command, *The Gray Zone*, September 9, 2015, p. 1.

Page 367 of 3957

Page 368 of 3957

the U.S. military's linear phasing construct for operational plans, but has contributed to conceptual muddling because it is not clear whether there are really boundaries between the phases. At the same time, it is clear that Russia has used various forms of unconventional warfare in both peacetime and as an element of large conventional military operations.[8] The gray zone as a middling level of competition also lends support to Russia's narrative that it is not engaged in traditional aggression in such places as Georgia.[9] The conflict in the Donbass is also dominated by traditional combat with a smattering of gray zone activities that are intended to sow doubt about the true nature of the conflict.[10] It is extremely difficult to distinguish what falls in one phase versus another, and what phase a conflict is currently in, which in turn makes it difficult to identify the appropriate behavior that should follow. During their deliberations, the U.S. teams in our games struggled to determine what phase they were in at various points, and observed that the concept of the gray zone as a phase of competition was not only ambiguous and difficult to apply in practice, but also potentially inaccurate and misleading. Therefore, it is both intellectually more coherent and, for the policymaker, more operationally useful to conceptualize gray zone activities as a type of tactic rather than a unique form of conflict or operating environment.[11] Seen this way, it is clear that gray zone *tactics* might be the only or primary approach employed, or they might simply be a supplement to more-traditional warfare.

---

[8] For more on the problems that this type of phased thinking creates for gray zone competition see: Paul Scharre, "American Strategy and the Six Phases of Grief," *War on the Rocks,* October 6, 2016.

[9] Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications*, Carlisle: Pa.: Strategic Studies Institute, June 2011.

[10] Michael Kofman and Matthew Rojansky, "A Closer Look at Russia's 'Hybrid War,'" *Kennan Cable,* No. 7, April 2015; Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016; Andras Racz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, FIIA Report 43, Helsinki, Finland: Finnish Institute of International Affairs, 2015, p. 14.

[11] This is similar to how Mazaar (2015) uses the term, p. 58. Jackson (2017) argues that it is better to look at revisionist tactics, in particular avoiding redlines, using intermediaries, and presenting a *fait accompli*.

Page 368 of 3957

Page 369 of 3957

It is also important to mention that gray zone or hybrid tactics are a Western concept and not used by Russian strategists to refer to their own actions. Writing that is often associated with Russia's hybrid strategy, such as those articles written by Russian chief of the General Staff General Valery Gerasimov, is actually describing a Western campaign of indirect action that is being waged against Russia using nonkinetic tools.[12] In the views of such authors, the West uses indirect actions to undermine unfriendly governments, which is what these authors believe happened in Ukraine.[13] This is not a radically new way of thinking about war for the Russians because the Soviet Union extensively engaged in active measures during the Cold War. Additionally, the Russian general staff has been studying asymmetry in modern conflicts for nearly 20 years.[14]

Are Gray Zone Tactics New?

Although the phrase *gray zone* is relatively new, the types of actions that it describes are not.[15] Some recently employed Russian gray zone tactics include the use of traditional and social media to spread propaganda and disinformation; cyberattacks against government communications and critical civilian infrastructure; efforts to surreptitiously buy up large stakes in key economic sectors in foreign countries or to

---

[12] See, for example, Valery Gerasimov, "Znacheniye nauki nakhoditsya v predvidenii: novyye vyzovy trebuyut pereosmysleniya form i metodov vedeniya boyevykh deystviy [The Value of Science Is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations]," *Voyenno-Promyshlennyy Kuryer [Military Courier]*, February 26, 2013; Vi Lutonvinov, "I ispol'zovanie nevoennykh razvitie mer dlia ukrepleniia voennoi bezopasnosti Rossiiskoi Federatsii [The Use of Nonmilitary Development Measures to Strengthen the Military Security of the Russian Federation]," *Voennaia mysl' [Military Thought]*, No. 5, May 2009; S. G. Chekinov, and S. A. Bogdanov, "Asimmetrichnyye mery po obespecheniyu voyennoy bezopasnosti Rossii [Asymmetrical Actions to Ensure Russia's Military Security]," *Voyennaya mysl' [Military Thought]*, Vol. 3, 2010.

[13] Samuel Charap, "The Ghost of Hybrid War," *Survival*, Vol. 57, No. 6, December 2015–January 2016, p. 51; Dmitry Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy*, Proliferation Papers, No. 54, IFRI Security Studies Center, November 2015, p. 20.

[14] Herbert Romerstein, "Disinformation as a KGB Weapon in the Cold War," *Journal of Intelligence History*, Vol. 1, No. 1, 2001; and Adamsky, 2015, p. 25.

[15] Brands, 2016.

Page 369 of 3957

Page 370 of 3957

coopt business elites; support for politicians or political parties, gangs, and paramilitaries; promotion of Russian, Slavic, or Orthodox culture; and the use of unmarked soldiers or "little green men." Table 3.1 provides an overview of major types of gray zone tactics employed by Russia and examples thereof. This list is not meant to be comprehensive, but instead is intended to provide a sense of the types and breadth of Russian gray zone tactics. Russia often employs multiple combinations of gray zone tactics together.

What has been new and surprising to the United States and its European allies is the idea that they are facing a Russia that is actively and aggressively trying to influence their domestic politics and weaken the Western institutions that have underpinned the post–Cold War international order through the employment of these tactics. NATO's newest members, especially the former members of the Soviet Union and Warsaw Pact (in addition to aspirant states) are thought to be likely targets and particularly vulnerable to Russian gray zone aggression. Despite this fact, many policymakers in Europe and especially in new member states believe that accession to NATO insulates them from violent gray zone tactics. Yet, the Red teams specifically chose new and aspirant NATO members to target in our games.[16] Recently, it has also become clear that Russia has sought to interfere, albeit in a much less overt way, in the politics of longstanding NATO members.[17] In response, NATO and the European Union (EU) have focused more attention and resources on challenging Russia's unconventional tactics and have taken several steps to counter this threat.

---

[16] Montenegro, in particular, was a consistent focus for the Russia teams in our games given its recent accession to NATO.

[17] United States Senate Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, minority staff report, Washington, D.C.: U.S. Government Publishing Office, January 10, 2018; Matt Burgess, "Here's the First Evidence Russia Used Twitter to Influence Brexit," *Wired*, November 10, 2017; Andy Greenberg, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure,'" *Wired,* May 9, 2017; Peter W. Singer, "What We Didn't Learn from Twitter's News Dump on Russiagate," *Defense One*, January 20, 2018.

Page 370 of 3957

Page 371 of 3957

Table 3.1
Russian Gray Zone Tactics

Gray Zone Tactics	Example
Religious and cultural influence	
• Promotion of Russian language and culture	• Establishment of Russian Centers in European states with ethnic Russian populations, funded by the Russkiy Mir Foundation[a]
• Expansion of Russian Orthodox Church	• The Kremlin financed the building of a Russian Orthodox Cathedral in Paris[b]
• Use Russian Orthodox Church to intervene in political issues	• The head of the Montenegrin Orthodox Church denounced Montenegro's decision to support the EU stance on Crimea[c]
• Passportization	• Intentional distribution of passports to ethnic Russians by Russian authorities in specific parts of foreign countries (e.g., Ukraine and Georgia)[d]
Propaganda and information operations	
• Disseminate propaganda through state-controlled news channels	• Crafted narrative in state media outlets that exaggerates impact of refugee crisis in Europe[e]
• Create local media outlets to promote pro-Russian messages	• Government-linked private Russian media conglomerates (e.g., Gazprom Media) broadcast popular channels with diverse programming (e.g., NTV Mir into the Baltics or the First Baltic Channel's local news program Latvian Time)[f]

Page 371 of 3957

Page 372 of 3957

Table 3.1—Continued

Gray Zone Tactics	Example
• False news and disinformation campaign	• Russian media report that NATO was planning to base nuclear weapons in Sweden as part of a broader campaign to discourage movement toward NATO[g]
• Amplify pro-Russian message with trolls and bots	• Russian trolls are used to spread disinformation in Ukraine online (e.g., denying that Russian forces are present)[h]
• Fund trolls and bots to take punitive actions against activists	• Disguised Internet Research Agency trolls and bots manipulate social media sites to get the accounts of Ukrainian activists suspended[i]
• Bribe or pressure journalists to influence content	• Paid Macedonian journalists to promote a common Slavic and Orthodox identity in their content[j]
Cyber operations	
• Hack sensitive or embarrassing information and provide to third parties to make public	• Macron campaign emails were hacked and given to WikiLeaks during the 2017 French presidential election[k]
• Disrupt online communications and commerce through distributed denial of service (DDOS) attacks	• Widespread DDOS attack against Estonian government, media, and financial institutions for two weeks in 2007[l]
• Boost pro-Russian narrative through malware attacks	• The Bedep Trojan Malware infected computers, forcing them to access a variety of pro-Russian content, artificially inflating the popularity of such content in searches[m]
• Disable or destroy infrastructure	• An explosion in Turkey damaged the Baku-Tbilisi-Ceyhan pipeline days before the Russian invasion of Georgia[n]

Page 372 of 3957

Table 3.1—Continued

Gray Zone Tactics	Example
• Disseminate destructive malware to disable governments and industries	• In June 2017, NotPetya malware hit Ukrainian financial, energy, and government institutions on the eve of a national holiday. The virus pretended to be ransomware, but this was deception because it actually aimed to delete and deny access to data and spread quickly to 64 countries[o]
Support for proxies	
• Provide financial support to nongovernmental organizations (NGOs) to further entrench ethnic and social cleavages	• Russian Ministry of Foreign Affairs has provided funding to the Latvian Human Rights Committee, which focuses on the Russian minority in Latvia[p]
• Develop and sustain ties to criminal networks to earn money, gain intelligence, and act as Russian agents	• Russian Federal Security Service (FSB) has ties to international criminal traffickers, including cigarette smugglers in Estonia; these ties allegedly led to the kidnapping of an Estonian intelligence officer who was investigating the illicit activity[q]
• Support paramilitaries and separatists	• In 2016, Russian military and intelligence helped to create the multinational Balkan Cossack Army, a militaristic pan-Slavic association, and tie it with the Night Wolves gang in Montenegro, which was later implicated in an attempted coup plot[r] • Russian Main Intelligence Directorate (GRU) ties with the Hungarian neo-Nazi group Hungarian National Front (MNA) dated back to 2012, and were revealed after an MNA leader murdered a policeman in 2016; the GRU participated in military style exercises with MNA[s]
• Provide financial support and publicity to political parties	• Russia funded the Euroskeptic and nationalist Alternative for Deutschland (AfD) party in Germany and provided positive coverage in Russian media before the 2017 elections[t]

Page 373 of 3957
Page 373 of 3957

Table 3.1—Continued

Gray Zone Tactics	Example
• Organize protests	• Russian diplomats reportedly worked with nationalists and the Orthodox church to help organize protests in the Greek town of Alexandroupolis against an agreement that ended the naming dispute over Macedonia[u]
Economic coercion	
• Secure controlling interest in critical economic sectors	• Russia's Sberbank purchased 40 percent of indebted Croatian food group Agrokor, becoming its largest shareholder[v]
• Disrupt energy flows or complicate access to energy supplies	• Russia raised gas prices for Ukraine by 80 percent in April 2014 because of an alleged export duty[w]
• Embargo goods under false pretenses	• Russian banned European pig meat, allegedly because of fears of African swine fever, during Maiden protests[x] • In 2006 and 2013, Russia banned Moldovan wine imports because of "sanitation concerns"[y]
Violent or military coercion	
• Unacknowledged military harassment	• Russian Su-24 fighters buzzed the USS *Porter* in February 2017, but Moscow denied that the incident occurred[z]
• Create and sustain frozen conflicts as a source of persistent instability	• Russia supported Transnistrian separatists with the 14th Russian Army in 1992 and then deployed "peacekeeping" forces, in addition to providing free gas and other subsidies to the breakaway Moldovan region[aa]
• Fuel civil war	• Russia provided arms, training, and direct military support to Ukrainian separatists fighting in eastern Ukraine during the 2014 conflict[bb]

Table 3.1—Continued

Gray Zone Tactics	Example
• Assassinate politicians, activists, journalists, and former officials opposed to Russian activities outside its borders	• A nerve agent was used to attempt to assassinate a former spy living in the UK in March 2018[cc]
• Attempt to oust uncooperative governments forcibly	• Russia backed a coup attempt to install a pro-Russian president in Montenegro to prevent NATO accession[dd]
• Intimidate or detain journalists	• Journalists in Ukraine were detained, harassed, and denied access by pro-Russian separatists in the Donbass[ee]
• Provide military cover to secession	• Russia supported a referendum on secession in Crimea that violated Ukraine's constitution and occurred under the cover of a Russian military occupation[ff]
• Creeping borders	• Russia incrementally shifts Georgia's internationally recognized border by moving the fence and FSB guards separating it from Russia in South Ossetia[gg]

[a] Russkiy Mir was established in 2007 by Vladimir Putin to promote Russian culture and language abroad. See map of Russia Centers, Russkiy Mir Foundation, "Russian Centers of the Russkiy Mir Foundation," webpage, undated.

[b] Andrew Higgins, "In Expanding Russian Influence, Faith Combines with Firepower," *New York Times*, September 13, 2016a.

[c] Francisco de Borja Lasheras, Vessela Tcherneva, and Fredrik Wesslau, *Return to Instability: How Migration and Great Power Politics Threaten the Western Balkans*, Brussels: European Council on Foreign Relations, European Council on Foreign Affairs, March 2016.

[d] Agnia Grigas, "How Soft Power Works: Russian Passportization and Compatriot Policies Paved Way for Crimean Annexation and War in Donbas," Atlantic Council, February 22, 2016.

[e] For other themes of Russian propaganda see Diana Kaljula and Ivo Juurvee, "Narratives About the Nordic-Baltic Countries Promoted by Russia," in *Russia's Footprint in the Nordic-Baltic Information Environment*, Report 2016/1027, Riga, Latvia: NATO Strategic Communications Centre of Excellence, January 2018, p. 61. An example of such an article is "Libya, Migrants & Karma: Europe's New Migration Policy Wrecks on North African Reality," *RT*, July 22, 2018.

Page 375 of 3957
Page 375 of 3957

Page 376 of 3957

Table 3.1—Continued

[f] Max Bergmann and Carolyn Kenney, *War By Other Means*, Washington, D.C.: Center for American Progress, June 6, 2017; Vera Zakem, Paul Saunders, Umida Hashimova, and P. Kathleen Hammerberg, *Mapping Russian Media Network: Media's Role in Russian Foreign Policy and Decision-Making*, Arlington, Va.: CNA, January 2018, p. 38; Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkleman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, 2018, RR-2237-OSD, p. 12; Asymmetric Operations Working Group, *Ambiguous Threats and External Influences in the Baltic States, Phase 2: Assessing the Threat*, Ft. Meade, Md.: U.S. Army Asymmetric Warfare Group, Johns Hopkins Applied Physics Laboratory, November 2015, p. 29; Andris Spruds, Anda Rozukaine, Klavs Sedlenieks, Martins Daugulis, Diana Potjomkina, Beatrix Tolgyesi, and Ilvija Brug, *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, July 2015, pp. 26–27.

[g] Martin Kragh and Sebastian Asberg, "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies*, Vol. 40, Issue 6, 2017, p. 5.

[h] Robert Szwed, *Framing of the Ukraine-Russia Conflict in Online and Social Media*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, January 2018, p. 66.

[i] Zakem et al., 2018, p. 38; Dave Lee, "The Tactics of a Russian Troll Farm," BBC News, February 16, 2018.

[j] Audrey Belford, Saska Cvetkovska, Biljana Sekulovska, and Stevan Dojçinovic, "Leaked Documents Show Russian, Serbian Attempts to Meddle in Macedonia," OCCRP, Spooks and Spin in the Balkans, blog post, June 4, 2017.

[k] Kim Willsher and Jon Henley, "Emmanuel Macron's Campaign Hacked on Eve of French Election," *The Guardian*, May 6, 2017.

[l] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

[m] Rami Kogan, "Bedep Trojan Malware Spread by the Angler Exploit Kit Gets Political," *SpiderLabs Blog*, April 29, 2015.

[n] Joshua Kucera, "U.S. Intelligence: Russia Sabotaged BTC Pipeline Ahead of 2008 Georgia War," *EurasiaNet*, December 10, 2015. Russia has used cyberattacks at least twice to temporarily take down Ukraine's electricity distribution system. See U.S. Senate, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, minority staff report for the Committee on Foreign Relations, Washington, D.C.: U.S. Government Publishing Office, January 10, 2018, p. 68.

[o] National Cyber Security Centre, UK Government Communications Headquarters, "Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber-Attack," February 15, 2018; Alina Polyakova and Spencer Phipps Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Washington, D.C.: Brookings Institution, 2018, p. 14.

Page 376 of 3957

Page 377 of 3957

Table 3.1—Continued

[p] Alexandra Jolkina and Markian Ostaptschuk, "Activists or Kremlin Agents—Who Protects Russian-Speakers in the Baltics?" *Deutsche Welle*, December 9, 2015.

[q] U.S. Senate, 2018, p. 106.

[r] Jasna Vukicevic and Robert Coalson, "Russia's Friends Form New 'Cossak Army' in Balkans," Radio Free Europe/Radio Liberty, October 18, 2016.

[s] Edit Zgut, "Hungary's Pro-Kremlin Far Right Is a Regional Security Threat," *EU Observer*, December 23, 2016.

[t] U.S. Senate, 2018, p. 50; Simon Shuster, "How Russian Voters Fueled the Rise of Germany's Far-Right," *Time*, September 25, 2017.

[u] Kerin Hope, "Russia Meddles in Greek Town to Push Back the West," *Financial Times*, July 13, 2018.

[v] "Russia's Sberbank to Get 40 Pct of Croatia's Agrokor After Debt Conversion," Reuters, June 8, 2018.

[w] "UPDATE 3-Russia Raises Gas Prices for Ukraine by 80 Percent," Reuters, April 3, 2014.

[x] Hans Von Der Burchard, "EU Takes Billion-Euro Battle to Russia," *Politico*, January 5, 2018.

[y] Mark Baker, "Drinking Games," *Foreign Policy*, July 29, 2015.

[z] Ivan Watson and Sebastian Shukla, "Russian Fighter Jets 'Buzz' US Warship in Black Sea, Photos Show," CNN, February 16, 2017.

[aa] Thomas Goltz, "Letter from Eurasia: The Hidden Russian Hand," *Foreign Policy*, No. 92, Autumn 1993, p. 95; Robert Orttung and Christopher Walker, "Putin's Frozen Conflicts," *Foreign Policy*, February 13, 2015; Laura Mallonee, "Meet the People of a Soviet Country That Doesn't Exist," *Wired*, March 7, 2016.

[bb] Holcomb, 2017; "In U.N. Lawsuit, Ukraine Demands Russia End Support for Separatists," Reuters, January 17, 2017.

[cc] Elias Groll, "A Brief History of Attempted Russian Assassinations by Poison," *Foreign Policy*, March 9, 2018.

[dd] "Montenegro Begins Trial of Alleged Pro-Russian Coup Plotters," Reuters, July 19, 2017.

[ee] Roy Greenslade, "Journalists Covering the Ukraine Crisis Suffer Intimidation," *The Guardian*, July 23, 2014.

[ff] David M. Herszenhorn, "Crimea Votes to Secede from Ukraine as Russian Troops Keep Watch," *New York Times*, March 16, 2014.

[gg] Stephanie Joyce, "Along a Shifting Border, Georgia and Russia Maintain an Uneasy Peace," National Public Radio, March 13, 2017; Andrew Higgins, "In Russia's 'Frozen Zone,' a Creeping Border with Georgia," *New York Times*, October 23, 2016b.

Page 377 of 3957

CHAPTER FOUR

"Everyday" Gray Zone Actions Must Be Differentiated from More Aggressive, Focused Gray Zone Actions

Our research, games, and postgame discussions suggest some critical differences between the types of Russian gray zone tactics. An understanding of these differences is central to developing a clear framework and sense of how gray zone activities fit with other conventional military tactics. A recent U.S. Senate staff report expressed criticism of the U.S. government for not "hav[ing] a coherent, comprehensive and coordinated approach to the Kremlin's malign influence operations."[1] This is undeniably true, but it is in part because of the fact that there are important differences among Russia's gray zone activities that are often overlooked and which necessitate different types of responses. The first key insight emerging from the games and our research is that there are two central variables: the target of the action and whether it involves outright violence or the threat of violence. These variables are important for understanding Russian gray zone tactics because they imply different time horizons, objectives, and stakes. Many of the unconventional tactics that Russia uses to try to gain influence are routine, diffuse, and long-term, although others have very specific short-term objectives. Russian gray zone tactics might also be nonviolent, such as propaganda and disinformation, or involve outright violence or the threat of violence, such as the planned coup in Montenegro. Figure 4.1 shows how these two variables intersect to create four types of gray zone tactics and examples of each.

[1] U.S. Senate, 2018, p. 3.

Page 378 of 3957

Figure 4.1
Types and Examples of Gray Zone Tactics

Page 380 of 3957

The upper left-hand box represents everyday nonviolent gray zone tactics, which often have very general, high-level goals, such as enhancing Russian influence, and an imprecise notion of how specific actions will create a desired effect.[2] The Russian government appears to hope that these routine gray zone actions will benefit Russia and weaken the West in some way, but exactly how, when, and why often is not known when the actions are performed.[3] The everyday gray zone activities include propaganda and disinformation disseminated through traditional media and social media outlets; efforts to promote Russian, Slavic, or Orthodox culture; cultivating allies in politics or business; gathering intelligence on government actions and key individuals; and expanding Russia's economic influence by, for example, purchasing debt or large portions of key business sectors.

Routine gray zone actions are low-cost and low-risk, which is why Russia widely and opportunistically employs them in the hope that some might ultimately pay off. Likewise, Russia also expects many of them to have little or no effect, especially in the short term. One example is the multifaceted Russian effort to promote Russian, Slavic, and Orthodox culture in its near abroad. On their face, these activities might appear benign, but they can create or deepen divisions within other countries, and provide Russia with intermediaries that it can use to further its interests, and a reason to be actively involved abroad.[4] For instance, the Federal Agency for the Commonwealth of Independent

---

[2] U.S. Senate, *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel II: Hearing Before the Select Committee on Intelligence of the United States Senate*, Washington, D.C.: U.S. Government Publishing Office, March 30, 2017, pp. 1–2, testimony of Thomas Rid. According to Rid, "active measures are semi-covert or covert intelligence operations to shape an adversary's political decisions. Almost always active measures conceal or falsify the source—intelligence operators try to hind behind anonymity, or behind false flags."

[3] Raphael S. Cohen and Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat*, Santa Monica, Calif.: RAND Corporation, RR-1793-A, 2019, p. 2.

[4] Orysia Lutsevych, *Agents of the Russian World: Proxy Groups in the Contested Neighborhood*, London: Chatham House, The Royal Institute of International Affairs, April 2016; Ieva Berzina, "Russia's Compatriot Policy in the Nordic-Baltic Region," in *Russia's Footprint in the Nordic-Baltic Information Environment*, Report 2016/1027, Riga, Latvia: NATO Strategic Communications Centre of Excellence, January 2018.

Page 380 of 3957

Page 381 of 3957

States, Compatriots Living Abroad, and International Humanitarian Cooperation (commonly known as *Rossotrudnichestvo*) fosters the concept of the Russian World (*Russky Mir)* and has more than 60 centers, mainly in former Soviet states.[5] Although *Rossotrudnichestvo* is an autonomous Russian government agency, the Kremlin also supports such ostensibly independent NGOs as the World Congress of Russian Compatriots and World Without Nazism, which encourage traditional Slavic and Orthodox values and practices. These NGOs use the shared historical experience of fighting fascists during World War II as a reference point to rally opposition to current threats to traditional values, in particular Western institutions, such as the EU and NATO.[6]

Russian gray zone activities also seek to develop relationships with non-Russian partners who have similar agendas to Moscow or can indirectly advance the Kremlin's agenda. For instance, after Marine Le Pen, the president of the French National Front (now National Rally) party, publicly supported Russia's annexation of Crimea and called for the ending of economic sanctions on Russia, the Moscow-based First Czech-Russian Bank provided her party a much-needed €9.4 million loan.[7] Le Pen denied that the loan had anything to do with her stance on sanctions, although it made Le Pen a potential partner for Moscow.

The behavior and decisions of the Russia teams in our games provided some new insights and support for this framework and relationships between gray zone and more conventional activities. Specifically, these teams liberally sprinkled routine gray zone activities across as many targets as possible and then opportunistically adjusted their strategies to capitalize on previous successes. Both in our analysis of actual Russian actions and in our games, the majority of steady-state gray zone activities are long-term ventures that seek to shape public opinion, create or deepen fissures in a society, develop proxies, expand Russian media presence, and enhance Russia's ability to undertake more pointed gray zone operations in the future. Most of these measures are

---

5 Lutsevych, 2016, p. 10.

6 Lutsevych, 2016, pp. 12, 16.

7 Max Seddon and Michael Stothard, "Putin Awaits Return on Le Pen Investment," *Financial Times,* May 4, 2017.

Page 381 of 3957

Page 382 of 3957

not likely to directly further Russian objectives on their own, but they might cumulatively alter the social, political, and economic fabric of a country in ways that facilitate a subtle or gradual pro-Moscow shift.

However, nonviolent gray zone tactics can also be employed in a concentrated manner to achieve a specific near-term goal, which is captured in the upper right-hand box of Figure 4.1. Examples of such behavior include organizing peaceful protests, cutting off economic exchanges for dubious reasons, and interfering in foreign elections.[8] Targeted actions often rely on mobilizing the contacts or sentiment that Russia had previously cultivated through long-term diffuse gray zone tactics. Similarly, these actions are largely reliant on opportunities and events for Russia to exploit in the target country. For example, Russia appears to have organized and resourced anti-fracking movements in Bulgaria and Romania in an effort to scuttle deals made by American energy corporations that threatened Gazprom's dominance in the region. Russia deployed a media blitz against shale exploration deals and called on a variety of old and new allies to oppose the moves, including socialist parties, the Orthodox Church, sports clubs, environmental NGOs, and business contacts. Moscow allegedly even paid to bus protestors to the demonstrations.[9]

Russia also tries to subvert the democratic processes in other countries by influencing electoral outcomes, as has been alleged in the 2016 Brexit referendum, the 2016 U.S. presidential election, and the 2017 French presidential election. Russia attempted to tilt these votes through sophisticated disinformation campaigns and cyberattacks. Although Moscow's actions might have had a significant, direct impact

---

[8] In 2014, Moscow announced a ban on Polish fruits and vegetable imports for "sanitary reasons," but it was believed to be in retaliation for EU sanctions against Russia. Polina Devitt, "Russia Bans Polish Fruit and Vegetable in Apparent Retaliation for Sanctions," Reuters, July 30, 2014.

[9] Andrew Higgins, "Russian Money Suspected Behind Fracking Protests," *New York Times*, November 30, 2014; Andrew MacDowall, "Chevron's Bulgaria Pull-Out a Blow for Energy Security," *Financial Times,* June 11, 2014; Sam Jones, Guy Chazan, and Christian Oliver, "NATO Claims Moscow Funding Anti-Fracking Groups," *Financial Times*, June 19, 2014; Keith Johnson, "Russia's Quiet War Against European Fracking," *Foreign Policy*, June 2014.

Page 382 of 3957

Page 383 of 3957

on the target country's policies, they still fall into the category of nonviolent targeted gray zone actions because Russia acted opportunistically and exclusively used nonmilitary tools in an effort to swing the polls. In our games, Red teams always tried to sway scheduled elections because the risks of doing so were relatively low and, although the probability of obtaining a payoff was also low, the reward was potentially very high.

However, many Russian gray zone tactics have a much sharper edge than those discussed previously because they involve the threat or application of force. The lower-left hand box of Figure 4.1 shows diffuse gray zone tactics that at least implicitly involve the threat of violence, including efforts by Russia to cultivate ties to criminal or paramilitary organizations. The Kremlin and, in particular, Russia's intelligence agencies have extensive ties to the criminal underworld and use these organizations as deniable agents that can carry out such illicit tasks as strongarming opponents, gathering intelligence, and at times having individuals within these organizations act as hitmen. Additionally, criminal organizations can be used to secure cash that can fund other ventures that the Kremlin does not want to traced back to it.[10] For instance, Moscow reportedly began funding the Night Wolves motorcycle gang in 2013, and through these efforts, managed to turn the organization into an ultranationalist government proxy.[11] The Night Wolves go on tours, such as their 2018 trip to the Balkans, to propagate pro-Russian views and to impress and intimidate observers.[12]

Russia also seeks to develop relationships with paramilitary organizations. In Bosnia, for instance, the Kremlin is reportedly helping to develop Serbian Honour, a new militia loyal to Milorad Dodik, the president of the semi-autonomous Republic of Srspka (RS), who is "a

---

[10] Mark Galeotti, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*, Brussels: European Council on Foreign Relations, April 2017, pp. 6–8.

[11] Mark Galeotti, "An Unusual Friendship: Bikers and the Kremlin," *Moscow Times*, July 20, 2018; Kira Harris, "Russia's Fifth Column: The Influence of the Night Wolves Motorcycle Club," *Studies in Conflict and Terrorism*, 2018.

[12] Whether the Night Wolves really intimidate has been questioned. Andrew Higgins, "Russia's Feared 'Night Wolves' Bike Gang Came to Bosnia. Bosnia Giggled," *New York Times*, March 31, 2018.

Page 383 of 3957

Page 384 of 3957

frequent visitor to Moscow."[13] Russian mercenaries with ties to the Kremlin allegedly began training Bosnian Serb recruits at a training center, funded by Moscow, in Serbia.[14] This is exacerbating already tense relations between RS and the Bosniak-Bosnian Croat Federation. RS seeks more autonomy—if not complete independence—from Bosnia, and promotes an ultranationalist Serbian agenda.[15] A Bosnian Serb paramilitary has heightened fears of sectarian violence and deepened divisions within Bosnia, and potentially could be used as a means of destabilizing the state should it seek to move closer to NATO.

Additionally, Russia has undertaken much more aggressive and directed short-term gray zone actions that involved the threat of or actual use of violence, usually when it perceived its vital interests to be at risk, which is displayed in the lower right-hand box. This category includes Russia's 2008 war in Georgia and the 2014 war in the Donbass in eastern Ukraine. From the start, the former was a conventional military offensive disguised as a peacekeeping operation, which included a small number of gray zone tactics, including cyberattacks to interrupt Georgian government communications, and a media campaign to promote the Russian government's narrative in the breakaway region of South Ossetia and to the international community.[16]

The latter operation began principally with gray zone tactics, primarily the use of Ukrainian proxies, such as the Donetsk People's Republic and Luhansk People's Republic militias, which were bolstered by both irregular and regular forces from Russia.[17] The Russian forces

---

[13] Economist Intelligence Unit, "Russia's Role in the Western Balkans," webpage, October 18, 2017.

[14] Julian Borger, "Russian-Trained Mercenaries Back Bosnia's Serb Separatists," *The Guardian*, January 12, 2018.

[15] Alan Crosby, "Here Are the Flashpoints You Should Be Watching in the Balkans," Radio Free Europe/Radio Liberty, April 28, 2017; Thomas Rosner, "The Western Balkans: A Region of Secessions," *Deutsche Welle*, October 4, 2017.

[16] Caroline V. Pallin and Fredrik Westerlund, "Russia's War in Georgia: Lessons and Consequences," *Small Wars and Insurgencies*, Vol. 20, No. 2, 2009.

[17] The Ukrainian insurgency was manufactured by the Kremlin, and the Ukrainian separatist organizations were fragmented, weak, and wholly dependent on Russian support to survive. Franklin Holcomb, *The Kremlin's Irregular Army: Ukrainian Separatist Order of*

Page 384 of 3957

Page 385 of 3957

were purported to be sympathetic "volunteers," including the Night Wolves, foreign fighters in the multinational Vostok Brigade, and Russian military personnel who supposedly took a leave of absence to support their Ukrainian allies.[18] Russia's initial strategy, which was heavily reliant on proxy and unmarked forces, failed as the Ukrainian government was able to push the separatists to the brink of defeat.[19] To save its proxies, Russia deployed large numbers of conventional forces beginning in August 2014 and moderated its goals from aiming to undermine the Ukrainian government to consolidating the separatists' foothold in the Donbass region, thereby ensuring that the conflict would continue and providing Moscow with a lever that it could use to dial up or dial down pressure on the Ukrainian government in Kyiv. Although Russian proxies and the GRU continue to be active in Ukraine, the fight is still predominantly conventional combined-arms operations of lower intensity, even though Moscow does not acknowledge its role in the war.

Even the takeover of Crimea, which arguably involved the most successful deployment of gray zone tactics to date—Russia was able to annex the peninsula without going to war—depended heavily on conventional Russian forces. While local pro-Russian self-defense "volunteers" and proxies assisted by, for example, blocking the roads in Sevastopol, the operation was led by Russian special forces (spetsnaz) and unmarked Russian soldiers from the 810th Independent Naval Infantry Brigade (a marine unit). The operation was facilitated by a large snap exercise in the Western and Central Military Districts to cover for troop movements, divert attention from the events in Crimea, and

---

Battle, Russia and Ukraine Security Report 3, Washington, D.C.: Institute for the Study of War, September 2017, p. 9.

[18] Galeotti, 2016, pp. 285–286; Racz, 2015, p. 12; Damon Tabor, "Putin's Angels: Inside Russia's Most Infamous Motorcycle Club," *Rolling Stone*, October 8, 2015; Jack Losh, "Putin's Angels: The Bikers Battling for Russia in Ukraine," *The Guardian*, January 29, 2016; Andrew Roth, "A Separatist Militia in Ukraine with Russian Fighters Holds a Key," *New York Times*, June 4, 2014a.

[19] Holcomb, 2017, p. 7.

Page 385 of 3957

Page 386 of 3957

deter the Ukrainian government from intervening.[20] In short, although gray zone tactics were employed in Georgia, Crimea, and the Donbass, all three involved Russian military forces capturing territory, and only in Crimea was conventional combat avoided.[21]

These high-intensity gray zone actions were not opportunistic, but were in reaction to a perceived threat to Russia's vital interests, specifically, the dangers posed by the potential expansion of NATO and EU membership to Georgia and Ukraine, respectively. As a result, Moscow was willing to use more risky tactics that directly involved Russian military forces and therefore had a higher probability of being uncovered and leading to unwanted consequences, as ultimately occurred in the Donbass. These Russian offensives were primarily military in nature, with support provided by diplomatic, economic, information, and cyber gray zone actions. In our games, the Russian players were quite reluctant to use military forces, even "little green men," for fear of inadvertent escalation. This result might be because the games did not present the Red teams with a scenario in which their vital interests were endangered, as they were perceived to be in 2008 and 2014. Additional iterations of the game would help to determine whether the Red teams generally preferred nonviolent gray zone tactics or whether they were willing to take covert violent action and overt military operations when the stakes were high enough, particularly when coupled with further research in this area.

There have also been less militarized—but still coercive and violent—Russian gray zone actions in response to a particular crisis, or intended to achieve a specific objective. In October 2016, Moscow conspired with two members of Montenegro's Democratic Front (DF) party and several Serb nationals to launch a last-ditch effort to derail Montenegro's entry into NATO by trying to overthrow the govern-

[20] Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Oleysa Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Santa Monica, Calif.: RAND Corporation, RR-1498-A, 2017, pp. 7–10; Galeotti, 2016, p. 285.

[21] Radin makes a similar point that so-called gray zone operations relied heavily on conventional forces. Radin, 2016, p. 7.

Page 386 of 3957

Page 387 of 3957

ment.[22] Russia only resorted to this elaborate scheme, which involved a planned attack on parliament and an assassination attempt on Montenegro's prime minister, after its softer gray zone tactics aimed at undermining Montenegrin support for NATO—including a concerted information operation campaign, funding the anti-NATO DF party, and backing anti-NATO protests—had failed.[23]

Similarly, during the 2007 "bronze soldier" incident, Russia orchestrated protests and riots in Tallinn, a siege of the Estonian embassy in Moscow, and widespread cyberattacks that disabled many Estonian websites for nearly two weeks in response to a decision by the Estonian government to relocate a Soviet World War II memorial.[24] Although the stakes were much lower in this episode, which was a test of Tallinn's resolve and Russia's ability to employ gray zone techniques, Russia was willing to use these varied gray zone tactics, including inciting violence, in an attempt to compel Tallinn to leave the bronze soldier monument in place.

---

[22] U.S. Senate, 2018, p. 77; Emily Holland and Rebecca Friedman Lissner, "Countering Russian Influence in the Balkans," *Lawfare*, August 6, 2017.

[23] Vera Zakem, Bill Rosenau, and Danielle Johnson, *Shining a Light on the Western Balkans: Internal Vulnerabilities and Malign Influence from Russia, Terrorism, and Transnational Organized Crime*, Arlington, Va.: CNA, May 2017, p. 17.

[24] U.S. Senate, 2018, p. 101.

Page 387 of 3957

CHAPTER FIVE

NATO and the EU Are Unlikely to Be Able to Compel Russia to Stop Using Nonviolent, Everyday Russian Gray Zone Tactics, but They Might Be Able to Deter Higher-Order Aggression

There is much talk about "deterring" Russian gray zone aggression, but many of these discussions are based on a misunderstanding of the concept. Both deterrence and compellence are types of coercive threats that work by altering a target's expectations about future pain, but deterrent threats aim to persuade the target not to initiate a particular action, and compellent threats aim to convince the target to change its behavior. As one of our players observed, because Russia is *already* engaging in diffuse gray zone actions, NATO and the EU need to *compel* Russia to stop these activities, which is a much harder task than deterrence.[1] To date, NATO and the EU remain focused on deterrence, rather than compellance, making this proposition a shift in these institutions' approach.

To successfully deter, one must credibly threaten painful consequences, which involves demonstrating a capability and willingness to follow through on that threat and waiting to see whether the target complies. In contrast, to successfully compel a target to reverse or halt its ongoing behavior, one must actually inflict pain and couple it with a promise to end the pain if the target relents. It is not clear that NATO

[1] Compellence requires the target to change its ongoing behavior—in which it is invested—at some cost to its reputation. To compel a target, one must alter or reduce the utility of its current course of action compared with the utility of ceasing. Thomas C. Schelling, *Arms and Influence*, New Haven, Conn.: Harvard University Press, 1966, pp. 69–90.

Page 388 of 3957

Page 389 of 3957

and the EU would go beyond the economic sanctions that are already in place to compel Russia to end its use of diffuse gray zone tactics.[2] Both the Green and Blue players in our games struggled to identify actions that they deemed to be sufficiently compellent *and* would be willing to implement. Moreover, the characteristics of routine or everyday gray zone tactics—the fact that they are largely nonmilitary, usually gradual, and difficult to decisively attribute—lowers the stakes and makes it difficult for the West to credibly threaten to punish Russia, even if the actions are conclusively traced back to Moscow.

Because many gray zone tactics are cheap in terms of cost and risk, Russia is willing to liberally use them even when the prospect of success is low. The Red teams in our games mirrored the real Russian government's indifference to having its covert gray zone activities uncovered, in part because of the lack of credible punishment. The Green and Blue players spent considerable time and effort trying to expose Red's clandestine activities, but even when they succeeded, this had little effect on any of the teams' behavior: Red teams continued their covert meddling as if nothing had happened, and the Green and Blue teams still found it hard to come up with credible ways to counter Red's activities or punish Red for engaging in them. Consequently, the Red teams saw nearly no downside to extensively making use of routine gray zone actions in the hopes that some would have an impact.

Even if more assertive and violent efforts—such as destabilizing a country or attempting to forcibly change the government through a coup—failed or were uncovered, there were few negative consequences for the Red teams in our games. This tracks not just with recent experience but also broader Cold War history. The United States was never able to halt Soviet active measures, which were the normal state of affairs during the Cold War: The Soviet Union conducted more than 10,000 individual disinformation operations during this time.[3]

Because of the challenges of attribution, deterrent threats against even targeted, nonviolent gray zone actions are not likely to be highly

---

[2] There are already many people calling for an end to the sanctions, despite Russia's continued use of diffuse and targeted nonviolent gray zone tactics across Europe.

[3] U.S. Senate, 2017, p. 2.

Page 389 of 3957

credible. It stretches the bounds of credulity to believe that a democratic country, which requires the support of its population, would take potentially costly coercive actions when the majority of its public remains unconvinced about who is responsible for a nonviolent attack. The need to convince 29 nations in the alliance makes it even less likely that a NATO threat would be viewed as credible. Although NATO has claimed that its Article V collective security clause applies to cyberattacks against members, it has not clearly articulated what types of cyberattacks would trigger this and what actions it would take in response. Establishing that Moscow is behind a gray zone tactic might put sensitive intelligence sources at risk and is also likely to take a considerable amount of time. For example, although the Federal Bureau of Investigation began to investigate Russian interference in the 2016 U.S. presidential election in June 2016, the investigation was still ongoing as of June 2019. The fact that consequences are not likely to be automatic or quickly implemented poses a further challenge to deterrence. Clandestine forms of retaliation, such as cyberattacks or covert action, might be possible because the public is not consulted, but these options are in and of themselves risky, cannot be threatened publicly, might be limited by the laws of a country, and therefore do not form the basis for a strong deterrent threat. Given these manifold challenges, it seems more effective to focus on improving the resiliency of vulnerable nations and taking other defensive measures to limit the effectiveness of Russian intervention, rather than focusing on deterring most gray zone tactics.

Outright Russian aggression—including gray zone tactics with the aim of territorial expansion—is an entirely different situation, and one that can be deterred. Because NATO did not have a security commitment or forces in place to defend Ukraine or Georgia, any attempts to deter Russia would likely have lacked credibility. In the future the alliance could, however, make it clear that it plans to stop aggression—whether conventional or masked by gray zone tactics—against any of its members. Doing so requires NATO to demonstrate the will and capability to act quickly to stop Russia from achieving its objectives,

Page 391 of 3957

as deterrence by denial would in any situation.[4] NATO military and intelligence services need to be on alert for Russian preparations disguised as gray zone subterfuge that could signal aggressive intentions. At the same time, political leaders need to be prepared for this eventuality and ready to listen to military and intelligence assessments so that they can quickly see through any ambiguity and take the appropriate actions. Both of these steps need to be buttressed by a military posture that would lend credibility to political leaders' warnings or threats about the consequences should Russia persist.

---

[4] Deterrence by punishment, the other alternative mode, does not appear to be a strong approach for dealing with Russian aggression against NATO. See David A. Shlapak, *The Russia Challenge*, Santa Monica, Calif.: RAND Corporation, PE-250-A, 2018; David A. Shlapak and Michael W. Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics*, Santa Monica, Calif.: RAND Corporation, RR-1253-A, 2016; Michael Petersen, "The Perils of Conventional Deterrence by Punishment," *War on the Rocks*, November 11, 2016.

Page 391 of 3957

CHAPTER SIX

Vulnerability to Russian Gray Zone Tactics Varies Significantly Across Europe

Russia employs gray zone tactics across Europe, but its interests vary, and its ability to successfully achieve its objectives through these means largely depends on the vulnerability of the targeted country.[1] This insight emerged from both our games and our analysis of past historical cases. In one of our early games, the Red team drew a map of Europe and defined different regions in which Russia had varied levels of interest and, in the Red team's perception, a different ability to influence because of the strengths and weaknesses of the countries in each area. Gray zone tactics often work best when they exacerbate preexisting tensions. Vulnerabilities fall into two different but not mutually exclusive categories: state fragility and polarization, and characteristics that provide Russia with leverage over the government and society.[2]

Fragile states provide openings because they suffer from pernicious factors, such as corruption; poverty; and political divisions, sectarian divisions, ethnic divisions, or some combination thereof, which can be exploited by Moscow's gray zone tactics to create instability.

[1] Treverton et al., 2018, p. 63.

[2] In the structured Balkans game, these factors affected a country's governance and orientation scores, which were relative, ordinal scales ranking from –2 to +2. Governance was a composite metric based on the Fund for Peace's Fragile States Index and the World Bank Worldwide Governance Indicators, although the orientation score was based on a more qualitative reading of the composition of a country's ethnic makeup, religious beliefs, and culture and its current attitudes toward Russia. As a part of scoring countries, we had regional experts review our initial scores and the justification for them. See Fund for Peace, "Fragile States Index," webpage, 2019; World Bank Group, "Worldwide Governance Indicators," webpage, 2019.

Page 392 of 3957

Page 393 of 3957

The politics in even relatively strong states might become polarized over divisive issues (e.g., immigration), opening avenues for Russian subversive actions. Countries can have cultural, economic, or historic ties to Russia that make it particularly susceptible to Russian gray zone influences. Proximity and, in particular, a shared border with Russia also ease Russian access to a country and concomitantly increase Russia's ability to undertake violent gray zone tactics. Economic dependence, particularly on Russian energy, is also an avenue that Moscow has been willing to exploit.

Although there are significant intraregional differences, one can identify four broad European regions—Russia's near abroad, the Baltics, the Balkans, and Western and Central Europe—where Russia's interests differ. But across these regions, there are roughly similar degrees of vulnerability to gray zone actions. This is depicted in Figure 6.1. Our games suggest that considering these four regions as distinct when preparing and planning to confront Russian gray zone tactics might be valuable, because of Russia's differing interests and the variation in vulnerabilities across these areas. The Red teams in our games emphasized that their interests varied across these areas and developed strategies unique to each region, based on their different objectives. Understanding these differences in interests, objectives, and existing vulnerabilities better enables NATO and the EU to identify the tools best used to counteract Russian gray zone tactics in different regions.

The countries that were identified of greatest importance were in Russia's near abroad: Armenia, Azerbaijan, Belarus, Georgia, and Ukraine.[3] Russia desires influence over these former Soviet states not only because of their shared history and language, but most importantly because these bordering nations provide an important defensive buffer against external attack.[4] Therefore, Russia views the expansion of NATO or the EU into its near abroad as a grave threat that must be stopped. The 2008 and 2014 Russian wars in Georgia and Ukraine

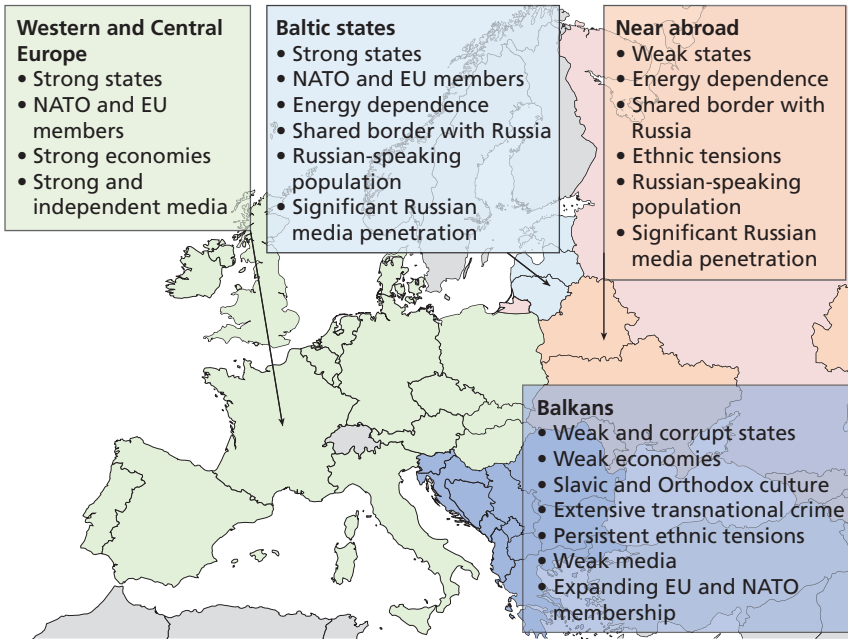
[3] The former Soviet republics in Central Asia are also usually included in the near abroad, but they were not a part these games.

[4] Andrew Radin and Clint Reach, *Russian Views of the International Order*, Santa Monica, Calif.: RAND Corporation, RR-1826-OSD, 2017, pp. 8–12.

Page 393 of 3957

Page 394 of 3957

Figure 6.1
Intra-European Vulnerability to Russian Gray Zone Tactics



were launched to thwart their membership bids by generating a persistent source of instability that would ward off further integration with the West.

Near-abroad nations bordering Russia have relatively weak militaries and poor governance, leaving them with few defenses against a Russian conventional offensive or clandestine infiltration, including land grabs by little green men. All also contain large Russian-speaking minorities that have historical, cultural, and economic links to Russia; these populations are consumers of Russian-controlled media and are potentially sympathetic audiences for gray zone information tactics.

By contrast, the Baltic states of Estonia, Latvia, and Lithuania are also former members of the Soviet Union, are adjacent to Russia, and Estonia and Latvia have sizable Russian-speaking minorities. However, they appear to be less susceptible to gray zone tactics than some other

Page 394 of 3957

Page 395 of 3957

regions.[5] This is due in part to the Baltic nations taking steps to mitigate some of their vulnerabilities. Estonia, for instance, has invested heavily in cyber defenses since the bronze soldier crisis, and all three nations are taking steps to reduce their dependence on Russian energy imports.[6] Additionally, the Baltic nations are relatively prosperous compared with other Eastern European nations and Russia, reducing the level of economic discontent into which the Kremlin can tap. Nevertheless, the Russian minority in the Baltics is less well-off than the rest of the population, in large part because economic opportunities still largely depend on being able to speak the official state language (i.e., not Russian); consequently, the Russian minority potentially could become aggrieved in the future.[7] Moreover, a favorite theme of the Russian media (which is popular among the Estonian and Latvian Russian-speaking populations) is how the Baltic states discriminate against their Russian minorities. To date, however, this message does not seem to resonate, because the benefits of living within the EU members of the Baltics—as opposed to Russia—seem to outweigh the relative disparity between Russian-speakers and the larger Estonian and Latvian populations.

The Baltics' most important defense against Russian gray zone attacks stems from the relative strength of their government institutions, which make them harder targets and better able to respond to covert infiltration than other former Soviet republics.[8] For instance, the Estonian defense chief stated that, if Russian special forces or clandestine agents entered their territory, they would "shoot the first one to appear."[9] All three Baltic nations have amended their laws to enable

---

5 Many argue that despite the fact that the Baltics are former members of the Soviet Union, they are of lesser interest to Russia since 2003.

6 Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News, April 27, 2017; Simon Hoellerbauer, "Baltic Energy Sources: Diversifying Away from Russia," Foreign Policy Research Institute, June 14, 2017; Asymmetric Operations Working Group, 2015, pp. 17–20.

7 Asymmetric Operations Working Group, 2015, pp. 24–28.

8 Asymmetric Operations Working Group, 2015, pp. 4–5.

9 Sam Jones, "Estonia Ready to Deal with Russia's 'Little Green Men,'" *Financial Times*, May 13, 2015.

Page 395 of 3957

Page 396 of 3957

their national militaries to operate in their countries during peacetime, and Estonia and Lithuania have exercised this capability.[10] Additionally, because the Baltics are members of NATO, and the alliance has stationed multinational battlegroups in each country, Russian covert infiltration or outright aggression is much riskier than in its near abroad.

Moreover, unlike Ukraine or Georgia, Russia does not seem to consider the Baltic states to be a critical part of its sphere of influence; instead, it aims to use the Baltics as a lever to destabilize and discredit NATO.[11] Given these factors, it appears that, although Russia could and has sought to destabilize Estonia, Latvia, and Lithuania through everyday gray zone operations, these tactics are likely to have limited effects. The Baltic states are also not particularly susceptible to clandestine land grabs. However, despite the enhanced forward posture, they remain vulnerable to a conventional offensive cloaked in gray zone tactics, especially information operations.[12]

There is considerable variation within the Balkans, but, in general, this region is an inviting target for Russian gray zone actions because of the weak rule of law, ethnic divisions, and relative poverty.[13] Nevertheless, because the Balkans are not contiguous with Russia and do not have significant Russian-speaking populations, Russia's gray zone activities would have a somewhat different character than the actions it takes in the former Soviet states, and are less likely to swing these states in a durably pro-Russian direction.

As a whole, the Balkans suffer from weak government institutions, resulting in autocratic leaders who can run roughshod over feeble

---

[10] Asymmetric Operations Working Group, 2015, p. 6.

[11] Radin and Reach, 2017, p. 10; Dmitri V. Trenin, *Post-Imperium: A Eurasian Story*, Washington, D.C.: Carnegie Endowment for International Peace, 2011, p. 107; Asymmetric Operations Working Group, 2015, p. 14.

[12] Radin, 2017, p. 31. For more on conventional vulnerability, see Shlapak and Johnson, 2016.

[13] There is no agreed definition of the Balkans. We consider the Balkans to include Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Kosovo, North Macedonia, Montenegro, Romania, Serbia, and Slovenia.

Page 396 of 3957

Page 397 of 3957

civil society, a subservient media, pervasive corruption, and extensive transnational criminal organizations.[14] The Balkans are also the poorest region in Europe with high unemployment rates, which means that there is widespread dissatisfaction and resentment toward Europe as a whole, which can be exploited by Russia.[15] Finally, the Balkans remain afflicted by ethnic tensions, currently being rekindled by a renewed focus on historic grievances and another surge of nationalist sentiment in the region.[16] Ethnic violence and secessionist movements are particularly a problem in the former Yugoslavia (Bosnia and Herzegovina, Croatia, North Macedonia, Montenegro, Serbia, and Slovenia), where Russia has historic, religious, and linguistic ties to several groups.

Opinions about Russia vary significantly in different Balkan nations; in some, such as the Slavic language–speaking nations of Bulgaria and Serbia, a sizable part of the population views Russia positively.[17] But unlike the near abroad, where Russian gray zone activities primarily focus on already sympathetic populations, Russia courts allies on multiple sides in many Balkan nations. This places Moscow in a good position to stoke tensions, provoke sectarian violence, or encourage separatism. Yet because the nearest Russian military forces are stationed in Crimea, this region is less at risk for a covert territorial attack or conventional Russian aggression accompanied by gray zone activities.

In terms of Russia's interests, the Balkans are a lower priority than the near abroad, but remain an area where Moscow desires to at least maintain—if not expand—its sway and curb Western influence.[18]

---

[14] Zakem, et al., May 2017, pp. 1–2.

[15] Zakem et al., 2017, p. 6; Martin Russell, *At a Glance: Russia in the Western Balkans*, European Parliament Members' Research Service, July 2017.

[16] Zakem et al., 2017, p. 6; Zoran Arbutina, "Balkan Countries See Rise in Hate Speech," *Deutsche Welle*, February 24, 2017.

[17] "IRI's Center for Insights Poll: Crises in Europe and EU Leave Serbs Turning Toward Russia," International Republican Institute, December 2016; Pew Research Center, *Religious Belief and National Belonging in Central and Eastern Europe*, Washington, D.C., May 10, 2017, pp. 35–37; Rick Lyman, "Bulgaria Grows Uneasy as Trump Complicates Its Ties to Russia," *New York Times*, February 4, 2017.

[18] Radin and Reach, 2017, specifically Figure 2.1, p. 11.

Page 397 of 3957

Page 398 of 3957

Consequently, Russia aims to prevent any further encroachment of Western multilateral organizations, but their expansion into this region is not seen as an existential threat unless it is tied to particular initiatives, such as missile defense.[19] Russia might also view the region, which includes many of the newest and most vulnerable members of NATO and the EU, as an opportunity for undermining Western consensus by exposing the weaknesses of these new members and testing the West's ability to support them.

Finally, Western and Central European states are the least vulnerable to Russian gray zone tactics and are outside Russia's desired sphere of influence. These states are characterized by strong government institutions, relatively low corruption, general prosperity, and strong and independent media. Nevertheless, Moscow undertakes everyday gray zone actions throughout this region, because although they have the worst odds of succeeding, they also offer the highest potential payoff should they weaken a long-standing NATO or EU member's commitment to European unity. By dividing these organizations, Russia could also undermine the economic sanctions put in place against it after its invasion of Ukraine. Moreover, there are fissures in many Western and Central European states that Russia could potentially exploit—most notably, the immigration crisis, widespread dissatisfaction with the EU, and concerns about terrorism. Moscow has also curried favor with several populist and right-wing parties that promote nationalist, anti-integration agendas, such as Le Pen's National Rally in France.[20]

---

[19] The Balkan Regional Approach to Air Defense is a joint NATO and Balkan initiative, initiated in 2010, to provide air defense capabilities to the Balkans. It is intended to be integrated into the broader NATO ballistic missile defense system, which is viewed with suspicion by Russia. NATO Communications and Information Agency, *Balkan Regional Approach to Air Defence (BRAAD)*, Brussels: North Atlantic Treaty Organization, undated.

[20] David Chazan, "Russia 'Bought' Marine Le Pen's Support over Crimea," *The Telegraph*, April 4, 2015.

Page 398 of 3957

CHAPTER SEVEN

Civilian Organizations, Rather Than the Military, Might Be Best Positioned to Counter Most Russian Gray Zone Tactics

NATO and its member states' armed forces have focused considerable attention on countering Russian gray zone actions. Clearly, there is an important role for the military in deterring high-order aggression, whether it is attempted through purely gray zone tactics or through conventional means—which almost surely will be coupled with gray zone activities—but the vast majority of Russian gray zone activities are not geared toward territorial gains, but instead are everyday operations seeking to enhance Russia's influence through nonmilitary means. In short, our research suggests that the fight against gray zone activities is primarily a social, political, and economic fight—not a military one. Our games illuminated this observation. Many of the Blue and Green teams in our games argued that this fight is better waged by civilian agencies and NGOs, whose core competencies lie in these domains. These players observed that the most effective countermeasures available to the Blue and Green teams were not military actions, but rather actions taken by the U.S. Department of State, ministries of foreign affairs or economy, or the United States Agency for International Development to strengthen governments and liberal institutions. These players viewed the military's role in countering Russian gray zone tactics as a supporting one, buttressing and reinforcing civilian activities, and something that needed to be included in a whole-of-government approach.

Page 401 of 3957

Moreover, the West should not simply react to Russian gray zone actions or try directly to counter them. Rather, the United States and Europe need to develop long-term strategies to address the underlying weaknesses in states that Russia's gray zone tactics try to exploit and build more resilient democratic societies that will be able to fend off these actions on their own.[1] This should include efforts to raise awareness about false news, strengthen independent journalism, improve media literacy, fight corruption, bolster the rule of law, and diversify Europe's energy sources to reduce Moscow's economic leverage, especially on less prosperous countries.

The military plays an important but limited role in countering Russian gray zone activities by improving cyber defenses, enhancing intelligence and counterintelligence capabilities, and building partner special forces capacity so that allies can independently and effectively respond to any Russian covert infiltrations. Additionally, to improve responsiveness, the United States should encourage collaboration between law enforcement and the military, so that intelligence can be shared in a timely fashion and to ensure that a country has clearly delineated the roles and responsibilities of different government organizations in the event that Russia employs violent gray zone tactics.[2] In general, however, security force assistance, especially targeting general-purpose forces, should be a lower priority than efforts to strengthen civilian government institutions, the media, and civil society when seeking to counter gray zone tactics. NATO and its member states' armed forces should remain focused on bolstering conventional and nuclear deterrence while enhancing crisis stability, not on Russia's gray zone tactics.

---

1 Mazarr, 2015, pp. 118, 126.

2 We thank Dara Massicot for this point.

Page 401 of 3957

CHAPTER EIGHT

The West Might Be Winning This Competition, but Does Not Recognize It

Although many question whether Russia would ever overtly attack the Baltics or any NATO member, few disagree with the contention that Russia takes gray zone actions against nations in Europe and the United States on a daily basis.[1] These everyday Russian gray zone operations have caused concern verging on the point of panic and defeatism in some parts of Washington and Brussels.[2] These sentiments seem mostly to stem from the idea that the West cannot stop Russia from using gray zone activities; therefore, it is somehow *losing*. These sentiments—echoed by many players in our games—neglect an evaluation of the larger strategic situation. Our games provided important insights on this point.

Generally, players agreed that it is very difficult to decisively prove what effect everyday gray zone tactics have had in a myriad of countries. At this time, the only conclusion we can reach is that Russia has been actively interfering in electoral contests; there is no conclusive

[1] Michael Kofman, "Fixing NATO Deterrence in the East Or: How I Stopped Worrying and Love NATO's Crushing Defeat by Russia," *War on the Rocks,* May 12, 2016.

[2] Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 13, 2018; European Union External Action Service, *Joint Communication: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*, Brussels: European External Action Service, June 13, 2018; "Countering 'Hybrid' Security Threats a Priority, Says EU," *EUbusiness*, July 19, 2017; Frank Jordans, "European Spy Chiefs Warn of Hybrid Threats from Russia, IS," Associated Press, May 14, 2018; Julian E. Barnes, "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attacks," *New York Times*, July 13, 2018.

Page 402 of 3957

Page 403 of 3957

evidence, however, that those efforts affected the outcomes.[3] After the French public was alerted to the fact that Russia was backing Le Pen, Moscow's gray zone tactics might have even backfired, contributing to a decisive victory for Emmanuel Macron.

By stepping back and taking a wider look at the situation, it appears that the West might *not* be losing. Russian gray zone tactics are now the normal state of affairs.[4] After one game, a player observed that the West cannot force Russia to desist in these actions, but it is far from clear that they are having much effect. Russia's largest victories—in Crimea and the perhaps Pyrrhic victory in the Donbass—have combined gray zone techniques with more traditional applications of military power, but these outcomes are the exception—not the norm.[5] Moreover, in the Donbass, gray zone tactics alone did not bring victory, and now Moscow is bogged down in an increasingly costly war against a determined Ukrainian resistance. At the same time, the Russian economy is in the midst of an economic crisis exacerbated by the international sanctions put in place after its offensives in Ukraine. More significantly, Russia's offensives in Crimea and the Donbass have unified and galvanized Europe in a way that was unimaginable only four years ago. In that short time span, NATO has gone from shrinking and consolidating its military posture to expanding it, pushing forces farther eastward in an effort to bolster the defenses of the Baltic states. As one of the Blue players observed, Russia's gray zone aggression in Crimea and conventional offensive in eastern Ukraine have succeeded in preventing Ukraine from entering the EU, but have reignited a strategic competition with the West, which Russia is not winning and, in the long term, cannot win.[6]

---

[3] U.S. Senate, 2018, p. 2; Indictment, *United States of America v. Internet Research Agency,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018); Indictment, *United States of America v. Viktor Borisovich Netyksho*, Case 1:18-cr-00215-ABJ (D.D.C. July 13, 2018).

[4] Mazarr, 2015, p. 107, warns of a sense of "relentless confrontation" or "persistent warfare."

[5] Mazarr, 2015, p. 121.

[6] Russia has several key weaknesses, most notably its economy, its demographic issues, and its authoritarian kleptocratic regime. Joss Meakins, "Why Russia Is Far Less Threatening Than It Seems," *Washington Post*, March 8, 2017. For a contrary perspective which argues

Page 403 of 3957

Page 404 of 3957

Just because Moscow has not gained a significant advantage with its gray zone activities to date does not mean that the West should ignore these Russian actions. The United States and its European allies need to take steps to strengthen their defenses against gray zone tactics and to improve their ability to identify when Russia is shifting from everyday gray zone tactics to a more targeted campaign. Even the strongest states need to combat "truth decay"—which Russian gray zone tactics contribute to—by expanding awareness about disinformation and teaching how to distinguish facts from fiction.[7] Additionally, they should shore up defenses by addressing critical cyber vulnerabilities. These steps will not entirely stamp out Russian gray zone actions, but by addressing critical vulnerabilities, they will increase the ability of a society to withstand them. The EU and NATO also need to work to strengthen the resiliency of weaker states by building democratic, civilian institutions and an independent media, both of which are the most vulnerable targets of gray zone aggression.[8]

In short, just because the West might be ahead in this competition does not mean that it can ignore gray zone aggression. At the same time, however, the United States and its European allies should not overreact. Russia's greatest tactical successes largely depended on its conventional military forces, not the gray zone tools that supplemented them.[9] High-order aggression is something that can be stopped through conventional deterrence. If Washington and Brussels focus most of their efforts on stopping Russian social media trolls, countering each false news story, and promoting their own strategic narrative,

---

that Russia's strategy of raiding could succeed, see Michael Kofman, "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," *War on the Rocks*, June 14, 2018.

[7] Jennifer Kavanagh and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica, Calif.: RAND Corporation, RR-2314-RC, 2018.

[8] Brittany Beaulieu and David Salvo, "NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence," *GMF Alliance for Security Democracy*, Policy Brief, No. 031, 2018, p. 5.

[9] For more on Russia's conventional military, see Scott Boston and Dara Massicot, *The Russian Way of Warfare: A Primer*, Santa Monica, Calif.: RAND Corporation, PE-231-A, 2017.

Page 404 of 3957

Russian gray zone activities could turn into a cost-imposing strategy that distracts the West from the main competition. If NATO wants to deter Russian aggression, whether it uses gray zone tactics or not, it should put in place sufficient military capabilities to stop Russia from quickly achieving its objectives when the gray zone threatens to turn red.

Russia's gray zone tactics will persist and should be countered by hardening Western societies against Russian propaganda and its disinformation and attempts to undermine democracy. However, overreaction only serves Moscow's purposes. Strong civil societies and robust democratic institutions, not panic at "losing" or attempts to fight Russia blow-by-blow, are the West's best defenses against Russia's gray zone tactics. Russia's gray zone tactics signify its weakness, and the West's stronger political, cultural, and social systems will prevail over them if given the chance.

APPENDIX

Wargaming the Gray Zone

The research documented in this report is drawn from a series of war games developed and conducted to explore a gray zone competition in Europe. These games were held between October 2016 and December 2017 and played by SMEs in Europe, Russia, and the United States.

Three distinct strategic political-military games were designed to conduct this research. The first game was a loosely structured argument-based matrix game and the next two games were card-driven games that differed in structure. All three games allowed players to take actions across different domains, with an emphasis on information, economic, military, and political-social actions. The scope of these games was varied as well, with the first two games allowing for free play within Europe and the last game limited to the Western Balkans. This final game built on the previous two games and incorporated insights derived from the earlier exercises to develop a tightly scoped and structured strategic level card-driven game.

The loose structure and seminar-style nature of the matrix game proved to be ill-suited to representing the nature of a gray zone competition, but helped us to identify key issues that merited further exploration. Because the variety of possible gray zone activities seemed limitless, the players were overwhelmed by the choices. Without a gaming platform to bound and focus the discussion, the players tended to fixate on covert tactical actions instead of the strategic competition. We initially attempted to provide more structure through simply adding cards that served as a menu for Blue, Red, and Green actions, but this proved disappointing as well, because it did not provide the players with the appropriate level of strategic feedback about the outcomes of their decisions. Free play within all of Europe further compounded the

Page 406 of 3957

Page 407 of 3957

problem because unconstrained geography impeded the players' efforts to develop a strategy and resulted in a deluge of unconnected actions that inundated the adjudicators and interfered with learning.

Ultimately, we developed a three-sided card-driven board game focused on Russian, American, and European gray zone actions in the Western Balkans. At first blush, our gray zone game looks similar to commercial games, such as Twilight Struggle.[1] The game consists of two game boards (seen in Figures A.1 and A.2)—a game timeline where players made their short- and long-term actions by laying down their cards, and the other illustrating the state of play in the Balkans, including key country-level information and larger metrics of success, including NATO unity and Russian regime stability.

Cards provide a starting menu of actions that the Russia, Europe, and U.S. teams could play overtly or covertly (i.e., playing the card face-down) on the game timeline board. In spite of this structure, the gray zone game was also constructed to maximize its flexibility so that the players could amend the provided cards, create new cards, and develop their own narrative by expanding on the cards and overtly messaging to partners and adversaries alike. Adjudication of these actions used a simple model that reflected our best understanding of how and why gray zone tactics succeed or fail. To inform the development of this model, we surveyed the empirical record on Russian gray zone tactics and the existing literature on the individual actions that are considered to be a part of gray zone activities (e.g., information warfare, covert action). Based on this literature and SME elicitation, we created combat results tables and probabilistically assigned outcomes to different gray zone tactics. The purpose of the structured adjudication, however, was not to predict what could or will happen in the real world. Rather, it is to focus the discussion and to allow for the systematic exploration of Red gray zone actions and Blue and Green countermeasures. Moreover, with the exception of covert actions, adjudication was done transparently, so the players could understand the outcomes and argue with the control team if the adjudication seemed off. If the white cell, or game adjudicators, were persuaded by these arguments, they would amend the rules in real time.

[1] Ananda Gupta and Jason Matthews, *Twilight Struggle*, GMT Games, 2015.

Page 407 of 3957

Figure A.1
Gray Zone Timeline Board

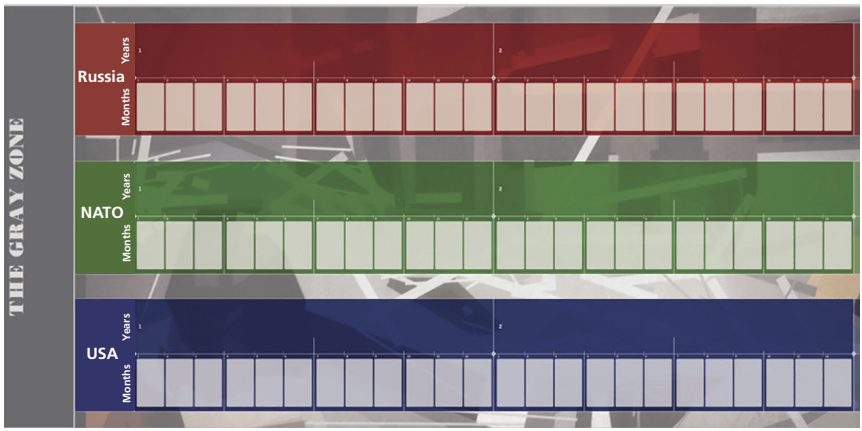
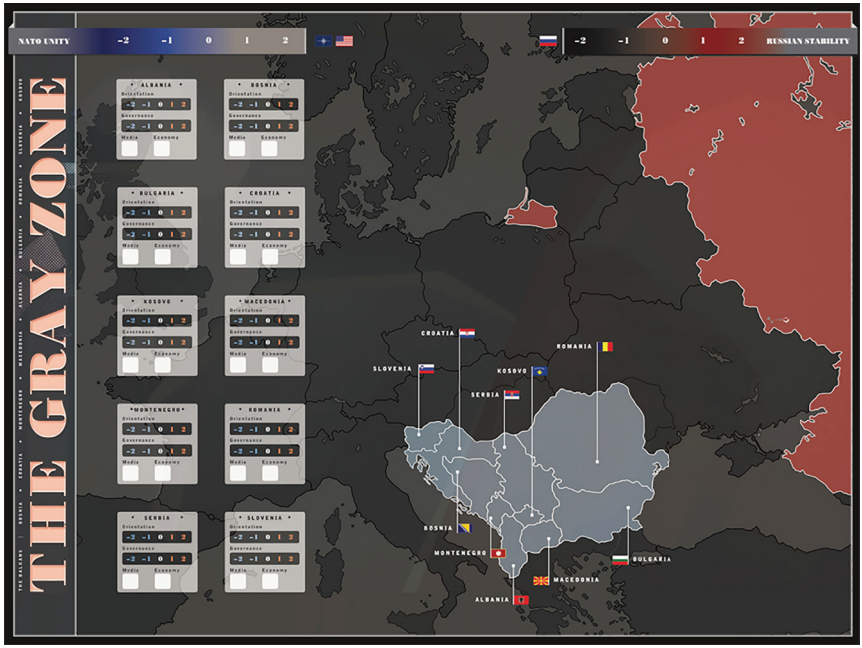


Figure A.2
Main Gray Zone Game Board



References

Adamsky, Dmitry, *Cross-Domain Coercion: The Current Russian Art of Strategy*, Proliferation Papers, No. 54, IFRI Security Studies Center, November 2015. As of July 30, 2018:
https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

Arbutina, Zoran, "Balkan Countries See Rise in Hate Speech," *Deutsche Welle*, February 24, 2017. As of July 25, 2018:
http://www.dw.com/en/balkan-countries-see-rise-in-hate-speech/a-37711134

Asymmetric Operations Working Group, *Ambiguous Threats and External Influences in the Baltic States*, *Phase 2: Assessing the Threat*, Ft. Meade, Md.: U.S. Army Asymmetric Warfare Group, Johns Hopkins Applied Physics Laboratory, November 2015.

Baker, Mark, "Drinking Games," *Foreign Policy*, July 29, 2015. As of July 31, 2018:
https://foreignpolicy.com/2015/07/29/
drinking-games-moldova-russia-eu-wine-embargo/

Barnes, Julian E., "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attacks," *New York Times*, July 13, 2018. As of July 31, 2018:
https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html

Barno, David, and Nora Bensahel, "Fighting and Winning in the 'Gray Zone,'" *War on the Rocks,* May 19, 2015. As of July 25, 2018:
https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/

Beaulieu, Brittany, and David Salvo, "NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence," GMF Alliance for Securing Democracy, Policy Brief, No. 031, 2018. As of July 31, 2018:
https://securingdemocracy.gmfus.org/wp-content/uploads/2018/07/NATO-and-Asymmetric-Threats.pdf

Belford, Audrey, Saska Cvetkovska, Biljana Sekulovska, and Stevan Dojçinovic, "Leaked Documents Show Russian, Serbian Attempts to Meddle in Macedonia," OCCRP, Spooks and Spin in the Balkans, blog post, June 4, 2017.

Page 411 of 3957

Bergmann, Max, and Carolyn Kenney, *War by Other Means*, Washington, D.C.: Center for American Progress, June 6, 2017. As of July 25, 2018: https://www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/

Berzina, Ieva, "Russia's Compatriot Policy in the Nordic-Baltic Region," in *Russia's Footprint in the Nordic-Baltic Information Environment*, Report 2016/1027, Riga, Latvia: NATO Strategic Communications Centre of Excellence, January 2018, pp. 31–56.

Borger, Julian, "Russian-Trained Mercenaries Back Bosnia's Serb Separatists," *The Guardian*, January 12, 2018. As of July 25, 2018: https://www.theguardian.com/world/2018/jan/12/russian-trained-mercenaries-back-bosnias-serb-separatists

Boston, Scott, and Dara Massicot, *The Russian Way of Warfare: A Primer*, Santa Monica, Calif.: RAND Corporation, PE-231-A, 2017. As of July 31, 2018: https://www.rand.org/pubs/perspectives/PE231.html

Brands, Hal, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, February 5, 2016. As of July 25, 2018: https://www.fpri.org/article/2016/02/paradoxes-gray-zone

Burgess, Matt, "Here's the First Evidence Russia Used Twitter to Influence Brexit," *Wired*, November 10, 2017. As of July 25, 2018: http://www.wired.co.uk/article/brexit-russia-influence-twitter-bots-internet-research-agency

Charap, Samuel, "The Ghost of Hybrid War," *Survival*, Vol. 57, No. 6, December 2015–January 2016, pp. 51–58.

Chazan, David, "Russia 'Bought' Marine Le Pen's Support over Crimea," *The Telegraph*, April 4, 2015. As of July 25, 2018: https://www.telegraph.co.uk/news/worldnews/europe/france/11515835/Russia-bought-Marine-Le-Pens-support-over-Crimea.html

Chekinov, S. G., and S. A. Bogdanov, "Asimmetrichnyye mery po obespecheniyu voyennoy bezopasnosti Rossii [Asymmetrical Actions to Ensure Russia's Military Security]," *Voyennaya mysl' [Military Thought]*, No. 3, 2010, pp. 46–53.

Chivvis, Christopher S., *Understanding Russian 'Hybrid Warfare' and What Can Be Done About it Addendum*, testimony before the U.S. House of Representatives Armed Services Committee, Washington, D.C., March 22, 2017.

Coats, Daniel R., "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 13, 2018. As of July 31, 2018: https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community

Page 411 of 3957

Cohen, Ariel, and Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications*, Carlisle, Pa.: Strategic Studies Institute, June 2011.

Cohen, Raphael S., and Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat*, Santa Monica, Calif.: RAND Corporation, RR-1793-A, 2019. As of October 2, 2019: https://www.rand.org/pubs/research_reports/RR1793.html

Connell, Mary E., and Ryan Evans, *Russia's 'Ambiguous Warfare' and Implications for the U.S. Marine Corps*, Arlington, Va.: CNA, May 2015.

"Countering 'Hybrid' Security Threats a Priority, Says EU," *EUbusiness*, July 19, 2017. As of July 31, 2018: https://www.eubusiness.com/news-eu/hybrid-threats.19xd/

Crosby, Alan, "Here Are the Flashpoints You Should Be Watching in the Balkans," Radio Free Europe/Radio Liberty, April 28, 2017. As of July 31, 2018: https://www.rferl.org/a/balkans-flashpoint-to-watch-macedonia-serbia-kosovo-montenegro-bosnia/28456971.html

Curry, John, and Tim Price, *Matrix Games for Modern Wargaming: Developments in Professional and Educational Wargames Innovations in Wargaming*, Vol. 2, Barking, UK: Lulu Press, Inc., August 2014.

Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe," *Wired,* August 21, 2007. As of July 25, 2018: https://www.wired.com/2007/08/ff-estonia/

Devitt, Polina, "Russia Bans Polish Fruit and Vegetable in Apparent Retaliation for Sanctions," Reuters, July 30, 2014. As of July 31, 2018: https://www.reuters.com/article/us-europe-russia-trade-poland/russia-bans-polish-fruit-and-vegetable-in-apparent-retaliation-for-sanctions-idUSKBN0FZ12220140730

Economist Intelligence Unit, "Russia's Role in the Western Balkans," webpage, October 18, 2017. As of July 31, 2018: http://country.eiu.com/article.aspx?articleid=946003478&Country=Montenegro&topic=Politics&subtopic=Forecast&subsubtopic=International+relations

Elkus, Adam, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense," *War on the Rocks*, December 15, 2015. As of July 25, 2018: https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/

European Union External Action Service, *Joint Communication: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*, Brussels, June 13, 2018. As of July 31, 2018: https://eeas.europa.eu/headquarters/headquarters-homepage/46397/joint-communication-increasing-resilience-and-bolstering-capabilities-address-hybrid-threats_en

Fund for Peace, "Fragile States Index," webpage, 2019. As of October 15, 2019: https://fragilestatesindex.org/

Galeotti, Mark, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadow*, blog post, July 6, 2014. As of July 25, 2018: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

———, "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's New Way of War?" *Small Wars and Insurgencies*, Vol. 27, No. 2, 2016, pp. 282–301. As of July 30, 2018: https://www.tandfonline.com/doi/full/10.1080/09592318.2015.1129170

———, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*, London: European Council on Foreign Relations, April 2017. As of July 31, 2018: https://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe

———, "An Unusual Friendship: Bikers and the Kremlin," *Moscow Times*, May 19, 2015. As of July 31, 2018: https://themoscowtimes.com/articles/an-unusual-friendship-bikers-and-the-kremlin-op-ed-46671

Gerasimov, Valery, "Znacheniye nauki nakhoditsya v predvidenii: novyye vyzovy trebuyut pereosmysleniya form i metodov vedeniya boyevykh deystviy [The Value of Science Is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations]," *Voyenno-Promyshlennyy Kuryer [Military Courier]*, February 26, 2013.

Goltz, Thomas, "Letter from Eurasia: The Hidden Russian Hand," *Foreign Policy,* No. 92, Autumn 1993, pp. 92–116.

Greenberg, Andy, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure,'" *Wired,* May 9, 2017. As of July 25, 2018: https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

Greenslade, Roy, "Journalists Covering the Ukraine Crisis Suffer Intimidation," *The Guardian*, July 23, 2014. As of July 25, 2018: https://www.theguardian.com/media/greenslade/2014/jul/23/journalist-safety-ukraine

Grigas, Agnia, "How Soft Power Works: Russian Passportization and Compatriot Policies Paved Way for Crimean Annexation and War in Donbas," Atlantic Council, webpage, February 22, 2016. As of July 24, 2018: http://www.atlanticcouncil.org/blogs/ukrainealert/how-soft-power-works-russian-passportization-and-compatriot-policies-paved-way-for-crimean-annexation-and-war-in-donbas

Groll, Elias, "A Brief History of Attempted Russian Assassinations by Poison," *Foreign Policy*, March 9, 2018. As of July 25, 2018: https://foreignpolicy.com/2018/03/09/a-brief-history-of-attempted-russian-assassinations-by-poison/

Gupta, Ananda, and Jason Matthews, *Twilight Struggle*, GMT Games, 2015.

Harris, Kira, "Russia's Fifth Column: The Influence of the Night Wolves Motorcycle Club," *Studies in Conflict and Terrorism*, 2018.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, RR-2237-OSD, 2018. As of July 25, 2018: https://www.rand.org/pubs/research_reports/RR2237.html

Herszenhorn, David M., "Crimea Votes to Secede from Ukraine as Russian Troops Keep Watch," *New York Times*, March 16, 2014. As of July 31, 2018: https://www.nytimes.com/2014/03/17/world/europe/crimea-ukraine-secession-vote-referendum.html

Higgins, Andrew, "Russian Money Suspected Behind Fracking Protests," *New York Times*, November 30, 2014. As of July 31, 2018: https://www.nytimes.com/2014/12/01/world/russian-money-suspected-behind-fracking-protests.html

———, "In Expanding Russian Influence, Faith Combines with Firepower," *New York Times*, September 13, 2016a. As of July 24, 2018: https://www.nytimes.com/2016/09/14/world/europe/russia-orthodox-church.html

———, "In Russia's 'Frozen Zone,' a Creeping Border with Georgia," *New York Times*, October 23, 2016b. As of July 31, 2018: https://www.nytimes.com/2016/10/24/world/europe/in-russias-frozen-zone-a-creeping-border-with-georgia.html

———, "Russia's Feared 'Night Wolves' Bike Gang Came to Bosnia. Bosnia Giggled," *New York Times*, March 31, 2018. As of July 24, 2018: https://www.nytimes.com/2018/03/31/world/europe/balkans-russia-night-wolves-republika-srpska-bosnia.html

Higgins, Andrew, Michael R. Gordon, and Andrew E. Kramer, "Photos Link Masked Men in East Ukraine to Russia," *New York Times*, April 20, 2014. As of July 25, 2018: https://www.nytimes.com/2014/04/21/world/europe/photos-link-masked-men-in-east-ukraine-to-russia.html

Hoellerbauer, Simon, "Baltic Energy Sources: Diversifying Away from Russia," Foreign Policy Research Institute, June 14, 2017. As of July 25, 2018: https://www.fpri.org/article/2017/06/baltic-energy-sources-diversifying-away-russia/

Hoffman, Frank, "On Not-So-New Warfare: Political Warfare vs Hybrid Threats," *War on the Rocks,* July 28, 2014. As of July 30, 2018: https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/

———, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," in Dakota L. Wood, ed., *2016 Index of Military Strength: Assessing America's Ability to Provide for the Common Defense*, Washington, D.C.: Heritage Foundation, 2015, pp. 25–36.

Holcomb, Franklin, *The Kremlin's Irregular Army: Ukrainian Separatist Order of Battle*, Russia and Ukraine Security Report 3, Washington, D.C.: Institute for the Study of War, September 2017. As of July 31, 2018: http://www.understandingwar.org/backgrounder/kremlin%E2%80%99s-irregular-army-ukrainian-separatist-order-battle

Holland, Emily, and Rebecca Friedman Lissner, "Countering Russian Influence in the Balkans," *Lawfare*, August 6, 2017. As of July 25, 2018: https://www.lawfareblog.com/countering-russian-influence-balkans

Hope, Kerin, "Russia Meddles in Greek Town to Push Back the West," *Financial Times*, July 13, 2018. As of July 30, 2018: https://www.ft.com/content/b5728090-86b0-11e8-96dd-fa565ec55929

"In U.N. Lawsuit, Ukraine Demands Russia End Support for Separatists," Reuters, January 17, 2017. As of July 24, 2018: https://www.reuters.com/article/us-ukraine-crisis-russia-court-idUSKBN1511EU

Indictment, *United States of America v. Internet Research Agency,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018). As of July 31, 2018: https://www.justice.gov/file/1035477/download

Indictment, *United States of America v. Viktor Borisovich Netyksho*, Case 1:18-cr-00215-ABJ (D.D.C. July 13, 2018). As of July 31, 2018: https://www.justice.gov/file/1080281/download

"IRI's Center for Insights Poll: Crises in Europe and EU Leave Serbs Turning Toward Russia," International Republican Institute, December 2016. As of July 25, 2018: http://www.iri.org/resource/iri%E2%80%99s-center-insights-poll-crises-europe-and-eu-leave-serbs-turning-toward-russia

Jackson, Van, "Tactics of Strategic Competition: Gray Zones, Redlines, and Conflicts Before War," *Naval War College Review*, Vol. 70, No. 3, Summer 2017, pp. 39–61.

Johnson, Keith, "Russia's Quiet War Against European Fracking," *Foreign Policy*, June 2014. As of July 31, 2018: https://foreignpolicy.com/2014/06/20/russias-quiet-war-against-european-fracking/

Jolkina, Alexandra, and Markian Ostaptschuk, "Activists or Kremlin Agents—Who Protects Russian-Speakers in the Baltics?" *Deutsche Welle*, December 9, 2015. As of July 25, 2018:
https://www.dw.com/en/activists-or-kremlin-agents-who-protects-russian-speakers-in-the-baltics/a-18903695

Jones, Sam, "Estonia Ready to Deal with Russia's 'Little Green Men,'" *Financial Times*, May 13, 2015. As of July 31, 2018:
https://www.ft.com/content/03c5ebde-f95a-11e4-ae65-00144feab7de

Jones, Sam, Guy Chazan, and Christian Oliver, "NATO Claims Moscow Funding Anti-Fracking Groups," *Financial Times*, June 19, 2014. As of July 31, 2018:
https://www.ft.com/content/20201c36-f7db-11e3-baf5-00144feabdc0

Jordans, Frank, "European Spy Chiefs Warn of Hybrid Threats from Russia, IS," Associated Press, May 14, 2018. As of July 31, 2018:
https://apnews.com/65c1a2a9ca0d46ac9ff77efe38c8fbba

Joyce, Stephanie, "Along a Shifting Border, Georgia and Russia Maintain an Uneasy Peace," National Public Radio, March 13, 2017. As of July 24, 2018:
https://www.npr.org/sections/parallels/2017/03/13/519471110/along-a-shifting-border-georgia-and-russia-maintain-an-uneasy-peace

Kaljula, Diana, and Ivo Juurvee, "Narratives About the Nordic-Baltic Countries Promoted by Russia," in *Russia's Footprint in the Nordic-Baltic Information Environment*, Report 2016/1027, Riga, Latvia: NATO Strategic Communications Centre of Excellence, January 2018, pp. 57–78.

Kavanagh, Jennifer, and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica, Calif.: RAND Corporation, RR-2314-RC, 2018. As of July 25, 2018:
https://www.rand.org/pubs/research_reports/RR2314.html

Kennan, George, "George F. Kennan on Organizing Political Warfare [Redacted Version]," Wilson Center Digital Archive, April 30, 1948. As of July 31, 2018:
https://digitalarchive.wilsoncenter.org/document/114320

Kofman, Michael, "Fixing NATO Deterrence in the East Or: How I Stopped Worrying and Love NATO's Crushing Defeat by Russia," *War on the Rocks,* May 12, 2016. As of July 25, 2018:
https://warontherocks.com/2016/05/fixing-nato-deterrence-in-the-east-or-how-i-learned-to-stop-worrying-and-love-natos-crushing-defeat-by-russia/

———, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016. As of July 25, 2018:
https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/

———, "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," *War on the Rocks*, June 14, 2018. As of July 31, 2018:
https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition/

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Oleysa Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Santa Monica, Calif.: RAND Corporation, RR-1498-A, 2017. As of July 25, 2018:
https://www.rand.org/pubs/research_reports/RR1498.html

Kofman, Michael, and Matthew Rojansky, "A Closer Look at Russia's 'Hybrid War,'" *Kennan Cable,* No. 7, April 2015. As of July 25, 2018:
https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf

Kogan, Rami, "Bedep Trojan Malware Spread by the Angler Exploit Kit Gets Political," *SpiderLabs Blog*, April 29, 2015. As of July 23, 2017:
https://www.trustwave.com/Resources/SpiderLabs-Blog/Bedep-trojan-malware-spread-by-the-Angler-exploit-kit-gets-political/

Kragh, Martin, and Sebastian Asberg, "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: the Swedish Case," *Journal of Strategic Studies,* Vol. 40, No. 6, 2017, pp. 773–816.

Kucera, Joshua, "U.S. Intelligence: Russia Sabotaged BTC Pipeline Ahead of 2008 Georgia War," *EurasiaNet*, December 10, 2015. As of July 25, 2018:
https://eurasianet.org/us-intelligence-russia-sabotaged-btc-pipeline-ahead-of-2008-georgia-war

Lanoszka, Alexander, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs*, Vol. 92, No. 1, 2016, pp. 175–195.

Lasheras, Francisco de Borja, Vessela Tcherneva, and Fredrik Wesslau, *Return to Instability: How Migration and Great Power Politics Threaten the Western Balkans,* London: European Council on Foreign Affairs, March 2016.

Lee, Dave, "The Tactics of a Russian Troll Farm," BBC News, February 16, 2018. As of July 25, 2018:
https://www.bbc.com/news/technology-43093390

"Libya, Migrants & Karma: Europe's New Migration Policy Wrecks on North African Reality," *RT*, July 22, 2018. As of July 30, 2018:
https://www.rt.com/news/433969-europe-refugee-crisis-migrants-libya/

Losh, Jack, "Putin's Angels: The Bikers Battling for Russia in Ukraine," *The Guardian*, January 29, 2016. As of July 31, 2018:
https://www.theguardian.com/world/2016/jan/29/russian-biker-gang-in-ukraine-night-wolves-putin

Lutonvinov, Vi, "I ispol'zovanie nevoennykh razvitie mer dlia ukrepleniia voennoi bezopasnosti Rossiiskoi Federatsii [The Use of Nonmilitary Development Measures to Strengthen the Military Security of the Russian Federation]," *Voennaia mysl' [Military Thought]*, No. 5, May 2009, pp. 2–12.

Page 418 of 3957

Lutsevych, Orysia, *Agents of the Russian World: Proxy Groups in the Contested Neighborhood*, London: Chatham House, Royal Institute of International Affairs, April 2016. As of July 31, 2018:
https://www.chathamhouse.org/publication/agents-russian-world-proxy-groups-contested-neighbourhood

Lyman, Rick, "Bulgaria Grows Uneasy as Trump Complicates Its Ties to Russia," *New York Times*, February 4, 2017. As of July 25, 2018:
https://www.nytimes.com/2017/02/04/world/europe/bulgaria-trump-russia-putin.html

MacDowall, Andrew, "Chevron's Bulgaria Pull-Out a Blow for Energy Security," *Financial Times,* June 11, 2014. As of July 31, 2018:
https://www.ft.com/content/347a30d3-d240-3a1b-9d7d-b07190dd90d3

Maigre, Merle, *Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO*, German Marshall Fund of the United States, February 2015.

Mallonee, Laura, "Meet the People of a Soviet Country That Doesn't Exist," *Wired*, March 7, 2016. As of July 31, 2018:
https://www.wired.com/2016/03/meet-people-transnistria-stuck-time-soviet-country-doesnt-exist/

Mazarr, Michael J., *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Carlisle, Pa.: Strategic Studies Institute and U.S. Army War College Press, December 2015.

McGuinness, Damien, "How a Cyber Attack Transformed Estonia," BBC News, April 27, 2017. As of July 25, 2018:
http://www.bbc.com/news/39655415

Meakins, Joss, "Why Russia Is Far Less Threatening Than It Seems," *Washington Post*, March 8, 2017. As of July 31, 2018:
https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/08/why-russia-is-far-less-threatening-than-it-seems/?utm_term=.9a6342e955b6

"Montenegro Begins Trial of Alleged Pro-Russian Coup Plotters," Reuters, July 19, 2017. As of July 24, 2018:
https://www.reuters.com/article/us-montenegro-election-trial/montenegro-begins-trial-of-alleged-pro-russian-coup-plotters-idUSKBN1A413F

National Cyber Security Centre, UK Government Communications Headquarters, "Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber-Attack," February 15, 2018. As of July 30, 2018:
https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

Page 418 of 3957

NATO Communications and Information Agency, *Balkan Regional Approach to Air Defence (BRAAD)*, Brussels: North Atlantic Treaty Organization, undated. As of July 31, 2018:
https://www.ncia.nato.int/Documents/Agency%20publications/Balkan%20Regional%20Approach%20to%20Air%20Defence%20(BRAAD).pdf

Orttung, Robert, and Christopher Walker, "Putin's Frozen Conflicts," *Foreign Policy*, February 13, 2015. As of July 24, 2018:
https://foreignpolicy.com/2015/02/13/putins-frozen-conflicts/

Pallin, Caroline V., and Fredrik Westerlund, "Russia's War in Georgia: Lessons and Consequences," *Small Wars and Insurgencies*, Vol. 20, No. 2, 2009, pp. 400–424.

Paul, Christopher, and Miriam Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016. As of July 25, 2018:
https://www.rand.org/pubs/perspectives/PE198.html

Petersen, Michael, "The Perils of Conventional Deterrence by Punishment," *War on the Rocks*, November 11, 2016. As of July 31, 2018:
https://warontherocks.com/2016/11/the-perils-of-conventional-deterrence-by-punishment/

Pew Research Center, *Religious Belief and National Belonging in Central and Eastern Europe,* May 10, 2017. As of July 25, 2018:
http://www.pewforum.org/2017/05/10/religious-belief-and-national-belonging-in-central-and-eastern-europe/

Polyakova, Alina, and Spencer Phipps Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Washington, D.C.: Brookings Institution, March 2018. As of July 30, 2018:
https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/

Racz, Andras, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, FIIA Report 43, Helsinki, Finland: Finnish Institute of International Affairs, 2015.

Radin, Andrew, *Hybrid Warfare in the Baltics: Threats and Potential Responses*, Santa Monica, Calif.: RAND Corporation, RR-1577-AF, 2017. As of July 25, 2018:
https://www.rand.org/pubs/research_reports/RR1577.html

Radin, Andrew, and Clint Reach, *Russian Views of the International Order*, Santa Monica, Calif.: RAND Corporation, RR-1826-OSD, 2017. As of July 25, 2018:
https://www.rand.org/pubs/research_reports/RR1826.html

Romerstein, Herbert, "Disinformation as a KGB Weapon in the Cold War," *Journal of Intelligence History*, Vol. 1, No. 1, 2001, pp. 54–67.

Rosner, Thomas, "The Western Balkans: A Region of Secessions," *Deutsche Welle*, October 4, 2017. As of July 31, 2018: https://www.dw.com/en/the-western-balkans-a-region-of-secessions/a-40793126

Roth, Andrew, "A Separatist Militia in Ukraine with Russian Fighters Holds a Key," *New York Times*, June 4, 2014a. As of July 31, 2018: https://www.nytimes.com/2014/06/05/world/europe/in-ukraine-separatist-militia-with-russian-fighters-holds-a-key.html

———, "From Russia, 'Tourists' Stir the Protests," *New York Times,* March 3, 2014b. As of July 25, 2018: https://www.nytimes.com/2014/03/04/world/europe/russias-hand-can-be-seen-in-the-protests.html

Russell, Martin, *At a Glance: Russia in the Western Balkans*, European Parliament Members' Research Service, July 2017. As of July 31, 2018: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA%282017%29608627

"Russia's Sberbank to Get 40 Pct of Croatia's Agrokor After Debt Conversion," Reuters, June 8, 2018. As of July 24, 2018: https://www.reuters.com/article/croatia-agrokor-sberbank/russias-sberbank-to-get-40-pct-of-croatias-agrokor-after-debt-conversion-idUSR4N1T800E

Russkiy Mir Foundation, "Russian Centers of the Russkiy Mir Foundation," webpage, undated. As of October 15, 2019: https://russkiymir.ru/en/rucenter/

Schadlow, Nadia, "The Problem with Hybrid Warfare," *War on the Rocks,* April 2, 2015. As of July 28, 2015: https://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/

Scharre, Paul, "American Strategy and the Six Phases of Grief," *War on the Rocks,* October 6, 2016. As of July 25, 2018: https://warontherocks.com/2016/10/american-strategy-and-the-six-phases-of-grief/

Schelling, Thomas C., *Arms and Influence*, New Haven, Conn.: Harvard University Press, 1966.

Schoen, Fletcher, and Christopher Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Washington, D.C.: Institute for National Strategic Studies, June 2012.

Seddon, Max, and Michael Stothard, "Putin Awaits Return on Le Pen Investment," *Financial Times*, May 4, 2017. As of July 31, 2018: https://www.ft.com/content/010eec62-30b5-11e7-9555-23ef563ecf9a

Shlapak, David A., *The Russia Challenge*, Santa Monica, Calif.: RAND Corporation, PE-250-A, 2018. As of July 31, 2018: https://www.rand.org/pubs/perspectives/PE250.html

Page 421 of 3957

Shlapak, David A., and Michael W. Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics*, Santa Monica, Calif.: RAND Corporation, RR-1253-A, 2016. As of July 25, 2018: https://www.rand.org/pubs/research_reports/RR1253.html

Shuster, Simon, "How Russian Voters Fueled the Rise of Germany's Far-Right," *Time*, September 25, 2017. As of July 30, 2018: http://time.com/4955503/germany-elections-2017-far-right-russia-angela-merkel/

Singer, Peter W., "What We Didn't Learn from Twitter's News Dump on Russiagate," *Defense One*, January 20, 2018. As of July 25, 2018: http://www.defenseone.com/ideas/2018/01/twitter-and-russiagate-takeaways-friday-news-dump/145342/

Spruds, Andris, Anda Rozukaine, Klavs Sedlenieks, Martins Daugulis, Diana Potjomkina, Beatrix Tolgyesi, and Ilvija Brug, *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, July 2015.

Szwed, Robert, *Framing of the Ukraine-Russia Conflict in Online and Social Media*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, January 2018.

Tabor, Damon, "Putin's Angels: Inside Russia's Most Infamous Motorcycle Club," *Rolling Stone*, October 8, 2015. As of July 31, 2018: https://www.rollingstone.com/culture/culture-news/putins-angels-inside-russias-most-infamous-motorcycle-club-56360/

Trenin, Dmitri V., *Post-Imperium: A Eurasian Story*, Washington, D.C.: Carnegie Endowment for International Peace, 2011.

Treverton, Gregory F., Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats,* Stockholm: Swedish Defence University, European Center of Excellence for Countering Hybrid Threats, May 9, 2018. As of July 30, 2018: https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf

U.S. Senate, *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel II: Hearing Before the Select Committee on Intelligence of the United States Senate*, Washington, D.C.: U.S. Government Publishing Office, March 30, 2017.

———, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, minority staff report, Committee on Foreign Relations, Washington, D.C.: U.S. Government Publishing Office, January 10, 2018.

U.S. Special Operations Command, *The Gray Zone*, September 9, 2015.

Page 421 of 3957

"UPDATE 3-Russia Raises Gas Prices for Ukraine by 80 Percent," Reuters, April 3, 2014. As of July 24, 2018: https://www.reuters.com/article/ukraine-crisis-gas-idUSL5N0MV2WL20140403

Ven Bruusgaard, Kristen, "Crimea and Russia's Strategic Overhaul," *Parameters*, Vol. 44, No. 3, Autumn 2014, pp. 81–90.

Von Der Burchard, Hans, "EU Takes Billion-Euro Battle to Russia," *Politico,* January 10, 2018. As of July 31, 2018: https://www.politico.eu/article/russia-sanctions-europe-trade-eu-takes-billion-euro-battle/

Votel, Joseph L., "Statement of General Joseph L. Votel, U.S. Army Commander, United States Special Operations Command Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities," March 18, 2015. As of July 25, 2018: http://docs.house.gov/meetings/AS/AS26/20150318/103157/HMTG-114-AS26-Wstate-VotelUSAJ-20150318.pdf

Vukicevic, Jasna, and Robert Coalson, "Russia's Friends Form New 'Cossak Army' in Balkans," Radio Free Europe/Radio Liberty, October 18, 2016. As of July 30, 2018: https://www.rferl.org/a/balkans-russias-friends-form-new-cossack-army/28061110.html

Wasser, Becca, Jenny Oberholtzer, Stacie L. Pettyjohn, and William Mackenzie, *Gaming the Gray Zone: Observations from Designing a Structured Gray Zone Strategy Game*, Santa Monica, Calif.: RAND Corporation, RR-2915-A, 2019. As of November 14, 2019: https://www.rand.org/pubs/research_reports/RR2915.html

Watson, Ivan, and Sebastian Shukla, "Russian Fighter Jets 'Buzz' US Warship in Black Sea, Photos Show," CNN, February 16, 2017. As of July 24, 2018: https://www.cnn.com/2017/02/16/us/russia-us-ship-fly-by/index.html

Wiggins, Warren, *War Game Adjudication: Adjudication Styles*, Newport, R.I.: United States Naval War College, 2014.

Willsher, Kim, and Jon Henley, "Emmanuel Macron's Campaign Hacked on Eve of French Election," *The Guardian*, May 6, 2017. As of July 25, 2018: https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election

World Bank Group, "Worldwide Governance Indicators," webpage, 2019. As of October 15, 2019: https://info.worldbank.org/governance/wgi/#home

Zakem, Vera, Bill Rosenau, and Danielle Johnson, *Shining a Light on the Western Balkans: Internal Vulnerabilities and Malign Influence from Russia, Terrorism, and Transnational Organized Crime*, Arlington, Va.: CNA, May 2017.

Zakem, Vera, Paul Saunders, Umida Hashimova, and P. Kathleen Hammerberg, *Mapping Russian Media Network: Media's Role in Russian Foreign Policy and Decision-Making*, Arlington, Va.: CNA, January 2018.

Zgut, Edit, "Hungary's Pro-Kremlin Far Right Is a Regional Security Threat," *EU Observer*, December 23, 2016. As of July 30, 2018: https://euobserver.com/opinion/136354

99TH CONGRESS
2d Session

SENATE

REPORT
99-522

MEETING THE ESPIONAGE CHALLENGE: A REVIEW OF UNITED STATES COUNTERINTELLIGENCE AND SECURITY PROGRAMS

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE

OCTOBER 3 (legislative day, SEPTEMBER 23), 1986.—Ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE
64-268 O WASHINGTON · 1986

SENATE SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

DAVE DURENBERGER, Minnesota, *Chairman*
PATRICK J. LEAHY, Vermont, *Vice Chairman*

WILLIAM V. ROTH, JR., Delaware
WILLIAM S. COHEN, Maine
ORRIN HATCH, Utah
FRANK MURKOWSKI, Alaska
ARLEN SPECTER, Pennsylvania
CHIC HECHT, Nevada
MITCH McCONNELL, Kentucky

LLOYD BENTSEN, Texas
SAM NUNN, Georgia
THOMAS F. EAGLETON, Missouri
ERNEST F. HOLLINGS, South Carolina
DAVID L. BOREN, Oklahoma
BILL BRADLEY, New Jersey

ROBERT DOLE, Kansas, *Ex Officio*
ROBERT C. BYRD, West Virginia, *Ex Officio*

BERNARD F. MCMAHON, *Staff Director*
ERIC D. NEWSOM, *Minority Staff Director*
DORTHEA ROBERTSON, *Clerk*

Page 425 of 3957

CONTENTS

	Page
I. Introduction and Summary	1
A. Background	1
B. Organization of the U.S. Government to Meet the Hostile Intelligence Challenge	3
C. Counterintelligence: Learning the Lessons of Recent Cases	4
D. Security Countermeasures: Defending on Many Fronts	6
E. Budgetary Impact	9
F. Legislative Proposals	10
G. Respect for Individual Rights	11
II. The Hostile Intelligence Threat	12
A. Damage to National Security	12
B. Sources of the Threat	17
1. Soviet Union	17
2. Warsaw Pact and Cuba	18
3. People's Republic of China	19
4. Other Countries	20
C. Human Intelligence Techniques	20
1. Official Presence	21
2. Other Aspects of the Hostile Intelligence Presence	23
3. Recruited Agents	25
4. Soviet Methods of Recruitment	26
5. Technology Transfer	28
6. Active Measures and Disinformation	30
D. Technical Collection Operations	33
1. Interception of Communications	33
2. Other Forms of Electronic Surveillance	34
3. Penetration of Computer Systems	35
4. Imagery	36
E. Summary	37
III. Counterintelligence	38
A. Need for a Counterintelligence Strategy	39
B. Hostile Presence Limits	40
C. Counterintelligence Awareness Programs	45
D. Domestic Operations	48
1. Coverage of Establishments and Officers	49
2. Offensive Operations	50
3. Espionage Investigations and Prosecutions	52
E. Overseas Operations	56
F. Personnel Management and Training	56
IV. Security Countermeasures	58
A. A National Strategic Security Program	59
B. Personnel Security	65
C. Information Security	74
D. Communications, Computer and Emanations Security	80
E. Technical and Physical Security	85
F. Industrial Security	87
G. Congressional Security	90
V. Appendixes	97
Appendix A. *U.S.* v. *Whitworth*, Affidavit of RADM William O. Studeman and Declaration of John L. Martin	97
Appendix B. Defense Security Institute Analysis of the Harper Case	105
Appendix C. Defense Security Institute Analysis of the Bell/Zacharski Case	112

Page 426 of 3957

Page

Appendix D. Defense Security Institute Analysis of the Cavanagh Case 126
Appendix E. *U.S.* v. *Zakharov,* Affidavit for an Arrest Warrant and Search Warrant; and Indictment 136
Appendix F. Forged letter from Herbert Romerstein to Senator David Durenberger; actual letter from Romerstein to LTG Robert L. Schweitzer; and forged letter from LTG Schweitzer to President Augusto Pinochet of Chile 142
Appendix G. Draft Senate Security Manual 146

99TH CONGRESS 2d Session | SENATE | REPORT 99-522

MEETING THE ESPIONAGE CHALLENGE: A REVIEW OF UNITED STATES COUNTERINTELLIGENCE AND SECURITY PROGRAMS

OCTOBER 3 (legislative day, SEPTEMBER 23), 1986.—Ordered to be printed

Mr. DURENBERGER, from the Select Committee on Intelligence, submitted the following

REPORT

I. INTRODUCTION AND SUMMARY

As espionage is ancient, so is counterintelligence. The Chinese military theorist Sun Tzu stated the principle in the fourth century B.C.: "It is essential to seek out enemy agents who have come to conduct espionage against you. . . ." [1] Today, over two millenia later, the battle is still being waged.

A. BACKGROUND

At the beginning of the 99th Congress, the Select Committee on Intelligence initiated a comprehensive review of the capabilities of U.S. counterintelligence and security programs for dealing with the threat to the United States from Soviet espionage and other hostile intelligence activities. This decision was an outgrowth of eight years of Committee interest in these issues. The review is also consonant with the Committee's mission to "oversee and make continuing studies of the intelligence activities and programs of the United States Government, and to submit to the Senate appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs." Senate Resolution 400, which established the Committee ten years ago, specifies that intelligence activities include "activities taken to counter similar activities directed against the United States."

The Committee's review had barely begun when the arrests of John Walker and two of his relatives began to make 1985 the "Year of the Spy." In June, 1985, the Committee pledged that it

[1] Sun Tzu, *The Art of War*, trans. by Samuel B. Griffith, Oxford University Press (London: 1963), p. 148.

Page 428 of 3957

would prepare a report to the full Senate at the earliest possible time. In light of this Committee's ongoing efforts, the Senate decided not to create a National Commission on Espionage and Security. On June 20, 1985, the Chairman of the Committee wrote to the President, saying, "You and we share an historic opportunity—both to dramatically improve U.S. counterintelligence and security and to demonstrate how Congress and the Executive can work together to achieve progress in sensitive intelligence areas."

The ensuing fifteen months have generated an amazingly sustained interest in counterintelligence and security on the part of both policymakers and the public. There have been over a dozen arrests for espionage, nearly all leading to guilty pleas or verdicts; Americans and West Germans with sensitive information have defected to the Soviet Union and East Germany; and Soviets with sensitive information have defected to the West, and in one major case then returned to the Soviet Union. Most recently, the Soviet arrest of an innocent American journalist in retaliation for the U.S. arrest of a Soviet U.N. employee has made it clear that counterintelligence, while seemingly a peripheral element in superpower relations, can even become the focus of U.S.-Soviet confrontation.

The "Year of the Spy" was characterized by intensive Executive branch attention to problems of counterintelligence and security. Of particular note were the efforts of the Department of Defense Security Review Commission, chaired by General Richard G. Stilwell, USA (retired), and the Secretary of State's Advisory Panel on Overseas Security, chaired by Admiral Bobby R. Inman, USN (retired) and Executive branch steps to implement their recommendations. The Stilwell Commission led to significant progress in Defense Department personnel and information security policies, and the Inman Panel led to restructuring of State Department security functions and a major embassy rebuilding program around the world.

The Committee's efforts have encouraged, and have greatly benefitted from, this sustained Executive branch attention to counterintelligence and security matters. The Committee received an unprecedented level of cooperation from the President, the National Security Council staff, the Intelligence Community Staff, and the many departments and agencies with counterintelligence or security functions. Executive branch experts and policymakers testified in sixteen closed hearings on specific counterintelligence cases and the current state of U.S. programs to counter hostile intelligence activities. Scores of staff briefings and the provision to the Committee of many sensitive Executive branch studies enabled the Committee to compile the very best ideas and recommendations of those in government, as well as suggestions from security experts in industry. The Committee, in turn, evaluated those ideas and submitted a comprehensive set of recommendations for Executive branch consideration.

The Intelligence Authorization Act for FY 1986 included a statutory requirement that the President submit to the House and Senate Intelligence Committees a report on the capabilities, programs and policies of the United States to protect against, detect, monitor, counter and limit intelligence activities by foreign powers,

Page 430 of 3957

within and outside the United States, directed at the United States Government. The report was to included plans for improvements that the Executive branch has authority to effectuate on its own, and recommendations for improvements that would require legislation. To assist the Senate Intelligence Committee in its work, the conferees on the Act requested an interim report developed in consultation with the Intelligence Committees. This Committee, in turn, prepared its own interim report, which it shared with the Executive branch last winter.

The many good ideas and recommendations that the Committee obtained from Executive branch officials and studies had not yet been implemented for two basic reasons: counterintelligence and security had failed to receive sustained attention; and the ideas frequently challenged established ways of doing things, cut across bureaucratic lines of responsibility, or required substantial changes in resource allocation. External events provided substantial impetus for interagency attention to these issues. The Committee's efforts and the Executive branch's cooperation are producing the interagency decision-making that is required for progress.

The President began, responding to a request from the Committee, by designating the Director of Central Intelligence to represent the Administration at a series of Committee hearings on counterintelligence and security programs and selecting a counterintelligence expert on the NSC staff as liaison to the Committee. An interagency mechanism under the Senior Interdepartmental Group for Intelligence (SIG–I) supplied coordinated Executive branch reactions to the Committee's interim report recommendations. This not only helped the Committee, but also gave the Executive branch itself the opportunity to address and decide these important policy issues. The resulting positions were conveyed to the Committee in the President's interm report and referred to an NSC staff committee for implementation.

The President's interim report and subsequent consultation between Executive branch officials and the Committee were thus of great value in the preparation of the present Report. The Committee looks forward to receipt of the President's final report, which will serve as an important benchmark of the progress achieved thus far to strengthen counterintelligence and security capabilities.

The summary that follows is based upon the Committee's unclassified public Report. The Committee's full Report to the Senate contains substantial additional material, including findings and recommendations that remain classified.

B. ORGANIZATION OF THE U.S. GOVERNMENT TO MEET THE HOSTILE INTELLIGENCE CHALLENGE

The Committee's findings underscore a fundamental challenge to the nation. The hostile intelligence threat is more serious than anyone in the Government has yet acknowledged publicly. The combination of human espionage and sophisticated technical collection has done immense damage to the national security. To respond to the threat, the United States must maintain effective counterintelligence efforts to detect and neutralize hostile intelligence oper-

Page 430 of 3957

ations directly, and defensive security countermeasures to protect sensitive information and activities.

The Committee believes that, as a result of significant improvements in recent years, the nation's counterintelligence structure is fundamentally sound, although particular elements need to be strengthened. The Executive branch and the Committee agree on the importance of developing and implementing a coherent national counterintelligence strategy that integrates the work of the FBI, the CIA and the Departments of State, Defense and Justice. Executive branch agencies are already drafting such a document. The Committee expects this strategy to play a major role in its oversight of Executive branch counterintelligence efforts in the years to come.

By contrast, defensive security programs lack the resources and national policy direction needed to cope with expanding hostile intelligence operations. Personnel security policies remain fragmented despite persistent attempts to develop national standards. Information security reforms are long overdue. America faces vulnerability to hostile intelligence activities in the areas of communications and computer security, where countermeasures must keep pace with increasing technological change. Consequently, in December, 1985, the Committee called for the development of a National Strategic Security Program that would address these issues. The Committee believes that a new and more permanent national policy mechanism is needed to create this program and then to coordinate and foster the protection of information and activities having the greatest strategic importance.

In recent months, the Executive branch has come to understand the sense of urgency with which the Committee views the need for an integrated strategic security program and an improved security policy structure. An effort to develop such a security program is now likely. The Director of Central Intelligence, in his capacity as chairman of the Senior Interdepartmental Group for Intelligence, recently revamped the security committee structure under the SIG–I and called for greater participation in those committees by policymakers, so that decisions could be reached on interagency issues and policy initiatives.

The Committee believes that these changes are insufficient because they fail to bridge the gaps between the various security disciplines. Most Executive branch officials, although opposing further changes at this time, do not dispute the likely need for them in the future. The Committee will continue to push for more effective policy review and formulation, for it believes that the national security cannot afford much more delay. This is especially true if the current Administration is to leave as a legacy a workable security policy system that will not have to be reinvented by each succeeding administration. The Committee recommends that the eventual new security policy structure be one that transcends current politics and policy and is codified in an Executive Order.

C. COUNTERINTELLIGENCE: LEARNING THE LESSONS OF RECENT CASES

The Committee has examined in detail each of the espionage cases that have come to public attention in recent years, as well as

the Yurchenko defection case and cases that remain classified. Although this Report does not discuss individual cases in detail, many of the recommendations in sections III and IV reflect lessons learned through those cases.

The first lesson of these cases is the need for greater counterintelligence and security awareness. The Committee found insufficient tailoring of security awareness material to the needs of particular audiences—defense contractors, workers at government facilities, U.S. personnel stationed overseas, members of ethnic groups known to be targeted by foreign intelligence services, congressional staff and others. The usefulness of such material is illustrated by the fact that once the U.S. Navy began to improve its security awareness briefings after the Walker case, co-workers of Jonathan Pollard noted his unusual pattern of document requests and alerted authorities.

The second lesson is the need for earlier involvement of the FBI and the Department of Justice in cases of suspected espionage. When offices or agencies have held back from bringing in the FBI, events have often gotten out of control. When the FBI has been alerted in time, their investigative resources and interview skills have often led to confessions. When the Justice Department has been involved at an early stage, cases destined for prosecution have been built on more solid ground, resulting in numerous convictions.

The third lesson is the need for more attention and better access to information on the finances, foreign travel and foreign contacts of persons with sensitive information. The Committee found that the FBI sometimes lacked access to financial and telephone records in its counterintelligence investigations; that insufficient attention was given to signs of trouble regarding former employees with sensitive accesses; and that too few people were alerting office security personnel or the FBI when they were approached by possible foreign intelligence officers.

The Chin, Pollard and Scranage cases have taught the clear lesson that espionage services outside the Soviet bloc also engage in illegal activities targeted at the United States, which must not be tolerated. The Bell and Harper cases, among many, underscored the need for controls on the activities of certain Eastern European representatives and of U.S. companies controlled by the Soviet Union or its allies. And the Zakharov case, like the Enger and Chernyayev case eight years ago, reminds us that the KGB is willing to use the United Nations Secretariat for intelligence cover.

The Edward Lee Howard case led to investigations and corrective action in the CIA, just as the Walker case led to formation of the Stilwell Commission and to additional steps by the U.S. Navy. The FBI and the Justice Department are still absorbing the lessons of the Howard case. The Committee will continue to monitor how well all the agencies implement improvements in response to those lessons.

The defection and re-defection of Vitaly Yurchenko, which highlighted both the counterintelligence value of defectors and apparent shortcomings in their handling and resettlement, also led to internal reviews and useful actions by the CIA to improve its handling of defectors. The Committee believes that more must be done, however, to change the basic objectives with which the U.S. Gov-

ernment approaches defectors. We must accept the obligation to help defectors succeed in, and contribute to, American society. Executive branch efforts to analyze and learn from the Yurchenko case continue, and the Committee expects to see more progress in this area.

The CIA has taken significant steps to improve recruitment and career development programs for counterintelligence personnel. The Scranage and Howard cases suggest that there was, and is, substantial need for improvement in CIA counterintelligence, and the Committee will continue to monitor CIA efforts. The military services and the FBI are also beginning to improve their recruitment and career development programs for counterintelligence, but progress is uneven.

The Committee will continue to press Executive branch agencies to incorporate into their operations improved counterintelligence awareness and procedures. While agencies have moved in the last year to remedy problems that were exposed in recent espionage cases, they have been much slower to accept the painful need to confront the implications of hostile intelligence successes. Attentiveness to possible hostile knowledge of classified U.S. operations must be increased, and analysis of the impact of known losses of classified information must extend to the unhappy possibility that operations or weapons systems will require modification. While there is always a need not to let worst-case analyses paralyze our military and intelligence services, the greater current danger appears to be a wishing away of the consequences of hostile intelligence efforts.

D. SECURITY COUNTERMEASURES: DEFENDING ON MANY FRONTS

The National Strategic Security Program that the Committee recommends will have to address a multitude of issues, cutting across both agency and disciplinary lines. Thus, different agencies have failed for years to agree upon the scope and methods to be used in background investigations for Top Secret and Sensitive Compartmented Information clearances; the result has been wasteful duplication of investigations. Military services, in particular, have been permitted to establish far too many special access programs, all in the name of security but sometimes with lower security standards than the regular programs maintain. Technical experts who run our nation's computer security programs have poured additional funds into specially-designed hardware and software to protect sensitive computer systems, while doing little to combat the major personnel problem of assuring the reliability of computer users with access to so much sensitive data. The various agencies that deal with technical security issues have only recently begun to forge effective cooperation on approaches to those issues. And this country has a long way to go in the development of operations security practices to protect sensitive programs against hostile intelligence collection activities.

This Report groups many security issues by discipline, but the Committee feels strongly that many, and perhaps most, of those issues will remain unresolved until a more effective security policy structure is implemented. There is a need to upgrade security

Page 434 of 3957

across the board, with improved recrutiment, improved training of personnel ranging from security clearance adjudicators to polygraphers and technical security personnel, and upgraded job classifications that reflect the increased importance and sophistication of modern security specializations.

In the field of personnel security, the Committee found, as did the Stilwell Commission, that insufficient attention was being paid to the reinvestigation of those who already have security clearances. Both the Defense Department and the intelligence community now understand the importance of reducing the backlog in those reinvestigations, and the Committee has worked to ensure that the needed funds to accomplish this swiftly are provided in legislation. One reason for recommending interagency agreement on a "single scope" background investigation is the hope that funds thus saved could be put to work on the pressing reinvestigation task, as well as on upgrading Secret clearance investigations as recommended by the Stilwell Commission. The Defense Department has reduced the number of cleared personnel by some 900,000 persons—over 20%—thus also easing some of the clearance investigation costs.

There is a crisis of standards in sensitive governmental positions. The Committee found no rigorous standards regarding the hiring of persons who have committed felonies. Follow-up measures after persons with admitted problems like past drug use are granted clearances are poor or nonexistent. Even the most sensitive clearances are granted to virtually anyone whose record does not contain clear disqualifying factors, rather than being based upon a selection process that chooses those persons most able to cope with the pressures of sensitive access and security. In light of this, the Committee has supported Defense Department efforts to develop counterintelligence polygraph programs with the highest quality controls, pursuant to the test program approved by the House and Senate Armed Services Committees.

The Committee has found that the classification system is unduly complicated and that it breeds cynicism and confusion in those who create and use classified information. The Committee believes that a streamlined system, in which the Confidential classification is eliminated and all information is either Secret or the equivalent of Sensitive Compartmented Information, would be much more workable despite the major changes and initial costs that this would entail.

The Committee also found that authorized (but uncontrolled) disclosures and unauthorized leaks of classified information are so commonplace as to imperil many sensitive programs and operations. Recent Executive branch efforts to investigate instances of unauthorized disclosure of classified information and to punish those responsible are a welcome development. The Committee calls on the Executive branch to go further, however, and to adopt procedures governing authorized disclosures, so that there will be a record of such disclosures—thus relieving the FBI of the need to investigate cases that are not real leaks—and so that those who originate classified information will have a chance to argue against its release. There must be both firmness and order in the information security system before it will gain the respect of the millions of people who handle classified information.

Page 434 of 3957

The Committee was pleased to learn of the National Security Agency's many efforts to improve the communications security of the U.S. Government. It supports NSA's plan for the development and licensing for distribution of low-cost secure voice telephone equipment. In addition, the Committee has proposed Fiscal Year 1987 funding to improve communications security by beginning the encryption of many domestic commercial communications satellite links.

The Committee endorses the role of NSA in developing computer security hardware, systems and standards for both the government and segments of the private sector, in cooperation with the National Bureau of Standards. The Committee recommends, however, increased attention to personnel security aspects of protecting computerized information. It supports State Department efforts to place U.S. citizens in charge of the computers in U.S. embassies overseas. The Committee believes that personnel with access to the most sensitive computer systems should be included in personnel reliability programs similar to those now being instituted for persons with sensitive cryptographic access. And it believes that there must be better analysis of information system vulnerabilities before permission is given to put sensitive information in those systems.

The Committee was very concerned over serious deficiencies in the security of U.S. facilities overseas, primarily those managed by the Department of State. The bugging of typewriters in the U.S. Embassy in Moscow graphically demonstrated both Soviet sophistication and U.S. vulnerabilities. Steps are being taken to combat technical penetration efforts, ranging from the embassy rebuilding program proposed by the Inman Panel to an equipment protection program that was funded in the Diplomatic Security Act. The Committee supports these and other efforts, and it has worked to ensure that agencies will work closely with each other to bring the best expertise to bear on technical security problems.

The Committee has also found the industrial security system for classified defense and intelligence contracts to be seriously deficient, to an extent that warrants consideration of major changes. The Committee recommends a pilot program to assign Defense investigative Service personnel to large sensitive contractor facilities on a full-time basis. It proposes changing the Federal Acquisition Regulations to make security a direct cost in contracts, rather than an overhead cost that is inevitably subjected to corner-cutting. It suggests greater incentives in contracts for security performance, as well as a requirement that security officers be trained and government-certified. Many of the Committee's recommendations regarding personnel and information security will also have a direct impact upon industrial security practices.

Attention to security requirements is also needed in Congress itself. The Committee found that there was no centralized registry of Senate personnel with clearances, little or no security awareness material for Congress, and little understanding of how to protect sensitive information that is provided to Member offices and committees. At the request of the Majority Leader, the Committee joined with the Committee on Rules and Administration and the Committee on Governmental Affairs in recommending that a

Senate security office be established to develop and oversee implementation of standards and procedures in these areas. The Committees recommended that the security office be instructed to survey the extent of clearances among Senate staff, to recommend how the number of cleared personnel might be reduced, and to develop a Senate security manual, the provisions of which would be binding on all Members, Officers and employees of the Senate. The Committee continues to work closely with Senate leadership on these efforts, with a goal of creating a security office early in the next session.

E. BUDGETARY IMPACT

The Committee's recommendations will not be cost-free. Some savings would be achieved through streamlining the classification system, adopting common standards for background investigations, and implementing current national policies that lessen the requirement for TEMPEST protection of U.S.-based information-processing equipment. But the Committee believes that the U.S. Government has suffered for years from inadequate investment in security countermeasures.

In the Intelligence Authorization Act for Fiscal Year 1987, the Committee has proposed substantial increases in spending for security in the intelligence community and in related Defense Department programs. Among these initiatives are an additional $129 million for communications security, including the first year of a five-year plan to encrypt sensitive domestic communications satellite channels, and an additional $22 million to improve personnel security in the Defense Department. In 1985, Committee members proposed what became a $35 million supplemental appropriation for improved technical security at U.S. facilities abroad. In 1986, the Congress passed the Diplomatic Security Act and a supplemental appropriation providing funds for a massive program to upgrade security at U.S. missions. This commitment is designed for protection against not only terrorism, but also hostile intelligence penetration.

The additional expenditures recommended by the Committee for FY 1987 would amount to an increase in annual spending for counterintelligence and security of at least $500 million above the funding level in FY 1985. This commitment must continue in the years ahead, when further increases may well be required because of the growing technical, communications and computer security vulnerabilities. From a larger perspective, however, the costs of improved security will be offset by the gains to the United States in the overall U.S.-Soviet balance of military, intelligence, economic and political capabilities. Soviet espionage successes have cost our country or saved our adversaries billions of dollars. Just as our nation's investment in intelligence-gathering programs has a significant payoff for national security, an increased investment in counterintelligence and security programs will help deny comparable advantages to the Soviets.

F. LEGISLATIVE PROPOSALS

The great majority of the Committee's findings and recommendations relate to administrative actions. Some needed actions do require, however, legislative authorization. In these cases, the Committee has either recommended or, often, already introduced the needed legislation.

Members of the Committee have sponsored several pieces of legislation in recent years to bring the hostile intelligence presence in the United States under some control. The Committee recommends that these be implemented so as to maintain a limit of 320 on permanently accredited Soviet embassy and consular personnel. The Committee also found gaps in current legislation and recommended three further steps: a legislated policy of equivalence between the U.S. and Soviet U.N. missions (introduced by Senators Leahy and Cohen as S. 1773); registration of commercial entities controlled by Warsaw Pact governments (introduced by Senator Roth as S. 1900); and extension of the Foreign Missions Act to include commercial and other entities controlled by foreign governments (introduced by Senators Durenberger and Leahy as S. 1947). All three proposals have been attached to the Intelligence Authorization Act for Fiscal Year 1987.

The FBI could benefit greatly from legislation in several areas. The Committee has added provisions to the Intelligence Authorization Act for Fiscal Year 1987 that would require banks and telecommunications companies to comply with FBI requests for access to customer records pursuant to duly authorized full counterintelligence investigations. State privacy laws and fears of civil suits have inhibited some companies from cooperating with the FBI in recent years. The Committee is also prepared to introduce legislation to create a court order system, comparable to that which now exists under the Foreign Intelligence Surveillance Act, to authorize physical searches for couterintelligence purposes. This would avert the need to rely on assertion of inherent Presidential powers in this area and would make it easier to use material thus obtained in eventual prosecutions.

The FBI has a problem in providing sufficient financial incentives to its Agents who must work in New York City, which in turn makes it difficult to retain counterintelligence specialists in that Field Office for substantial periods of time. If the FBI determines that legislation is required to address this problem, the Committee is prepared to work with the FBI to develop a suitable legislative approach.

The Committee recommends that the FBI and the Justice Department develop improved means of prosecuting foreign intelligence officers or agents who enter the United States illegally or under non-official cover and who engage in intelligence support functions without actually passing classified information. This could result in legislative proposals in the next Congress.

Although the Committee has not recommended legislation regarding assistance to defectors, it is quite possible that the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs will make such recommendations when it completes

Page 438 of 3957

its inquiry into that matter. The Intelligence Committee expects to work closely with the Permanent Subcommittee on this issue.

The Committee supports recent Defense Department efforts to develop a counterintelligence polygraph program with strict quality controls, modeled on the Air Force's successful Seven Screens program. The Committee recommends that the Armed Services Committee either propose legislation to establish a permanent authority for this polygraph effort or extend the current test program under which DoD is operating and set a date by which the issue of permanent authority will be decided.

Deficiencies in congressional security have prompted the Committee, in conjunction with the Committees on Governmental Affairs and Rules and Administration, to propose that the Senate establish a Senate security office with responsibilities in the areas of personnel and information security. The office would be established by Senate Resolution.

The Committee has not recommended any legislation at this time to deal with the unauthorized disclosure of classified information. It believes that consideration of this issue should be postponed until appeals are completed in the *Morison* case and the applicability of the federal espionage statutes to leaks and other disclosures has been decided. In addition, the Committee believes that there are significant administrative steps that can and ought to be implemented more quickly, in particular the adoption of procedures to govern the authorized disclosure of classified information.

G. RESPECT FOR INDIVIDUAL RIGHTS

A free society cannot allow the fear of foreign adversaries to undermine the constitutionally protected rights that define the true character of our nation. This principle has guided the Committee in its review of counterintelligence and security programs. As President Reagan stated on June 29, 1985:

> [W]e can counter this hostile threat and still remain true to our values. We don't need to fight repression by becoming repressive ourselves. . . . But we need to put our cleverness and determination to work and we need to deal severely with those who betray our country. We should begin by realizing that spying is a fact of life and that all of us need to be better informed about the unchanging realities of the Soviet system. . . . There is no quick fix to this problem. Without hysteria or finger pointing, let us move calmly and deliberately together to protect freedom.

The Committee's recommendations seek to strengthen U.S. counterintelligence and security measures without violating constitutional rights or upsetting the delicate balance between security and freedom. A broad range of improvements can be made without adversely affecting the rights of individuals, and the additional tools needed for counterintelligence and security purposes can be made subject to reasonable safeguards that minimize intrusion into the privacy of American citizens.

Page 438 of 3957

II. The Hostile Intelligence Threat

The hostile intelligence threat to the United States is severe, and it confronts the Government and the American people with increasingly serious challenges. The threat spans all types of intelligence operations from traditional human espionage to the most sophisticated electronic devices. Every kind of sensitive information is vulnerable, including classified government information, emerging technological breakthroughs and private financial transactions. Foreign intelligence services also sometimes target the political process, seeking both information and influence.

What has made the threat more vivid to the Congress and the public are the many espionage cases that surfaced publicly in the last few years. During 1984–86, twenty-five people have been convicted or have pleaded guilty to charges of spying against the United States. Another person charged with espionage, Edward Lee Howard, has defected to the Soviet Union; a Soviet employee of the United Nations has pleaded "no contest" to espionage charges; and several foreign diplomats have been detained and/or ousted because of their espionage activities. The upsurge in espionage prosecutions began in the late seventies; and FBI Director William H. Webster said in 1984 that the espionage cases that came to public attention were "merely the tip of the iceberg." The Committee believes it is vital for the Senate and the public to be aware of the full dimensions of the threat, technical as well as human.

A. Damage to National Security

National policymakers must recognize as clearly as possible the extent and gravity of the damage to national security interests caused by hostile intelligence operations. Based on the public and classified record, the Committee has found the aggregate damage in recent years to be far greater than anyone in the U.S. Government has yet acknowledged publicly. The Committee has reviewed the actual and probable injury resulting from recent espionage cases, technical security compromises and technology transfer. The inescapable conclusion is that the damage was immense:

U.S. military plans and capabilities have been seriously compromised;

U.S. intelligence operations were gravely impaired;

U.S. technological advantages have been overcome in some areas;

U.S. diplomatic secrets were exposed to the scrutiny of our adversaries; and

Sensitive aspects of U.S. economic life were subject to constant Soviet monitoring.

Foreign intelligence services have exploited human and technical vulnerabilities to penetrate some of the most vital parts of our defense, intelligence and foreign policy structure, including many Executive branch agencies and the Congress. A sober examination of the damage is essential to make rational decisions on policy initiatives and resources allocation for counterintelligence and security programs.

In assessing the military damage, the Committee agrees with an estimate by a senior FBI official that the espionage cases over the

Page 440 of 3957

past several years have involved billions of dollars of actual and potential damage to U.S. military programs. The cases primarily include John Walker and Jerry Whitworth, James Harper, William Holden Bell, Thomas Cavanagh, Christopher Cooke and Ernest Forbrich.

Walker-Whitworth

Although the assessment in the Walker and Whitworth cases is still incomplete, their information may have enabled the Soviets to read some of the U.S. Navy's most secret messages to the fleet from the 1960's to the time of their arrests in 1985 and also possibly reduced the U.S. lead in anti-submarine warfare. The cryptographic material passed by John Walker and Jerry Whitworth was exceptionally harmful, because the Soviets could use it to decipher encrypted U.S. Naval communications. Vitaly Yurchenko, the Soviet KGB defector who later returned to the Soviet Union, told U.S. authorities that the Soviets read over a million coded messages as a result.

(An official assessment of the damage, prepared by the Director of Naval Intelligence and a senior Justice Department official, is provided in Appendix A.)

Harper

In 1979–81 James Harper passed to Polish intelligence a huge array of materials pertaining to the survivability of the Minuteman missile system and to U.S. defenses against ballastic missile attack. He obtained the information from a private firm doing contract research for the U.S. Army Ballistic Missile Defense Advanced Technology Center in Huntsville, Alabama. Harper received approximately $250,000 for documents whose loss Army experts have rated as "beyond calculation." He also provided computer data-base tape available through his contacts in Silicon Valley. Harper's largest single delivery occurred in 1980, when he took some 100 pounds of classified reports to Warsaw, where a team of 20 KGB experts flown in from Moscow declared them to be extremely valuable. KGB Chairman Yuri Andropov commended the Polish intelligence unit handling Harper for its efforts. (An account of the Harper case prepared by the Defense Security Institute is provided in Appendix B.)

Bell

William Holden Bell was recruited by a Polish intelligence officer operating under commercial cover. As a project manager in the Advanced Systems Division, Radar Systems Group at Hughes International Corporation, Bell was responsible for development and promotion of the radar fire control product line of tank vehicles. From 1978 to 1981, Bell supplied Polish (and presumably Soviet) intelligence extensive classified documents on the Covert All-Weather Gun System [CAWGS], a proposed tank gun using Low Probability of Intercept Radar [LPIR] or "quite radar." LPIR uses a disguised radar signal that is difficult for enemy targets to identify as radar; an enemy is thus prevented from taking evasive action or using the radar signal for directing return fire. (An account of the

Page 440 of 3957

Bell-Zacharski case prepared by the Defense Security Institute is provided in Appendix C.)

Cavanagh

The defense contractor case with the greatest potential for devastating harm involved Thomas Cavanagh, an engineer at Northrop Corporation. He was arrested in December, 1984, for attempting to sell classified documents on Stealth technology to the Soviets. The FBI intercepted his attempt, and FBI agents posing as KGB officers made the arrest after giving him $25,000 for the documents. While no serious compromise actually occurred, FBI Director Webster has said that Cavanagh's documents contained "the core of the Stealth technology" which had "cost this country over $1 million an hour to develop." (An account of the Cavanagh case prepared by the Defense Security Institute is provided in Appendix D.)

Cooke

Lt. Christoper Cooke, deputy commander of an Air Force Titan missile crew, was charged with passing classified information to the Soviets on U.S. strategic missile capabilities in 1980-81. While the damage was serious, the charge was dismissed because Air Force prosecutors had offered him immunity to find out if he was a part of a larger spy ring (which he apparently was not).

Forbrich

Ernest Forbrich, a West German auto mechanic, was arrested in 1984 in Florida after buying a classified military document from an undercover agent posing as an Army officer. Forbrich appears to have been a conduit who passed U.S. military secrets to East German intelligence, and he admitted selling documents to the East Germans for 17 years. Forbrich traveled frequently to the United States, contacting former U.S. military personnel who had served in West Germany. Although he was convicted of espionage, none of the former U.S. military personnel whom Forbrich contacted was charged.

The espionage damage to U.S. intelligence over the past decade has been as great as the harm to military programs. The cases that surfaced in 1985—Howard, Pelton, Chin and Pollard—represent a severe blow to U.S. intelligence, with Howard, and Pelton doing the greatest harm because they compromised collection efforts directed at high-priority targets in the Soviet Union. Other recent cases involved FBI Agent Richard Miller, Army counterintelligence specialist Richard Craig Smith, and CIA employees Sharon Scranage and Karl Koecher.

Howard

Edward Lee Howard, a former case officer dismissed by the CIA, was accused of selling intelligence secrets to the Soviets and subsequently defected to Moscow. Howard probably gave the Soviets information on sensitive CIA operations in Moscow.

Pelton

Ronald Pelton, a former communications specialist with the National Security Agency from 1965 to 1979, was convicted in 1986 of selling the Soviets information about a highly classified U.S. intelligence collection project targeted at the Soviet Union. Other aspects of the damage caused by Pelton that did not surface at the trial have not yet been completely evaluated.

Chin

Larry Wu-tai Chin gave the Chinese an inside view of U.S. intelligence reporting on China and related topics for decades, first as a translator for the U.S. Army and then as a translator and foreign media analyst for the CIA. Chin was a "plant" who received intelligence training before his employment by the Army in 1943. His reporting was highly praised by Chinese officials.

Pollard

Jonathan Jay Pollard, a civilian intelligence analyst with the Naval Investigative Service, pleaded guilty in 1986 to the charge of illegally passing classified documents to Israel. Pollard obtained a wide array of intelligence reports on the Middle East for his Israeli contacts.

Miller

FBI Agent Richard Miller injured the entire intelligence community, not just the FBI, when he provided the Soviets in 1984 (through his Russian emigre lover Svetlana Ogorodnikova) a document outlining overall U.S. foreign intelligence collection priorities.

Smith

Richard Craig Smith, a former Army counterintelligence agent, was charged in 1984 with selling information to Soviet agents in Tokyo identifying U.S. double agents being operated against Soviet intelligence. Smith was acquitted in 1986 after asserting as his defense that be had been working under the direction of CIA operatives in Honolulu.

Koecher

Karl Koecher, a naturalized U.S. citizen of Czech origin, worked as a translator for the CIA in the 1970s. He and his wife were arrested in 1984 as they prepared to fly to Switzerland. By then, the FBI had sufficient information to establish that Koecher was trained and sent to the United States in the 1960s to work as a Czech "illegal" and penetrate U.S. intelligence. Koecher was able to give Czech intelligence everything he knew about such sensitive CIA information as he was provided in his job as a translator.

Scranage

Sharon Scranage, a CIA operations support assistant in Ghana, was convicted in 1985 of turning over classified information, including the identities of CIA case officers and clandestine sources, to Ghanaian intelligence officials.

In addition to the damage to classified U.S. military and intelligence programs, hostile intelligence services have acquired sensitive technological data in the United States, Western Europe, Japan and elsewhere. Soviet acquisition of U.S. technology has significantly reduced the time it took the Soviets to develop new weapons systems and field countermeasures to U.S. systems. A recent example is the case of Manfred Rotsch, a Director of Planning for a prominent West German aerospace company, who was arrested as a Soviet agent. Rotsch was in a position to transfer detailed manufacturing information on Western weapon systems to the KGB, and the case points up the vulnerability of U.S. advanced technology released in coproduction or licensing programs. The research and development cost savings to the Soviet Union from illegal Western technology acquisition are believed to be enormous. The Ministries of Defense Industry and Aviation Industry alone are estimated to have saved half a billion rubles (roughly $700 million at official conversion rates) between 1976 and 1980, although that figure probably reflects operating cost savings as well as R&D.

In the diplomatic field the recent discovery of bugged typewriters in the U.S. embassy in Moscow exposed an operation of some duration. For years, the Soviets were reading some of our most sensitive diplomatic correspondence, economic and political analyses, and other communications.

More difficult to assess, yet with enormous danger to the United States, is the Soviet interception of U.S. communications from collection facilities throughout the world, including Soviet diplomatic establishments in the United States and an extensive site at Lourdes, Cuba. The Soviets could monitor many U.S. domestic telecommunications channels, including most satellite links and certain ground-to-ground transmissions. While the risk to military secrets from poor communications security is widely understood, the U.S. business community is also highly vulnerable.

Taken together, the damage to national security from espionage, technology theft and electronic surveillance amounts to a staggering loss of sensitive information to hostile intelligence services. As an open society, the United States already allows its adversaries unfettered access to vast amounts of information that must be shared widely so that our political system can function democratically and the process of free scientific inquiry can be most productive. Our openness gives hostile intelligence services the ability to focus their efforts on those few areas of our government and society where confidentiality is required.

The following discussion of the hostile intelligence threat to the United States is designed to give the Senate and the American people a better appreciation of the challenges we will continue to face in the future. It is based upon an assessment prepared by the intelligence community at the Committee's request. By understanding the nature and scope of ongoing hostile intelligence efforts, public officials and private citizens alike can better understand why the Committee recommends increased emphasis on counterintelligence and security programs. There is much that the ordinary citizen can do to strengthen the nation's defenses, especially if the individual works for the federal government, a government con-

Page 444 of 3957

tractor, or a high-tech industry or research program. The key requirement is knowledge of the dangers.

B. SOURCES OF THE THREAT

Among foreign intelligence services, those of the Soviet Union represent by far the most significant intelligence threat in terms of size, ability and intent to act against U.S. interests. In fact, the activities of the Warsaw Pact country and Cuban intelligence services are primarily significant to the degree that they support the objectives of the Soviets. The threat from intelligence activities by the People's Republic of China (PRC) is significant but of a different character, as explained below. The intelligence activities of North Korea, Vietnam and Nicaragua pose a lesser, but still significant, threat to U.S. foreign policy interests, although these countries have only a limited official presence in the United States.

Many other countries—hostile, allied, friendly and neutral—engage in intelligence operations against the United States. While these activities cannot be ignored, they do not represent a comparable threat. Nonetheless, in 1985, arrests for espionage included U.S. Government employees who had passed classified information to Israel and to Ghana.

1. Soviet Union

The KGB and the GRU are the two principal Soviet intelligence organizations. The KGB (or Committee for State Security) maintains internal security in the USSR and, as a secret intelligence service, collects intelligence and conducts covert political influence operations (termed "active measures") abroad. The GRU (or Chief Directorate for Intelligence) is the Soviet military intelligence organization and engages only in foreign intelligence activities.

In no other country in the modern world have intelligence and security services played such a crucial, long-term role in sustaining a government and controlling its citizens. In recent years, the KGB has become a vital tool for protecting the Communist Party at home and implementing its policies worldwide, especially through energetic espionage and covert action operations both against Western governments and in the Third World. (Covert action efforts are coordinated with the International Department of the Communist Party, which has lead responsibility for worldwide Soviet "active measures," including propaganda and political influence operations.) Soviet military intelligence came into its own during and just before World War II, and the GRU aggressively supplements the KGB with espionage and massive technical surveillance operations. The GRU coordinates and supports Soviet SIGINT and overhead photography and trains foreign revolutionary cadres and insurgents. In the operational Soviet military, "Spetsnaz" (Special Forces) units have an overseas role as special-purpose commando forces capable of covert infiltration, sabotage and assassination operations.

The highest Soviet collection priority is accorded to policy and actions associated with U.S. strategic nuclear forces. Other high priority subjects are key foreign policy matters, congressional intentions, defense information, advanced dual-use technology, and

Page 444 of 3957

U.S. intelligence sources and methods. The Soviets also target NATO intensively, partly as a means to obtain U.S. foreign policy and military information; recent arrests in West Germany and Greece are indicative of the successes of the USSR in targeting U.S. and NATO classified weapons systems.[2] The Soviets heavily influence the collection activity of the Cuban and Warsaw Pact services, in effect expanding their own collection resources through exploitation of the ethnic ties that other services can use in their recruitment efforts, as well as the normally less stringent U.S. controls on the activity of non-Soviet visitors and representatives.

The Soviets acquire much of the information they need through non-clandestine means—diplomatic activities, trade representatives, visitors, students, and other open inquiry. They carefully select participants in exchange programs to maximize access to information of intelligence interest. The Soviet government also has access to computerized U.S. and other Western reference systems, to U.S. Government programs designed to facilitate legitimate dissemination of information, and to open literature ranging from technical journals and industry publications to the news media. Soviet collection efforts are further aided by the absence of effective U.S. Government controls over foreign visitors and indirect exports.

The Soviets aggressively screen information on Western technology to avoid technological surprise and to improve their economy and weapons systems. The methods used to acquire technology will depend largely on the cost and the risk involved. It is likely that increased controls on trade with the Soviets and on Soviet visitors and official personnel will cause changes in Soviet collection techniques. Thus, more use of clandestine methods to acquire technology is likely when it cannot be obtained in other ways.

2. Warsaw Pact and Cuba

The intelligence services of Poland, East Germany, Czechoslovakia, Bulgaria, Hungary and Cuba not only serve their own national interests, but also act as surrogates for Soviet intelligence. While a member of the Warsaw Pact, Romania has looser ties to the Soviets in the intelligence arena. Recent cases demonstrate the aggressiveness of the Warsaw Pact services. In 1983, an employee of the Bulgarian trade office in New York was arrested for espionage based on evidence that he bought a secret document on security procedures for American nuclear weapons. The Bell and Harper cases illustrated the effectiveness of Polish intelligence in penetrating U.S. defense industry. East German agents arrested in the United States over the past three years include a women courier in a KGB espionage network and a prominent scientist attempting to recruit American scientists.

The recent interagency report on Soviet Acquisition of Militarily Significant Western Technology documents fully the relationship between Soviet intelligence and the Warsaw Pact services. The

[2] This Report concentrates upon the direct hostile intelligence threat to the United States and does not include the counterintelligence and security implications for the United States of hostile intelligence activities that target U.S. allies or alliances. The Committee will examine these matters in its continuing oversight of U.S. counterintelligence and security programs.

Page 446 of 3957

KGB, more than the GRU, relies on the collection capabilities of the East German, Polish, Bulgarian and Czech services. The success of the East European services can be attributed partly to the Western misperception that their countries are less of a threat than the USSR. East European nationals operating in most Western countries have fewer (or no) travel restrictions and, in some cases, find it easier to work in a Western cultural and commercial environment. At the same time, however, the West also has easier access to Warsaw Pact countries than to the Soviet Union. Reciprocity considerations limit the West's ability to impose extreme controls on East Europeans.

The Cuban DGI has long been under the direct influence of Soviet intelligence. While in recent years the Cubans have emphasized operations against anti-Castro emigre groups and illegal acquisition of embargoed U.S. technology and equipment, Cuban intelligence also targets U.S. Government plans and intentions, especially regarding Latin America. There are indications, dating back many years, of Cuban support and training for Puerto Rican terrorists and of propaganda operations to influence segments of American public opinion.

3. People's Republic of China

The PRC has several intelligence services whose personnel are represented among the approximately 1,500 Chinese diplomats and commercial representatives located at some 70 PRC establishments and offices in the United States. They also have some access to the approximately 15,000 Chinese students and 10,000 individuals arriving in 2,700 delegations each year. PRC intelligence also seeks to exploit the large ethnic Chinese community.

The implications of PRC intelligence activities are markedly different from those of the Soviet Union and its surrogates. The forces of the Warsaw Pact are arrayed against those of NATO; and the Soviet Union's expansionist policy poses a current and continuing global challenge to the United States and its allies. The PRC is not now in strategic competition with the United States. Indeed, the United States has fundamental interests in maintaining friendly relations with the PRC and promoting its modernization, to include selective upgrade of its military defensive capabilities. Intelligence collection priorities of the two major communist powers reflect their respective foreign policies. The Soviet intelligence services have urgent requirements with respect to U.S. plans, intentions and capabilities, as well as technology; the PRC services concentrate primarily on advanced technology not approved for release so as to further PRC military and economic modernization in the 1990s and beyond.

Despite these differences, the PRC intelligence threat continues to be significant. The evidence of PRC espionage in the Chin case and from other counterintelligence sources justifies alerting American citizens to the current risks. The recent detention of a British national employed by the New York Times as a reporter in China reflects an increased emphasis by PRC intelligence and security services on surveillence of foreign visitors. PRC efforts to cultivate Chinese-Americans in scientific and technical fields should be recognized as including potential intelligence approaches, as long as

Page 446 of 3957

the PRC continues to mount espionage operations against classified U.S. programs and embargoed technology.

4. Other Countries

Other countries also conduct human intelligence operations in the United States, both overt and covert. Their targets include largely the same range of interests as those of the Soviets and the PRC, including high technology and political, military and economic policies and intentions that might affect the particular country.

Among the common activities of foreign intelligence services in this country are attempts to penetrate emigre communities. A large number of expatriate political and emigre groups in the United States are viewed as a threat by authorities in the former homelands. From a national security viewpoint, these activities are less significant than those of the USSR and its allies, although they are clearly in violation of U.S. sovereignty and may have an effect on the U.S. political system. Foreign intelligence services also target ethnic groups in the United States, directly or through front organizations, to influence U.S. decisions on foreign aid, trade agreements and other issues where foreign governments have strong interests.

Two recent incidents illustrate the threat from non-communist governments. In 1984, a vocal opponent of the current regime in Taiwan was murdered in California, and the Taiwanese government later admitted that officials of its intelligence service were implicated. Also in 1984, the South African military attache was expelled from the United States for activities incompatible with his diplomatic status. In 1978, the Committee issued a public report on Activities of "Friendly" Foreign Intelligence Services in the United States which examined, as a case study, South Korean operations in the early-to-mid 1970s. The Pollard case has raised questions as to whether the Israeli government, or significant elements thereof, have engaged in more extensive espionage operations in the United States. While the strategic threat in such cases in less than from Soviet bloc or PRC operations, the harm to specific U.S. foreign policy interests and legal safeguards is still substantial and unacceptable.

C. HUMAN INTELLIGENCE TECHNIQUES

The hostile intelligence threat can be divided roughly between the human side and the wide array of technical collection operations. The human dimension begins with the trained intelligence officer, dispatched under official or nonofficial cover to operate abroad. Intelligence officers recruit and handle agents employed by foreign governments, industries, or political organizations; and they "co-opt" other members of their own government and citizenry for particular assignments. In general, hostile intelligence HUMINT operations fall into the following categories:

"Legal" operations are conducted by intelligence officers under official cover. The term does not mean "lawful," because case officers recruit and handle espionage agents. The FBI estimates that at least 30% of the 1,500 Soviet officials in the U.S. are KGB or GRU staff officers. Reportedly, over 3,000 KGB of-

Page 448 of 3957

ficers and approximately 1,500 GRU officers are posted outside the Soviet Union.

"Illegals" are trained intelligence officers sent abroad, often with false identities, who maintain no overt contact with their government. The number of Soviet illegals and their activities are very difficult to estimate.

"Co-optees" are officials or visitors tasked to do particular tasks, such as spotting potential recruits or servicing drops. Many Soviet officials are co-opted, as are many official visitors and some emigres.

"Agents" are American or third-country nationals recruited for current operational purposes or, in some cases, as "sleepers" to be activated at a later date. Apart from the agents surfaced publicly in espionage or illegal export cases, the FBI has numerous other suspected agents under investigation.

Despite the development of increasingly sophisticated technical means of collection, the human agent continues to be the most important key to satisfying a nation's intelligence needs. An intelligence community study summarized the human threat in the following terms:

> The Communist countries depend to a large degree on their human collection networks throughout the world to satisfy their U.S.-related intelligence requirements—requirements ranging from acquisition of advanced technology, location and determination of the quality of strategic and conventional military forces, and assessment of U.S. reaction to international political incidents, to discovery of techniques used by U.S. counterintelligence.

An analysis of hostile human intelligence operations against the United States must address the role of the Soviet-bloc official presence in the United States; the non-official United Nations and "illegal" hostile presence; the recruitment of agents; the Soviet Union's systematic technology acquisition program; and covert political action operations (or "active measures").

1. Official Presence

The spearhead of the Soviet, other Warsaw Pact and Cuban intelligence collection effort is their official presence in the United States. In 1985, there were about 4,250 diplomats, commercial officials and other representatives from Communist countries in the United States, 2,100 of whom were from the Soviet Union and the other Warsaw Pact countries. The Soviet Missions to the United Nations in New York have approximately 275 accredited diplomats; the Department of State has recently mandated a reduction in this number to 170 by April 1988. The Soviets have 320 accredited personnel at their Embassy in Washington and Consulate General in San Francisco, in comparison to the approximately 200 American diplomatic personnel assigned to the Soviet Union. Additional Soviets come to the United States on temporary assignment, as do American personnel to the USSR.

The FBI estimates that at least 30 percent of the Soviet bloc officials and representatives in the United States are professional intelligence officers of the Soviet KGB and GRU or one of the other

Page 448 of 3957

East European intelligence services. Under diplomatic cover, Soviet bloc diplomatic personnel accredited to the United States and to the U.N. missions in New York have complete immunity from criminal prosecution for espionage. (By contrast, Soviet nationals employed by the U.N. Secretariat, such as Gennadiy Zakharov, do not have such diplomatic immunity.)

Soviet bloc use of official representatives for espionage purposes is well documented. In the Walker and Miller cases, Soviet officials involved with handling American agents left the country shortly after their agents were arrested. In other instances, successful U.S. counterintelligence operations have led to the exposure of Soviet officials engaged in clandestine communications with agents, such as by servicing "drops." Soviet bloc intelligence officers under diplomatic cover also seek to use overt contacts with Americans as an opportunity to develop long-term relationships providing an opportunity to assess and exploit vulnerabilities for espionage recruitment purposes. In one case in the early 1980s, a Soviet official who attempted to recruit a Congressional staff member was expelled from the country. The staff member had reported the approach and cooperated with the FBI's investigation, which led to exposure of the Soviet official's intelligence recruitment efforts.

The sheer volume of intelligence activity is increased by the number of officials from other Communist countries in the United States as well as the large number of establishments from which they can operate. Soviet bloc and PRC establishments—government offices and U.N. missions—are located in seventeen different cities. The largest numbers are in New York (92), Washington (34), Chicago (11), San Francisco (9), Houston (9), and Newark (9). While most officials are concentrated in New York and Washington, all but the Soviets are allowed to travel almost anywhere they wish in the country, subject to notice requirements and certain other conditions under the Foreign Missions Act in the case of most Warsaw Pact countries.

Within the Soviet services, GRU personnel are targeted primarily against military and scientific and technical information, while KGB personnel in its First Chief Directorate (foreign intelligence) are assigned to one of four operational departments or "lines"—Scientific and Technical (Line X), Political (Line PR), Counterintelligence (Line KR), or Illegals Support (Line N). S&T personnel specifically target U.S. advanced technology. Often, clandestine collection of S&T information is preferred over buying or developing technology because it is cheaper and provides the best short-term results, although there is a risk factor in theft. KGB Line PR officers target governmental policy information and, frequently, seek to advance Soviet objectives via contacts with persons of influence or through covert activities. Certain Line PR officers focus specifically on the Congress. Line KR officers have the security responsibility for preventing defections of Soviet personnel and particular concern for penetration of the U.S. intelligence community, although all lines are tasked with this important function as a matter of general concern. "Illegals" support personnel comprise a small group that helps maintain those networks.

2. Other Aspects of the Hostile Intelligence Presence

The Soviet Union is effectively using U.N. organizations, particularly the Secretariat, in the conduct of its foreign relations and as a cover for the activities of Soviet intelligence officers and co-optees. The United Nations employs, worldwide, approximately 800 Soviet nationals as international civil servants, with about 300 of them in New York. Approximately one-fourth of the Soviets in the Secretariat in New York are considered to be intelligence officers, and many others are co-optees who have been told to respond to KGB and GRU requests for assistance. The Soviet intelligence services also use their developed agents in the United Nations to collect information on U.N. activities; to spot, assess and recruit American and foreign-national agents; to support worldwide intelligence operations; and to collect scientific and technical information on the United States.

The KGB has succeeded in infiltrating its officers into the U.N. bureaucracy, with some reaching positions of authority. The KGB has held the position of Assistant to the Secretary General since Viktor Lesiovskiy held the post under U Thant. The current Assistant is a KGB China expert. The Soviets take full advantage of U.N. personnel procedures such as liberal sick leave. This permits KGB U.N. employees to be absent as often as they desire, enabling them to carry out intelligence activities further abetted by the comparative freedom of movement enjoyed by U.N. employees.

While the State Department has recently required Soviet U.N. employees to give notice of unofficial travel outside the New York area, they are not subject to the geographical off-limits restrictions placed on Soviet diplomats in response to equivalent restrictions placed on travel by U.S. diplomats in the Soviet Union. Little can be done about the number of Soviets employed by the United Nations in view of the large number of Americans similarly employed.[3]

There have also been reports of the U.N. Secretariat being used for clandestine activity by Warsaw Pack officials. Currently, State Department conditions for travel in the United States by U.N. Secretariat employees from the Soviet Union still do not apply to U.N. employees from other Warsaw Pact countries.

The hostile intelligence threat is further expanded by the number of Soviet bloc commercial entities in the United States that can be used as cover for clandestine collection activities. These commercial establishments include the USSR's AMTORG and INTOURIST, the Polish-American Machinery Company (Polamco), and similar East German, Czechoslovak and other East European entities. Through their legitimate business activities, intelligence officers in those firms have access to Americans in business, industry and government who are potential targets for agent recruitment. A Czech, Pole or other East European is frequently able to contact U.S. companies without arousing the suspicion that contact by a Soviet official would occasion. The primary interests of hostile collectors operating under commercial cover are economic data and

[3] For a more detailed discussion of the Soviets at the United Nations, see the Committee's report on *Soviet Presence in the U.N. Secretariat*, S.Rpt. 99-52 (May, 1985).

advanced technology. Altogether, nearly 70 U.S.-chartered corporations, although owned by Warsaw Pack countries, function legally as U.S. corporations and thus are subject to few restrictions on acquiring technologies. East Europeans employed by these firms are subject to no travel controls or notice requirements.

In addition to the threat posed by their official establishments, U.N. employees and front companies, hostile intelligence services have infiltrated intelligence collectors into the United States among the thousands of exchange students, commercial and cultural visitors, tourists and ship crewmen who enter this country each year. Some 2,000 Soviets come to the United States each year under the auspices of the Soviet Academy of Sciences, the Ministry of Trade, the State Committee for Foreign Economic Relations, and other Soviet agencies. They collect not only overt information for non-defense industries, but also classified and proprietary data, in response to intelligence tasking on behalf of military research projects. The number of U.S. universities and institutes subject to focused Soviet efforts reportedly increased from 20 to over 60 from the late 1970s to the early 1980s.

Soviet trade or scientific representatives travel to California about four times a month in delegations ranging from two to ten people, supplementing the 41-person staff of the Soviet San Francisco Consulate. It is reasonable to assume that, just as 30–40 percent of the personnel in each Soviet establishment are intelligence officers, the same percent of the personnel in a Soviet visiting delegation are intelligence officers and/or co-optees. Thus, the Soviets are able to target more intensively the 1,500 high-technology companies in the area known as "Silicon Valley," which constitute the largest collection of electronics and computer manufacturers in the United States.

In recent years, a number of intelligence agents of the USSR, Cuba and other countries have been uncovered among the flood of immigrants into the United States from Communist countries. While not all of these agents are considered classic "illegals," investigations have determined that many have been sent with intelligence missions.

The deep-cover "illegals" dispatched to the United States in the emigre flow and through other means by Soviet bloc and PRC intelligence services represent a particularly perplexing problem because of their completely clandestine manner of operation. They generally enter the United States under false identities with forged or stolen documents. They often acquire U.S. citizenship, and they have attempted to assume the appearance of ordinary Americans having no connection with their home country and intelligence service.

An example of a KGB illegal agent was disclosed publicly by the FBI in 1981. Col. Rudolf Hermann (a pseudonym) had earlier been identified and recruited to work as a U.S.-controlled double agent. Hermann's 25-year career with the KGB had begun in the 1950s while he was serving in the military of a Soviet-bloc country. His initial training in espionage techniques such as secret writing and cipher systems took place in East Germany. More advanced training was received in the Soviet Union.

Page 452 of 3957

Before coming to the United States, Col. Hermann practiced his intelligence skills in West Germany and Canada. He and his family entered the United States illegally in 1968, and he established a home and found work as a free-lance photographer. He did not directly collect classified information, but performed support functions such as locating drop sites for other agents and spotting potential recruits. He was also prepared to conduct more active collection operations in the event of the expulsion of Soviet officials in time of crisis or war. Col. Hermann's son had enrolled in an American college, under KGB orders, and was preparing to seek U.S. Government employment, possibly in a sensitive position.

3. Recruited Agents

Visitors and emigres are no substitute for recruited agents inside sensitive U.S. programs. The spy of the 1980s has been described as a new breed, motivated more by greed than by ideology. However, the cases uncovered in 1985 suggest more complex motivations; political beliefs, intrigue, and job dissatisfaction or alienation also appear to have been reasons for engaging in espionage. Most Americans arrested for espionage in recent years actually volunteered their services to the other side.

Soviet intelligence efforts include active programs outside the United States against U.S. Government personnel and businessmen. Even those recruited agents who live in the United States are frequently met in third countries to avoid U.S. domestic counterintelligence. Vienna, Austria, was used as the meeting place for John Walker, Ronald Pelton and Edward Howard.

KGB residencies abroad target principally American embassy employees with access to classified information. Other targets include American journalists, businessmen, and scientists who can furnish sensitive technological information, as well as students with job prospects in sensitive positions for long-range development.

The widespread use of foreign nationals in U.S. embassies and consulates compounds the problems faced by U.S. intelligence in most hostile countries. Over 9,800 foreign nationals are so employed for a number of reasons, including cost considerations. Despite their value in dealing with local government organizations because of their language fluency and understanding of local customs and regulations, their threat to the security of U.S. operations must be recognized.

The employment of foreign nationals in U.S. establishments in the Soviet Union and other Eastern European countries, as well as in numerous other countries where the Soviet bloc has influence, affords hostile security services the opportunity to conduct a variety of observations of U.S. personnel and technical penetrations of U.S. facilities. The foreign nationals' personal observations are used by the KGB to assess possible recruitment targets among the American personnel (e.g., those with financial, family, alcohol, or drug problems), as well as to identify U.S. intelligence personnel. The U.S. Embassy in Moscow faces particular problems in this regard. Soviet nationals operate the carpool, including making mechanical repairs and, until recently, operated the telephones, cleaned the offices, and performed all the maintenance tasks in the

Page 452 of 3957

embassy compound. Approximately 200 Soviets are employed at the embassy, contrasted to fewer than a dozen Americans in the Soviet establishments in Washington. The Soviets strictly limit the use of local hires in their own embassies—apparently concerned that if they can succeed, so could U.S. intelligence.

U.S. military installations and personnel abroad continue to attract major Soviet intelligence interest, both to gain potential access to military plans and to acquire sensitive technical data. It is probable that third-country nationals are used to target U.S. bases, just as they are at embassies. There are over 120,000 third-country nationals employed at such installations; and 930 of these have accesses, of which 371 are at the Secret level, to see certain classified material.

4. Soviet Methods of Recruitment

A study by the Defense Security Institute outlines some of the most common Soviet methods of recruiting and handling agents. The agents who steal most of the U.S. classified information lost through human espionage are not foreign nationals, legal or illegal, but Americans already employed in sensitive positions who are recruited, or who volunteer, to provide information to hostile intelligence services.

Social occasions and situations are a favorite hunting ground for Soviet bloc intelligence officers, such as diplomats or U.N. employees, on the look-out for potential recruits. So are restaurants, bars and clubs in the vicinity of defense contractor facilities. The intelligence officer looks for a combination of access to desired information and some motivating factor or factors that might be exploited for drawing a person into espionage. Ideological affinity is not frequently encountered, although it is a desired inducement. Blackmail is a last resort. The most common motivation is financial gain, often combined with conscious or unconscious anger at the employer.

In typical fashion, an intelligence officer proceeds with his cultivation of a prospect by stages, attempting to establish a pattern of payment for seemingly harmless services. The aim is to avoid scaring off the prospect with premature demands for classified information. After classified material is passed, the officer may shift the mode of communication from personal meetings to more secure methods such as "dead drops"—that is, the placement of a package in an inconspicuous agreed location where it can be picked up by the recipient at a later time.

Recruitment of this sort is a process of salesmanship, almost of seduction. Soviet intelligence officers vary in their skill, but some possess the finesse to do an effective job of cultivation without rushing the potential agent. Most of our information concerns the least successful recruitment attempts, such as those reported by persons who become FBI-controlled double agents. KGB training documents, however, describe instances of successful recruitment involving bribery of employees with sensitive access.

In one case cited in KGB training materials, an intelligence officer spotted a possible recruit while serving as interpreter for a Soviet scientist visiting the laboratory of a private U.S. company. The KGB account states that the scientist was aware of his inter-

preter's intelligence function and actively assisted him in that role. The intelligence officer's attention was drawn during the visit to a young lab assistant who seemed poorly dressed. When the Soviet scientist offered to provide copies of a number of his writings to the head of the laboratory, it was revealed that this assistant was studying Russian and could assist in translating the material.

On this basis the Soviet intelligence officer was able to cement an acquaintance with the young worker during the deliberately prolonged process of delivering the documents to the laboratory. As suspected, the lab assistant was having financial difficulties. He was married and attending graduate school and his job was a low-paying one. The KGB officer developed a friendship with him over the course of three months and then began requests for unclassified information in return for payment. Ultimately he persuaded the lab employee to join him in the formation of a consulting firm for the sale of scientific data, which the lab assistant would obtain and the KGB officer would market. In furtherance of this business venture, the lab assistant was persuaded to provide secret as well as unclassified information.

This recruitment approach reflects both subtlety and ingenuity. The prospective agent was never confronted with a stark proposal to spy for the KGB, but was gradually drawn into such activity through apparent friendship and an ostensibly legitimate business arrangement. Similar techniques apparently were used by Gennadiy Zakharov, the Soviet physicist employed at the United Nations who was arrested on August 23, 1986, for buying classified documents from an FBI-controlled double agent whom he had attempted to recruit. See Appendix E for the indictment and an FBI affidavit filed in this case. The recruitment of William Bell, which also used a consulting ploy, is described in Appendix C. The finesse with which a good intelligence officer can draw a person into espionage is a strong argument for informing the FBI when one is approached by foreign officials, as this Report recommends later. Advice from counterintelligence experts can help to prevent tragedies.

Recruitment is more commonly accomplished on the basis of positive inducement than by coercive approaches such as blackmail, which are the last resort for the hostile intelligence service. Blackmail produces the least satisfactory, because least willing, sort of agent. But such methods are nonetheless used with some frequency when preferable methods fail or are unavailable. This is particularly true outside the United States, and especially in Communist countries where hostile intelligence services control the total environment. Entrapment through contrived circumstances can easily be arranged. Sexual entanglements, currency exchange violations and black market involvement are favorite recruitment ploys. U.S. diplomatic personnel, among others, have been targets of hostile intelligence services using these techniques.

Visitors with intelligence value are routinely approached by provocateurs with proposals of this kind, and ensuing arrests or threats of arrest or exposure serve as leverage for enlistment in espionage. For example, employees of U.S. firms with defense contracts who visit the Soviet Union or Eastern Europe will be given special attention and assessment for possible intelligence exploita-

tion. Visa applications reveal where an American works, and falsification of such information is itself an offense that can be used against an American visitor. Whether active recruitment is attempted depends upon whether the American provides indications of susceptibility to inducement or coercion. While travel to Eastern Europe is not, for the most part, discouraged, those who go can reduce their vulnerability by not doing or saying anything that could be recorded or photographed for future reference in the archives of the KGB.

In the final analysis, however, the most dangerous agents of all, who account for the greatest losses of the most highly classified information, are not those who are laboriously recruited, but those who walk in the door of a Soviet embassy somewhere and volunteer information for sale. For the "walk-in" as for the recruited agent, the motivating factors are usually greed or indebtedness plus an additional element of grievance or disgruntlement. The individual usually is dissatisfied with his or her job or harbors some grudge against his organization or both.

Some characteristic signs that may betray an agent at work, if security people and co-workers are sufficiently alert, include:

Attempts to obtain information when there is no need to know and excessive curiosity about what others are doing;

Unauthorized removal of classified material from work areas or introduction of cameras or recorders into work areas;

Repeated overtime or unusual work hours not required by the job; and

Unexplained affluence.

Indicators of espionage are, unfortunately, generally much more noticeable in retrospect than during the course of the crime. In many cases, it is difficult to distinguish the spy from an exceptionally hard worker. But suspicious activities such as those listed, combined with job dissatisfaction or other disgruntlement, would certainly provide grounds for heightened attention to an individual's actions. It was sensitivity to such behavior, after receiving a security awareness briefing in the wake of the Walker-Whitworth arrests, that led Jonathan Pollard's co-workers to alert the FBI, resulting in his arrest and conviction for espionage. This Report later recommends both improved security awareness programs and, in some areas, personnel reliability programs that incorporate peer-group cooperation.

5. Technology Transfer

The Soviet drive to achieve technological equality with the United States and other Western countries has led the USSR to commit enormous resources to the acquisition of open-source information, unclassified but proprietary information, and high-technology equipment that the West has agreed not to export to the Soviet bloc. Soviet intelligence services actively engage in these efforts in addition to their pursuit of U.S. secrets. As a result, the Western lead in many key technological areas has been reduced, with serious economic and military consequences for the United States.

Moscow has devised two programs to obtain Western technology. The first, under the Military Industrial Commission (VPK) of the Presidium of the Council of Ministers, seeks to obtain military and

Page 456 of 3957

dual-use hardware, blueprints, product samples and test equipment to improve the technical levels and performance of Soviet weapons and defense manufacturing equipment. By adapting design concepts from the acquired hardware and documents, the Soviets reduce their own research and development costs. In the early 1980s, more than 3,500 requirements were levied by the VPK each year, with about one-third being satisfied. Some 60 percent of the most significant acquisitions were of U.S. origin, although not necessarily collected in the United States. Nearly half of the up to 10,000 pieces of military hardware and 20 percent of the 100,000 engineering and research documents the USSR acquires annually worldwide are used by the Soviets to incorporate Western technology into their military research projects. Most of the documents, about 90 percent of which are unclassified, contain patented or copyrighted proprietary information and are illicitly obtained.

The GRU is believed to have satisfied considerably more VPK requirements than the KGB. This success is attributed partly to the GRU's greater scientific orientation and its wider variety of technology-related cover positions. The approximately 1,500 GRU officers serving outside the USSR have scientific and technological collection as an integral part of their responsibilities. The KGB S&T unit, Line X, has nearly 300 officers on foreign assignment operating under cover of Soviet embassies, trade and commercial organizations, as members of exchange groups, and as employees of international organizations (the United Nations Secretariat, for instance, as in the case of Gennadiy Zakharov).

The second program, managed by the Ministry of Foreign Trade and the KGB/GRU, seeks, through trade diversions, to acquire relatively large amounts of dual-use manufacturing and test equipment for direct use on production lines. This program attempts to obtain export-controlled microelectronic, computer, telecommunication, machine-tool, robotic, diagnostic and other sophisticated equipment. This program also utilizes both legal and illegal means.

Major Soviet collection efforts are targeted at microelectronics fabrication equipment and computers; nearly one-half of detected trade diversions fall into these categories. The acquisition of much of the information concerning these high-technology areas is not particularly difficult. Information is often available to the public (and, therefore, accessible to the Soviets and their surrogates) from U.S. Government agencies.

The Soviets and their allied intelligence services have for many years been regular attendees of scientific, technical and industrial conferences in the United States and abroad. The Soviets considered some of the information obtained from these conferences to be among the most significant contributions to their military projects. The VPK identifies those having the most potential; in recent years, these have included conferences assembled by several well-known professional engineering societies.

In addition, the Soviet Ministry of Foreign Trade and academic-related collectors contribute to Soviet exploitation of open-source Western information. The Ministry of Foreign Trade has hundreds of trade organizations and companies around the world. KGB and GRU officers operating under cover of these establishments collect large quantities of data openly, in addition to that derived from

64-268 O - 86 - 2

Page 456 of 3957

their covert operations. The Ministry, as an independent collector, helped meet about 15 percent of all fully satisfied VPK requirements during the late 1970s and early 1980s. It specializes in acquiring microelectronics, manufacturing equipment and communications dual-use products.

Equipment is obtained through the use of dummy firms, false end-user certificates and falsifications of export licenses by the Soviets and professional trade diverters whom they hire. Many advances in Soviet microelectronics have been made possible by the illegal acquisition of equipment from the West. The result, according to U.S. Government estimates, has been a marked reduction in the Western technological lead from about 10–12 years a decade ago to about half that today.

Richard Mueller, a West German citizen, has been involved in illegal technology acquisitions for the Soviets for more than a decade. Using dummy and front firms, he has diverted advanced computers and microelectronics equipment of significant value to the Soviets. Mueller was the moving force in the 1983 attempted diversion to the USSR of several Digital Equipment Corporation VAX super mini-computers that would have assisted the Soviets in computer-aided design applications for microelectronics fabrication.

6. Active Measures and Disinformation

"Active measures" and "disinformation" are terms for Soviet covert action operations designed to implement Soviet policy goals by attacking U.S. policy and by promoting a positive image of the Soviet Union. They are significant weapons in the Soviet strategy to discredit and deceive the United States and its allies. The Soviets' principal techniques include the use of front groups, agents of influence, media manipulation and forgeries. The nature and scope of Soviet "active measures" was spelled out in detail in published hearings before the House Permanent Select Committee on Intelligence in 1982 and before the Senate Foreign Relations Subcommittee on European Affairs in 1985.[4] Deputy Director of Central Intelligence John McMahon testified that the Soviets have a $3–4 billion program to influence public opinion in countries throughout the world. It combines all forms of overt propaganda and covert political action, including systematic disinformation efforts.

"Disinformation" is a convenient label to describe a variety of techniques. The classic example is forged documents used to discredit the United States or to supply proof of Soviet propaganda claims. Another method is to recruit and pay agents in foreign news media to slant their reporting and plant false stories. The Soviets also secretly fund and control front organizations and individual agents to promote pro-Soviet or anti-U.S. positions. The Soviets themselves use the term "active measures" to describe their covert disinformation and political influence operations.

---

[4] *Soviet Active Measures*, Hearings before the Permanent Select Committee on Intelligence, House of Representatives, July 13–14, 1982, U.S. Government Printing Office (Washington: 1982).

Soviet Active Measures, Hearing before the Subcommittee on European Affairs, Committee on Foreign Relations, United States Senate, September 12–13, 1985, U.S. Government Printing Office (Washington: 1985).

It is also fair to say that most overt Soviet propaganda is also a form of disinformation because of its systematic distortion of reality to advance Soviet interests. Whenever a prominent Soviet citizen addresses a foreign audience, his or her remarks are likely to reflect a calculated effort to influence the audience. The same is true of Soviet print and electronic media.

Every country tries to sell its viewpoint. What distinguishes the Soviet effort are the immense resources and systematic controls that are employed. Two organizations develop and implement the Soviet "active measures" strategy: (1) the International Department of the Communist Party of the Soviet Union, which coordinates foreign policy and propaganda objectives and now includes most of the work of the Party's former International Information Department; and (2) Service A of the KGB's First Chief Directorate, which conducts covert political influence and forgery operations. The CIA has estimated that if the United States were to undertake a campaign the size of the Soviet "neutron bomb campaign" of the 1970s, it would cost over $100 million.

Currently, there is evidence of a major Soviet active measures campaign against U.S. development of the Strategic Defense Initiative (SDI). The Soviets are making every effort to convince a world audience that SDI will destabilize an already precarious superpower armaments balance. In addition, Soviet active measures directed at U.S. allies, such as in West Germany and Japan, are designed to sow distrust of American policies and to intensify financial and commercial rivalries with the United States by holding out the promise of favorable terms to the business communities in both countries. Such techniques are more subtle than blatant forgeries, which may be less effective in furthering Soviet objectives in sophisticated Western countries.

Soviet active measures efforts are focused primarily on Third World countries. The Soviets appear to employ massive active measures currently in South Asia, in an effort to depict the United States as interfering in the affairs of India, Pakistan and Bangladesh. The media in all three countries have consistently carried stories to this effect. One long-running disinformation ploy concerns alleged attempts by CIA to aid separatist movements in India, thereby splitting the country, supposedly to America's economic advantage. Another frequent theme is accusations of CIA biological warefare efforts in the region. Discrediting U.S. intelligence agencies, particularly the CIA, has long been an important objective of Soviet active measures.

In some cases Soviet active measures directly involve domestic U.S. matters. During July, 1984, for example, the Soviets began a widespread disinformation campaign to discredit the Los Angeles Olympic Games and booster worldwide support for their boycott of them. This campaign featured three forged documents purportedly from racist groups, threatening Third World athletes with bodily harm if they participated in the Olympic Games. Shortly after their discovery, then-Attorney General William French Smith announced that the letters were KGB forgeries and part of a major Soviet disinformation effort. It has been determined that these documents fit the pattern of other Soviet forgery operations and were

part of the overall Soviet active measures campaign to discredit the Reagan administration and its handling of U.S.-USSR relations.

A very recent forgery sought to implicate the Chairman of this Committee. In August, 1986, U.S. news media received copies of a forged letter purportedly from an official of the United States Information Agency to Senator Dave Durenberger, purporting to discuss a proposed plan to exploit the Chernobyl nuclear power plant disaster for propaganda purposes. Analysis of the forged letter revealed that the letterhead and signature had been taken from a copy of an entirely different letter from the USIA official to the President of the Inter-American Defense Board. Ironically, the USIA official's letter had alerted the President of the Inter-American Defense Board to an earlier forged letter, in Spanish, purportedly from the Board President to Chilean President Pinochet. The circumstances of the earlier forgery indicated Cuban-Nicaraguan involvment. (See Appendix F for copies of the forged letters and the true letter.)

According to the CIA's 1982 assessment, it is sometimes hard to judge the success of Soviet active measures because they "tend to capitalize on and manipulate existing sentiments that are parallel to or promote Soviet foreign policy objectives. Whenever a political movement supports policies that coincide with the goals or objectives of Soviet foreign policy, the exact contribution of Soviet active measures to that movement is difficult to determine objectively." The CIA cites evidence that the Soviets themselves believe that their efforts are worthwhile. They appear to consider the "neutron bomb campaign" in Europe to be one of the most successful. On the other hand, the more recent campaign against Pershing and cruise missile deployment in Europe had much less impact. The FBI has described Soviet operations in the United States, moreover, as "often transparent and sometimes clumsily implemented." The FBI also states, "The American media is sophisticated, and generally recognizes Soviet influence attempts."

As noted later in this Report, the U.S. Government has stepped up efforts to expose Soviet disinformation and covert manipulation worldwide. The State Department now regularly publicizes the facts about Soviet forgeries and Soviet control of political organizations such as the World Peace Council, the Christian Peace Conference, and the 12th World Youth Festival.

The most sensitive aspect of the disinformation threat is Soviet deception of U.S. intelligence as part of an attempt to confuse or to manipulate the perceptions of U.S. policymakers. The Soviet military doctrine of *maskirovka* and the KGB concept of *dezinformatsiya* both emphasize the need for measures to mislead opposition intelligence services and to create false perceptions that will influence Western policy and undermine strategic capabilities.

The U.S. intelligence community recognizes the danger of deception and has a community-wide program to assess systematically the possibilities of successful Soviet efforts. The deception threat has been a focus of the Committee's oversight in recent years, and the Committee continues to support intelligence community efforts to maintain vigilance in this area.

One major means of countering any Soviet deception efforts is to leave our adversaries uncertain regarding the full extent of U.S. in-

telligence collection capabilities. Steps to maintain the security of U.S. human and technical intelligence capabilities make it much more difficult for the Soviets to engage confidently or successfully in deception efforts.

D. TECHNICAL COLLECTION OPERATIONS

Hostile intelligence services use the full range of intelligence-gathering technologies to collect sensitive information from the United States and our allies. Public discussion of technical collection methods is more difficult than the explanation of human intelligence techniques, because we do not want to tell the Soviets just how much we know about their operations. Countermeasures against technical threats work best when the hostile service does not recognize U.S. defenses and continues to conduct operations that can be substantially neutralized. At the same time, however, wider knowledge of the technical collection threat is essential to develop better security awareness and to explain the need for major resource investments. Technical threats include the interception of communications, other forms of electronic surveillance, collection of emanations from equipment, penetration of computer systems, and photoreconnaissance.

1. Interception of Communications

The interception of electronic communications and deciphering of machine-generated codes played a vital role in Allied intelligence during World War II—although the methods of collection were so sensitive that many aspects of these operations remained secret for thirty years after the war. An Anglo-American team of top mathematicians and cryptologists provided Allied commanders with vital realtime intelligence on German and Japanese intentions and plans. The interception of electronic communications and the computer-assisted assault on crytographic systems remains a central part of present-day signals intelligence.

The Soviet electronic monitoring effort represents a significant worldwide threat to U.S. military and civil telecommunications. This threat derives from large collection facilities that are operated in the Soviet Union, as well as in other countries around the world, such as Cuba. The Soviets also maintain a fleet of intelligence collection vessels that operate worldwide—including off both coasts of the United States. The latest of these vessels has been built from the keel up specifically for this role, unlike earlier ships that were reconfigured trawlers or other types of vessels. The Soviets also use merchant ships and possibly commercial aircraft to perform collection operations against targets of opportunity.

A serious threat is posed by the Soviet intelligence collection facility located at Lourdes near Havana, Cuba. Established in the mid 1960s, the site has steadily grown to its present size of about 2,000 technicians and is the most sophisticated collection facility outside the Soviet Union.

Evidence of the seriousness of the threat to electronic communications was emphasized by the issuance in 1984 of National Security Decision Directive No. 145, which concluded that "the compromise of U.S. information, especially to hostile intelligence services,

does serious damage to the United States and its national security interests."

The technology to exploit U.S. electronic communications is widespread, and many foreign countries use it extensively. Currently, more than half of all telephone calls in the United States made over any distance are vulnerable to interception. Calls that the caller believes to be on less vulnerable circuits may be automatically switched to more vulnerable ones. The Soviet diplomatic facilities at their Riverdale complex in New York City, at their consulate in San Francisco and at their new Mt. Alto embassy in Washington all occupy high ground, thus providing superior opportunities for communications intercept. The "Silicon Valley" concentration of high technology centers and the government's sensitive facilities in Washington and New York are at risk of intercept because of these Soviet sites.

It is especially important for civilian agencies and the private sector to understand the nature of the risk from Soviet interception of their communications. The Defense Department and the CIA have elaborate programs to inculcate communications security awareness and to protect classified communications links. The massive Soviet surveillance efforts from Cuba and elsewhere demonstrate, however, that the Soviet intelligence payoff from interception of unsecured communications is immense. One reason is that too many government officials and contractor employees discuss classified matters on unsecure lines because of the difficulty and expense of using currently available secure communications equipment. Another significant problem is the Soviet ability to exploit unclassified pieces of information that are relatively harmless in isolation, but in the aggregate provide highly damaging insights into U.S. capabilities. The Committee's classified Report contains several examples of how both industrial and national security can be harmed by such intercepts.

Public awareness of the hostile intelligence threat to domestic communications is essential, because there are real limits to what the U.S. Government can do to provide secure communications for the private sector. Although this Report later discusses some government initiatives, the protection must depend on the willingness of private organizations to invest in secure communications, not only for their immediate self-interest, but for the larger interests of the nation as a whole.

2. Other Forms of Electronic Surveillance

The Soviets have a long history of electronic attacks on the U.S. Embassy in Moscow, dating back to the 1950s when a replica of the Great Seal of the United States in the embassy was found to contain an audio device. In the late 1970s, a Soviet antenna was found in the chimney of the chancery. Additionally, Soviet and other hostile intelligence services try to gain access to office or communications equipment in order to "read our mail."

The vulnerability of the U.S. Embassy in Moscow was dramatized vividly by the recent discovery of the technical compromise of embassy typewriters. The typewriters were shipped to the Soviet Union by unaccompanied commercial means, thus affording the Soviets access to them. The compromised typewriters were used in

Page 462 of 3957

the embassy for a significant period. What made this incident especially astonishing was that it occurred despite a similar discovery in 1978, when security officers found that a shipment of IBM Selectric typewriters destined for the U.S. Embassy had been shipped from Antwerp to Moscow by a Soviet trucking line. The potentially compromised equipment identified in 1978 was returned to the United States before being placed in service. Unfortunately, the Soviets again gained access to several similar IBM machines that were not recognized for a substantial time as being compromised.

As noted earlier, foreign nationals with access to U.S. embassies and other establishments abroad provide a means for hostile intelligence services to make other electronic penetrations. Offices, residences and cars are all vulnerable to the planting of audio or video devices by foreign nationals with access, legitimate or otherwise, to the U.S. target.

Although all high technical threat U.S. diplomatic posts have eliminated the authorized access of foreign nationals to the vicinity of classified work areas, there remains a serious problem of common walls with uncontrolled adjacent areas from which technical attacks and even physical entries can be mounted. Offices and residences are also vulnerable to planted devices when access by foreign nationals is not properly monitored and technical countermeasures are not routinely employed.

In 1985, the Secretary of State's Advisory Panel on Overseas Security, chaired by Admiral Bobby R. Inman, provided to the Intelligence Committees of the House and Senate a classified annex to its report, covering, electronic and physical penetration of U.S. diplomatic facilities. The Inman Panel described the Soviet technical surveillance effort as "a technologically advanced and sophisticated program obviously supported by tremendous resources." The report went on to describe scores of discoveries of Soviet and Soviet-bloc technical exploitation of U.S. diplomatic premises. Noncommunist host nationals have also been detected mounting technical penetrations of U.S. missions.

The threat to office and communication equipment from the exploitation of unintended emissions is greater at U.S. facilities abroad than in the domestic environment, where the risks and costs of detection are considerably higher. Consequently, as noted by the Stilwell Commission on DoD Security Policies and Practices, the previously rigid requirements for expensive equipment shielding have been modified to prescribe shielding only when inspection verifies that a threat exists. There is, however, no question that such a potential threat does exist at especially sensitive locations in this country.

3. Penetration of Computer Systems

The hostile intelligence threat to U.S. computer systems is magnified by the enormous growth in the number and power of computers and the vast amount of data contained in them. The General Services Administration has estimated that the number of U.S. Government computers has increased from 22,000 in 1983 to over 100,000 in 1985. The increase in the number of computers in use in industry, business and other private sectors has been equally stag-

Page 462 of 3957

gering. Computers multiply enormously the information to which a single individual may obtain access.

There is a real possibility that the Soviets may exploit these vulnerabilities. Computers and computer software are high-priority items of both the VPK's and the Ministry of Foreign Trade's technology acquisition programs by legal or illegal means. The Soviet and other Warsaw Pact intelligence services have also obtained information concerning the methods used in the West to provide computer security, and constantly seek more knowledge. Over the past decade, the Soviets have acquired over 300 different types of U.S. and other Western computer hardware and software, which has enabled them to develop the technical ability to penetrate at least some U.S. automated systems. The Soviets are making a concerted effort to access state-of-the-art computers, including supercomputers.

The first Annual Report of the National Telecommunications and Information Systems Security Committee, completed in September, 1985, emphasized the challenge of computer security in both government and the private sector:

> Future technologies, particularly the growth of desktop computers, the increased local storage of data and the widespread networking, will exacerbate existing security vulnerabilities as well as create new ones. As this technology has grown, the resources and awareness needed to allow security technology to grow with it have not kept pace. The use of traditional COMSEC, physical security, personnel security, and administrative security protection techniques does not sufficiently protect the type of information-sharing that is becoming increasingly common in new automated information systems, especially distributed processing and networked systems.
>
> As storage costs decrease, the amount of data stored at the mainframes increases, creating more appealing targets. As the uses of networks and remote access expand, more and more users will have potential access to a broader range of information. As end-users of computers continue to increase their technical competence and computer literacy, the technical and management automated systems security task of protecting data and controlling users has fallen even further behind.

The NTISSC Annual Report admitted that "the full extent of the threat to and vulnerabilitis of automated information systems is unknown." Specific cases of unauthorized access to government computer systems have been detected and reported widely, including cases of access to and manipulation of Defense Department data in order to divert military equipment and weapons. There is no reason to believe that hostile intelligence services or their agents will ignore similar opportunities.

4. Imagery

The final category of technical intelligence collection is photographic or imagery intelligence—collection by means of overhead vehicles against adversary installations. The history of this disci-

pline dates to the use of observation balloons as platforms for photography during the Civil War and then use of aircraft for the same purpose during the two World Wars. The use of U-2 aircraft for imagery collection was extensively publicized in the 1960s. Today U.S. and Soviet imagery intelligence is collected primarily by satellite. The use of photographic satellites by both sides has gained wide recognition in the context of verification of compliance with arms control limitations.

Intelligence collection against the United States and U.S. interests worldwide using photographic means, or imagery, is carried out principally by the Soviet Union (with some assistance from its Warsaw Pact allies and Cuba). The Soviet imagery effort is mainly conducted from spaceborne and airborne platforms. The continued proliferation of Soviet satellites has given the USSR the concomitant capability for increased photoreconnaissance of its most obvious targets—U.S. and NATO strategic and tactical military forces, and crisis situations any place in the world. In addition to these uses of photoreconnaissance, the Soviets employ it to conduct earth resource surveys for economic and agricultural data.

Soviet spaceborne satellite reconnaissance capabilities are supported by the capability of military and civilian aircraft to collect photographic intelligence. The potential value of airborne reconnaissance conducted by the Soviet airline Aeroflot, which, in April, 1986, resumed operations to the United States, and by other Warsaw Pact national airlines' flights remains of concern. These Communist country overflights in the United States are under the jurisdiction of an FAA committee.

The Soviets continue to pursue intelligence-related manned space programs. In February, 1986, they launched a new type of modular space station, the MIR, replacing the older SALYUT-type modules. The MIR, as did the SALYUT, gives the Soviets the capability to perform a number of functions in space, including the use of cosmonauts to augment their other reconnaissance and surveillance efforts. The apparent military usefulness of their manned space program has been indicated in the Soviet announcement that "earth surface surveys" have been conducted; however, no photographs were ever published.

The seriousness of the imagery collection threat posed by Soviet and Bloc overflights in the NATO area can be illustrated by two examples. In March 1985, Norway banned or restricted Soviet and Bloc passenger airplanes from several airports on the basis that they were conducting electronic surveillance. Bulgarian aircraft were specifically mentioned as having departed from scheduled routes to overfly sensitive areas. In West Germany, some 1,500 Soviet Bloc overflights occurred in a three-month period in 1985, offering a tremendous opportunity for both electronic and photographic reconnaissance.

E. SUMMARY

Until the espionage arrests and disclosures of technical security compromises in 1985, the American people and most Government officials did not fully appreciate the magnitude and intensity of the hostile intelligence threat, despite previous espionage prosecutions

and knowledge of the vulnerability of U.S. communications to Soviet intercept operations. The barrage of revelations in 1985–86 has changed these perceptions, so that today there is a better recognition in Government and in the private sector of the continuing efforts by hostile intelligence services to collect sensitive information by human and technical means. There is also a greater awareness of Soviet efforts to influence the political process through "active measures" directed at countries throughout the world.

The Committee intends that this description and analysis of the hostile intelligence threat serve as a benchmark against which to measure further evolution of the threat in the years ahead and the effectiveness of counterintelligence and security programs. It is also important that the American people—especially responsible officials of private organizations in business and industry, science and technology, and international affairs—remain aware of the changing threat from foreign intelligence services. Such awareness does not mean exaggerating the dangers or engendering an atmosphere of suspicion. Rather, it is part of a mature understanding of the reality of U.S. relations with other countries in the world of competing national interests. The political and military rivalry between the Soviet bloc and the West is a fact of life that requires constant attention to ongoing and emerging Soviet bloc intelligence operations.

The hostile intelligence threat is, of course, only half the equation. On the other side are U.S. activities to counter this threat: counterintelligence, to uncover and to neutralize hostile intelligence activities; and security, to protect against both known and undiscovered hostile efforts by setting obstacles in the path of anyone seeking unauthorized access to sensitive information, activities, equipment or facilities. The rest of this Report examines the nature and effectiveness of those critical U.S. programs.

III. Counterintelligence

An effective response to the foreign intelligence threat requires a combination of counterintelligence and security measures. The Committee believes it is important to distinguish between counterintelligence efforts and security programs, while ensuring that both are part of a national policy framework that takes account of all aspects of the threat. The best way to explain the difference is to say that counterintelligence measures deal directly with foreign intelligence service activities, while security programs are the indirect defensive actions that minimize vulnerabilities. The FBI, CIA, and the counterintelligence components of the Defense Department have primary responsibility for operations and analysis dealing directly with foreign intelligence services. In addition, the Committee and the Executive branch have included within the national counterintelligence policy structure those diplomatic and regulatory policies that control the numbers and movements of particular countries' foreign intelligence service officers and co-opted agents in the United States and at U.S. facilities abroad.

Page 466 of 3957

A. NEED FOR A COUNTERINTELLIGENCE STRATEGY

By statute and executive order, counterintelligence functions are divided among the FBI, CIA, and components of the Defense Department. The FBI has the lead within the United States, while the CIA is in charge abroad. The Defense Department, which deals with threats to classified defense information worldwide, divides its counterintelligence functions among the military services, DIA, and NSA. No single official is responsible for the full range of counterintelligence activities below the level of the President and his National Security Adviser. Given these circumstances, there is a constant risk of fragmentation and conflict among organizations with different methods and priorities.

The Committee has found that communication and cooperation among U.S. counterintelligence agencies have improved greatly in recent years and are probably better today than at any time since World War II. Nevertheless, more needs to be done to ensure that agencies learn from each other's experiences and that progress achieved in one area can have benefits for others. The issue is not just communication and operational coordination to bridge jurisdictional boundaries. Better long-range planning is also needed to make optimal use of limited resources worldwide against well-organized and sophisticated adversaries.

Soviet bloc and PRC intelligence operations do not respect geographic boundaries. Thus, in many recent cases Americans who committed espionage in the United States met their foreign intelligence service contacts abroad. The targets and techniques needed for counterintelligence success transcend agency jurisdictions. For these and other reasons, the Chairman and Vice Chairman of the Committee stated in October, 1985, that the Executive branch should develop a national counterintelligence strategy that establishes national objectives and integrates the planning and resources of each agency to achieve these objectives. The President's interim report to the Intelligence Committees indicated agreement with this proposal, and in fact the Executive branch is now preparing such a document.

The organizational structure is already in place, fortunately, to develop a national counterintelligence strategy. Under the National Security Council, there is a Senior Interdepartmental Group for Intelligence (SIG–I) chaired by the Director of Central Intelligence. Within that framework, an Interagency Group for Counterintelligence (IG–CI), chaired by the FBI Director, develops national policy recommendations and provides a forum for agreement on new initiatives. A small secretariat for the IG–CI has expert personnel drawn from the FBI, CIA, and Defense Department. This staff evaluates the threat and recommends policy initiatives for counterintelligence and countermeasures improvements.

The IG–CI, assisted by its secretariat, is the proper place to develop a national counterintelligence strategy. This structure ensures joint participation by the FBI, CIA and Defense Department; and other interested departments and agencies (such as the State and Justice Departments) are also represented on the IG-CI. Ultimate responsibility for resolution of policy issues rests with the Na-

Page 466 of 3957

tional Security Council, which has recently brought onto its staff an experienced FBI counterintelligence specialist.

The President's interim report to the Intelligence Committees indicates that the IG-CI has, in fact, been tasked to frame strategic guidance of the sort proposed by this Committee. As noted earlier, member agencies are now engaged in the drafting process.

Findings and Recommendations

1. Findings.—The IG-CI has been chartered to frame national counterintelligence objectives and an associated strategy (or master plan) to further those objectives, and to submit the objectives and plan for consideration by the SIG–I and thence the NSC. The Committee is pleased to learn that Executive branch agencies are actively drafting this document. This is a positive response to proposals presented by the Chairman and Vice Chairman in testimony before the Permanent Subcommittee on Investigations in October, 1985.

2. Recommendation.—The National Security Council should approve a statement of major counterintelligence objectives and a strategy, i.e., a time-phased master plan, to attain those objectives. The House and Senate Intelligence Committees should receive this document. An effective oversight mechanism should be established to ensure that major programs and associated budgets, legislative proposals, and other key actions are validated against the master plan, constitute judicious and operationally efficient allocation of resources, and achieve all feasible synergism. There should also be a process for continuing review and evaluation.

3. Recommendation.—The National Foreign Intelligence Program should provide for, and Congress should authorize, augmentation of the staff that assists the IG–CI to ensure effective performance of its expanded responsibilities regarding the development and implementation of the national counterintelligence strategy.

B. HOSTILE PRESENCE LIMITS

An effective national counterintelligence strategy should include diplomatic and regulatory policies that control the numbers and movements of hostile intelligence service officers and co-opted agents in the United States and at U.S. facilities abroad. Each year, in the formal classified justification for funds for its Foreign Counterintelligence Program, the FBI advises Congress that, even with increased resources, the FBI cannot cope with the hostile intelligence threat unless measures are also taken to reduce the number of potential intelligence officers in this country. Where the numbers cannot be reduced, controls on their movements can assist the FBI in making better use of limited resources.

The Foreign Missions Act of 1982, which created a new Office of Foreign Missions in the State Department, provided the authority to exercise greater control over the activities of foreign officials in this country. Although such control is normally exercised within the framework of diplomatic reciprocity, the Act also facilitates actions to enhance U.S. security and counterintelligence interests. Limits on numbers of foreign representatives allowed into the United States are usually left to Executive branch discretion, but

the Leahy-Cohen amendment in 1985 established a policy of equivalence between the number of Soviet embassy and consular personnel in the United States and the number of U.S. embassy and consular personnel in the Soviet Union. The 1985 Roth amendment provided for regulation of travel by U.N. Secretariat personnel from countries whose diplomats are subject to such regulations under the Foreign Missions Act.

National Security Decision Directive (NSDD) 196, signed by the President on November 1, 1985, established national policy objectives for restricting and controlling the hostile intelligence presence and travel in the United States. In addition to implementing the Leahy-Cohen and Roth amendments, the Administration has imposed Foreign Missions Act travel regulations on representatives of Warsaw Pact countries whose intelligence services act as Soviet surrogates, has begun reducing the number of Soviet representatives in the United States, and has supported extension of Foreign Missions Act controls to commercial and other entities used by hostile intelligence services in this country. Consistent with these Presidential objectives, Committee Members introduced legislation to establish a policy of equivalence for the size of the U.S. and Soviet Missions to the United Nations (Leahy-Cohen), to broaden the scope of the Foreign Missions Act to cover commercial and other entities controlled by foreign governments (Durenberger-Leahy), to require registration by commercial entities controlled by Warsaw Pact governments (Roth–Nunn), and to require imposition of Foreign Missions Act travel regulations on representatives of Warsaw Pact countries (Roth–Nunn).

The 1985 Roth amendment has been implemented by imposing travel restrictions on U.N Secretariat representatives/employees from the Soviet Union, Afghanistan, Vietnam, Libya, Iran and Cuba. The State Department's Office of Foreign Missions Travel Bureau Service has been required for use by U.N. Secretariat personnel from East Germany, Czechoslovakia, Bulgaria, and Poland. Most recently, it was publicly announced that effective October 1, 1986, the Soviet Missions to the United Nations will be required gradually to decrease their size from 275 to 170, to be accomplished by April, 1988.

In 1986, the Committee received three reports on Executive branch efforts to control the hostile intelligence presence. The first was a report on the respective numbers and treatment of officials from countries that conduct intelligence activities in the United States contrary to U.S. interests and the numbers and treatment of U.S. officials in those countries. Under the Leahy-Huddleston amendment of 1984, this requirement covers the Soviet bloc, Cuba, China, and any other nation designated on the basis of the threat posed by its intelligence or terrorist activities. The second was a report from the Secretary of State and the Attorney General on plans for implementation of the policy of substantial equivalence between U.S. and Soviet embassy and consular personnel pursuant to the Leahy-Cohen amendment of 1985. The third was the annual report of the State Department's Office of Foreign Missions, which regulates many aspects of the treatment of foreign government establishments and officials in the United States.

These reports reflect uneven progress in limiting the hostile intelligence presence in the United States. While the planned reduction in the size of the Soviet U.N. mission is an important step forward, the intent of the Committee in recommending the Leahy-Cohen amendment was also to reduce the number of Soviet embassy and consular personnel in the United States. The plan for implementation of diplomatic equivalence does not achieve that objective. Instead, there is a potential for actually increasing the number of Soviet embassy and consular personnel in the United States if the State Department carries out its plan for a Soviet consulate in New York and permitting a U.S. consulate in Kiev. According to the plan received by the Committee, the number of Soviet diplomatic and consular officials will increase from 320 to as many as 350, depending on the number of Americans sent to Kiev. Current plans call for thirty U.S. officials in Kiev. Apart from the merits of the need for so large an establishment in Kiev, the Committee believes that at a minimum the Soviets should be required to staff their New York consulate within the 320 ceiling on overall representation in the United States. The State Department should plan accordingly to staff the U.S. embassy and consulates in the Soviet Union within a comparable 320 ceiling.

The Committee supports the State Department's plan to reduce the Soviet work force at the U.S. Embassy in Moscow. This plan would also allow the staffing of a small consulate in Kiev within the 320 ceiling and still permit some reduction in Soviet embassy and consular positions in the United States. Such reductions could be made, for example, by refusing to allow the Soviets to replace officials expelled from the United States for espionage-related activity. Further reductions should be possible as the Americans who replace Soviet employees learn to do their jobs more efficiently.

Apart from issues of numerical equivalence, the State Department through the Office of Foreign Missions has made considerable progress in imposing more effective controls. In addition to regulating the travel of Soviet bloc representatives and U.N. Secretariat personnel, the Office of Foreign Missions (OFM) is requiring Soviet bloc embassies to secure prior OFM approval of purchases or leases of property for housing as well as business purposes. A Soviet request to construct a new apartment building in their existing compound in Riverdale, New York, has been denied because it is deemed excessive to Soviet housing needs. On May 28, 1985, the Soviets were advised that their procurement within the United States of building equipment, materials, or services for the remaining construction work at their Mt. Alto site in Washington, D.C., must be arranged through OFM. In response to a Soviet request to expand its recreational facilities at Pioneer Point, Maryland, OFM has told the Soviets they must abide by the same terms and conditions applied to construction on the site of U.S. Embassy recreational property in Moscow.

The Committee believes the OFM program is one of the most important recent counterintelligence initiatives, and is recommending legislation to broaden OFM's authority to impose travel controls on certain Soviet bloc-controlled businesses located in the United States. The Committee also supports OFM's plans to require Soviet bloc missions to lease residential units from OFM, to purchase tele-

Page 470 of 3957

communications goods and services through OFM, and to use OFM banking services. OFM's effectiveness will be enhanced by the Administration's decision to give Ambassador status to its current Director. (By law, his successor will have such status.) The Committee supports the decision to make this appointment, so as to strengthen the Director's ability to deal with foreign representatives.

The need to combat the hostile intelligence presence must also be taken into account in developing policies and regulations for exchange programs. There is clear evidence that some exchange visitors are used for clandestine intelligence purposes. While foreign policy considerations may dictate greater openness between the United States and certain countries, they must be balanced against the counterintelligence risks. The President's interim report to the Intelligence Committees states that efforts are made to do this.

Overseas, the hostile presence problem has three separate dimensions. The first is employment of Foreign Service Nationals (FSNs) at U.S. diplomatic missions. While most attention has been focused on the large number of Soviet nationals employed at our Embassy in Moscow, similar concerns arise in other countries. The Inman Panel on Overseas Security recommended reducing the number of FSNs at embassies in other Warsaw Pact countries and segregating them from sensitive areas and positions in other missions. The State Department has developed a plan to reduce the number of FSNs in Moscow to 95 and to begin such reductions elsewhere.

The Committee supports both the Moscow effort and the modest FSN reductions planned in Eastern Europe. The Administration requested $6.3 million for FY 1986 and $28.3 million for FY 1987 to meet the costs of such staffing changes; the urgent supplemental appropriations bill met $12.0 million of that need. The Committee urges the State Department to reprogram the remaining needed funds, especially if construction funds appropriated in the urgent supplemental cannot be fully expended in FY 1987.

A second aspect of the problem is the employment of over 120,000 foreign nationals at U.S. military installations. Close to 1,000 of these personnel have access to some classified information; roughly 370 have access to some Secret material. The Stilwell Commission recommended stricter personnel security safeguards in such cases, and consideration should also be given to reducing the military's reliance on foreign nationals, who are much more likely to be recruited by a foreign intelligence service than are U.S. personnel. The Committee recognizes that status of forces agreements limit the hiring of U.S. citizens to perform unclassified work at overseas bases, but the number of foreign national employees with authorized or unauthorized access to classified information can and should be reduced to the minimum feasible level. The Committee supports the tighter investigation requirements for foreign employees that have been recommended by the Stilwell Commission.

The State Department plays a key role in developing and implementing these policies and in ensuring that they take into account other U.S. foreign policy objectives. Components of the State Department vary in their understanding and appreciation of counterintelligence concerns. It is important to provide better training and other information on the foreign intelligence threat to State Department officials. While the State Department is not a counterin-

Page 470 of 3957

telligence agency, its officials should be kept fully apprised of the threat so they can be better prepared to support Foreign Missions Office and other policies designed to implement a national counterintelligence strategy.

Findings and Recommendations

4. Recommendation.—Recent Administration initiatives and legislation (Leahy-Cohen amendment, Roth amendment) should be implemented in a manner that places effective limitations on the numbers and activities of hostile intelligence service personnel in the United States and takes into account our foreign policy and intelligence collection efforts. The limit of 320 on permanently accredited. Soviet embassy and consular personnel should not be increased, and the State Department should plan to staff the U.S. embassy and consulates in the Soviet Union so as to require some reduction in Soviet embassy and consular personnel in the United States.

5. Recommendation.—Congress should enact legislation establishing a policy of substantial equivalence between the size of the Soviet and U.S. missions to the United Nations in line with the Administration's plan to reduce the size of the Soviet U.N. Mission.

6. Recommendation.—Congress should strengthen the authority of the Office of Foreign Missions to regulate commercial and other entities controlled by foreign governments and require registration of commercial entities controlled by Warsaw Pact governments.

7. Recommendation.—The Committee supports efforts through the Office of Foreign Missions to enhance U.S. counterintelligence effectiveness, including new initiatives to require Soviet bloc missions to acquire residential property, telecommunications services and equipment, and banking services through OFM. The Committee also supports the granting of Ambassador status to the current OFM Director.

8. Recommendation.—Policies and regulations for exchange programs with other countries should take counterintelligence concerns into account.

9. Recommendation.—The State Department should reprogram whatever funds are needed to supplement the $12.0 million appropriated through FY 1987 to implement plans to replace a substantial number of Foreign Service Nationals with Americans at U.S. missions in the Soviet Union and other high-risk countries. The Defense Department should reduce the use of foreign nationals with access to classified information at DoD installations abroad, and Congress should appropriate sufficient funds to replace them with Americans. Funds for this purpose should be requested in the FY 1988 budget, and DoD should determine what changes may be required in mandated military ceilings overseas.

10. Finding.—In conjunction with the CIA, FBI and DoD counterintelligence components, the State Department should have a program of formal training sessions, briefings and intelligence reporting arrangements to provide more and better information to State Department officials on the foreign intelligence threat and U.S. counterintelligence requirements. The Committee notes with pleasure that progress is being made in this area.

C. COUNTERINTELLIGENCE AWARENESS PROGRAMS

One key to a successful counterintelligence strategy is thorough analysis of the hostile intelligence threat and communication of the results to those who need to take countermeasures. Current efforts range from the FBI's Development of Counterintelligence Awareness (DECA) program for briefing defense contractors to the improved assessment of Soviet deception, disinformation and active measures. Informing the public, industry and other government agencies can have a direct payoff, as in the case where a student at Columbia University contacted the FBI about a Bulgarian exchange visitor after seeing a TV documentary on espionage that described conduct similar to that of the Bulgarian. The student's report led to an FBI offensive double agent operation resulting in the arrest of a Bulgarian intelligence officer. At a classified level, U.S. counterintelligence agencies must work with a great variety of government programs and security officials to provide tailored information and analysis.

On November 1, 1985, the President issued NSDD-197 requiring each U.S. Government agency to establish a security awareness program for its employees, including periodic formal briefings on the threat posed by hostile intelligence services, and to provide for the reporting of employee contacts with nationals of certain foreign powers. These programs are to be tailored to the sensitivities of particular work and designed so as not to intrude into employees' privacy or freedom of association.

According to the NSC staff, department and agency heads have responded positively and have given high priority to this enterprise. The State Department contact reporting directive, which has been provided to the Committee, serves as a good model because it specifies reporting procedures clearly and identifies those countries that require the greatest attention. Civilian agencies without extensive national security responsibilities also appear to be taking this policy initiative seriously.

The Committee strongly supports this policy and is recommending that a similar security awareness program be established for the U.S. Senate. The Committee has used the State Department's new program as its model.

The Larry Wu-tai Chin case highlighted the threat posed by Chinese intelligence operations. As indicated in section II of this Report, however, the PRC intelligence threat differs greatly from the Soviet one. These differences require development of new counterintelligence approaches geared to the special characteristics of the PRC threat. In particular, the FBI should develop specialized threat awareness briefings geared to the unique problems posed by PRC operations. At the same time, FBI threat awareness programs do not—and should not—leave the implication that lawful association with or assistance to Chinese technical and scientific researchers is a sign of disloyalty to the United States.

Another aspect of counterintelligence awareness is the knowledge by agency security officials of when to bring a matter to the attention of a U.S. counterintelligence agency. In the Edward Lee Howard case, CIA security officials failed to alert and involve the FBI in a timely fashion. The CIA has taken steps recently to guard

against a recurrence of this problem. The FBI should continue to work closely with security officials of all U.S. Government agencies to ensure that they understand its requirements and guidelines. A good example is the Pollard case, where the Naval Investigative Service Command brought in the FBI at an early stage. The Committee is pleased that the Navy has given a commendation and a monetary award to the official who was responsible for bringing the FBI into the Pollard case promptly when certain questionable behavior was observed.

The lessons of the Howard and Pollard cases should be extended to all departments and agencies that handle highly sensitive information. Interagency procedures for reporting suspicious conduct to the FBI should be strengthened. Moreover, the Howard and Pelton cases demonstrate that former employees with grievances or financial problems can compromise our most sensitive national security programs. Individuals who choose to work in positions as sensitive as those occupied by a Howard or a Pelton should expect to be held to a higher security obligation than personnel with access to less sensitive information. Therefore, the FBI should be informed when employees with access to extremely sensitive information resign or are dismissed under circumstances indicating potential motivations for espionage. The decision as to whether the circumstances justify investigation in varying degrees should be made by the FBI, in light of its counterintelligence experience, not by the employing agency. Interagency procedures should be established to address borderline cases.

Threat analysis functions are shared among U.S. counterintelligence, foreign intelligence and security agencies. Development of an effective national counterintelligence strategy, as well as a comprehensive and balanced set of security measures, requires centralized assessment of the threat posed by all forms of collection—technical as well as human. Since 1981, an interagency staff has compiled assessments of the hostile intelligence services threat and U.S. countermeasures, based on inputs from throughout the Government. The Committee has found these assessments to be increasingly valuable and is pleased that they continue to have high priority.

National assessments are no substitute, however, for high-quality threat assessments tailored to meet more specific needs. The Committee is pleased to learn that progress is being made regarding one such need for tailored material that was highlighted in the most recent interagency assessment.

DoD counterintelligence agencies have taken the lead in analyzing the threat to particular military installations and activities. The Committee supports increased efforts in this area, especially to assess the threat to highly sensitive research and development projects and to make the findings available to the officials responsible for security countermeasures. In recognition of the importance of this function, the Stilwell Commission has recommended, and the Secretary of Defense has directed, that the Defense Intelligence Agency establish a Multidisciplinary Counterintelligence Analysis Center as a service of common concern for DoD to meet the counterintelligence analytic requirements of the Defense Counterintelligence Board and the various DoD components. DIA should have

the task of ensuring that other agencies' threat assessments are responsive to security and program management needs of DoD components. Efficient allocation of limited security resources depends on careful evaluation of the threat.

Special attention is required for two aspects of the hostile intelligence threat that directly relate to U.S. foreign intelligence analysis: deception; and "active measures," including disinformation, forgeries and other political influence operations. Hostile intelligence services conduct these operations in addition to their collection efforts.

An interagency committee and a community-wide intelligence analysis office are both active in the analysis of deception efforts. Pursuant to the Committee's classified reports accompanying the Intelligence Authorization Acts for FY 1985 and FY 1986, a small interagency staff has been assigned to the analysis office.

In recent years, with the help of the intelligence community, the State Department has stepped up efforts to expose Soviet "active measures," such as forgeries and Soviet control of political organizations and conferences abroad. The Committee supports recent initiatives to improve intelligence support for U.S. efforts to counter these Soviet activities.

The State Department and other appropriate agencies should do more to disseminate the results of such analyses to opinion leaders and policymakers worldwide. Recent steps to increase the effectiveness of the Active Measures Working Group, which is chaired by State/INR, are welcomed by the Committee. The Working Group has briefed U.S. embassies on its role, encouraged the formation of embassy committees to monitor and combat Soviet active measures, and arranged for both classified and unclassified guidance to be provided to the field on specific cases. These efforts should be supported and fully staffed by the relevant agencies, especially the State Department. The Committee is pleased that a new office has been established recently in State/INR for this purpose.

The FBI prepares reports and testifies before Congress on efforts in the United States by the Soviets and other designated countries to influence public opinion and government policy through "front" organizations and other covert operations. For example, in 1986 the Committee received a classified FBI report on "Trends and Developments in Soviet Active Measures in the United States," which updated a previous study prepared in 1982. The FBI report reviews covert Soviet political influence operations directed at U.S. public opinion and policymakers. The Committee regularly requests further counterintelligence information from the FBI on such operations. The Bureau should continue to report these assessments in a manner that provides the necessary facts about hostile intelligence activities and that fully respects First Amendment rights.

Findings and Recommendations

11. Recommendation.—All elements of the U.S. Government should give high priority to implementation of the policy requiring security awareness briefings and the reporting of contacts with nationals of designated countries. A similar procedure should be adopted for U.S. Senate personnel.

12. Recommendation.—The Howard case demonstrates the need for strengthening interagency procedures for bringing possible espionage cases to the FBI's attention in a timely manner. The FBI should also be informed when employees with access to extremely sensitive information, such as Howard and Pelton, resign or are dismissed under circumstances indicating potential motivations for espionage.

13. Recommendation.—The FBI should develop threat awareness briefings tailored to the special characteristics of the PRC espionage threat. Such briefings should alert American citizens to the risks of giving assistance to PRC nationals who may have espionage assignments, while respecting the freedom to associate with lawful scientific and technical research.

14. Finding.—Significant efforts are underway to improve counterintelligence threat analysis, including publication of regular interagency assessments of the hostile intelligence services threat and U.S. countermeasures and the establishment in DIA of a Multidisciplinary CI Analysis Center to meet DoD threat analysis requirements in conjunction with other DoD components. The Committee is also pleased to note that there has been progress in the effort to provide tailored analyses of the hostile intelligence threat.

15. Recommendation.—The relevant interagency intelligence analysis office should coordinate and sponsor analytic efforts on Soviet deception, disinformation and active measures. The State Department and other agencies should increase dissemination of information about Soviet active measures abroad. The FBI should continue to be responsible for reports on active measures in the United States by hostile intelligence services and should cooperate with interagency analytic efforts. Reports on active measures in the United States that are prepared by agencies other than the FBI should be prepared in coordination with the FBI and/or the Attorney General.

D. DOMESTIC OPERATIONS

Counterintelligence operations in the United States differ from such operations abroad, because the environment is generally more favorable. U.S. counterintelligence has greater resources, easier access to the target, and public attitudes favorable to citizen cooperation. While legal requirements place constraints on surveillance techniques and investigative methods, those limits are vital for maintaining our free society and (with exceptions discussed below) do not inhibit necessary counterintelligence efforts.

Domestic operations can be divided into the following categories: surveillance coverage of foreign government establishments and officials; offensive operations to recruit agents-in-place and defectors or to control double agents; and espionage investigations and prosecutions. Many of the strategic requirements for domestic operations are unique, especially with respect to surveillance of establishments and officials and the investigation and prosecution of espionage cases. Other requirements have more in common with overseas operations, particularly with regard to penetration of hostile services, handling of defectors and double agents, and analysis of the *bona fides* of sources. Unique features of overseas operations,

as well as personnel management and training programs that cross geographic divisions, are treated in later sections of this Report.

1. Coverage of Establishments and Officers

The foundation for domestic counterintelligence is systematic collection on a foreign country's official representatives in the United States. Such collection may be technical or human.

Recent cases have shown the vital importance of comprehensive coverage of Soviet bloc embassies and consulates as a means of detecting offers to sell U.S. secrets. Pelton, Cavanagh, Jeffries and others made their initial contacts with the Soviets by contacting an establishment. Skilled counterintelligence work is required in such cases, and frustrations may be unavoidable. The Pelton case is an example in which it took years to achieve a positive identification.

The stratgegic importance of covering certain foreign establishments and their employees justifies continuing resource investments to upgrade the FBI's surveillance capabilities. The Committee has supported such investments over the years and continues to do so.

In this connection, the importance of the contact reports discussed earlier in this Report cannot be overemphasized. While government regulations can require federal employees to report contacts with possible foreign intelligence officers, a free society must rely on the voluntary cooperation of private citizens to advise the FBI of approaches and other contacts by such officials. Frequently the FBI requests citizens to report this information about particular individuals, based on surveillance of a contact. The FBI's DECA briefings, which are designed to encourage such contact reports from defense contractors and their employees, have now reached over 15,000 contractor employees. FBI and other intelligence community officials have used speeches and public appearances to emphasize the importance of public cooperation.

The American people have a legitimate concern that their government should not intrude upon their lawful associations with foreign officials and their First Amendment right to exchange ideas with visitors from abroad. For that reason, the FBI operates under guidelines established by the Attorney General and internal FBI policies overseen by the Committee that are designed to respect the free exercise of constitutional rights. As Director Webster stated in a recent speech:

> We certainly don't have enough Agents to keep track of every citizen of this country nor do we want to investigate the activities of lawful organizations without predication for doing so. Rather, our focus—indeed our strategy—must be on the intelligence operatives themselves and the identification of those who have come here with intelligence commissions. By building a spiderweb throughout the United States that focuses on them rather than on our own citizens, we make it much more difficult for those who would betray our country by surreptitiously supplying national secrets to foreign intelligence officers. I believe that in a free society this is the only way we can function without turning ourselves into a police state.

The existence of those safeguards should give the public confidence that cooperation with FBI counterintelligence not only serves the national interest, but is consistent with respect for constitutional rights.

Findings and Recommendations

16. Recommendation.—Congress should continue to fund increases in FBI surveillance capabilities.

17. Recommendation.—American citizens in all walks of life should be encouraged to assist U.S. counterintelligence efforts by providing information to the FBI, either upon request or when they are approached by possible foreign intelligence officers.

2. Offensive Operations

A major element in counterintelligence is offensive operations, especially efforts to recruit agents-in-place within hostile intelligence services and to induce defections from those services. The strategic payoff of agents and defectors can be immense, as demonstrated by the exposure of Edward Lee Howard and the successful prosecution of Ronald Pelton.

The greatest area of concern is the handling of defectors, as dramatized by the Yurchenko case. According to a CIA survey, most of the defectors resettled in the United States with CIA assistance are basically satisfied with their treatment. Nevertheless, a significant minority have problems that require special attention on a continuing basis.

In the aftermath of the Yurchenko re-defection, the CIA has undertaken a comprehensive review of its practices for handling defectors. Deputy Director of Central Intelligence Robert M. Gates summarized the CIA's conclusions and corrective actions at his confirmation hearing on April 10, 1986:

> There were organizational deficiencies. We have made organizational changes so that a single individual and a single organization are accountable and are in charge of the entire process for defectors. Another element that we have changed . . . is to ensure that the same person is basically the principal case officer for a defector with continuity, so that a defector isn't facing a whole new set of people all the time and there is somebody there that he gets to know and that he can depend upon and that understands him and understands his concerns, and can identify when he is going through a particular psychological crisis. . . .

Mr. Gates also called it "imperative" to assign individuals who speak the same language as a defector so that someone is available to talk in his or her own language; he did not know, however, whether the CIA has actually been able to implement this approach.

The actions taken and under consideration by the CIA reflect a constructive effort to upgrade the defector program and respond to the lessons of the Yurchenko case. They need continuing high-level support, both in the CIA and in other agencies. The Committee will

continue to assess the CIA improvements along with other approaches.

The Executive branch continues to examine the broad question of how defectors might best be welcomed, assisted and utilized. A private organization formed to assist defectors, the Jamestown Foundation, has recommended major changes in the defector handling program. The Committee intends to follow this issue closely in the coming year and looks forward with great interest to seeing the results of Executive branch deliberations.

The Committee considers it of the utmost importance that our nation's goals in welcoming and assisting defectors be more clearly enunciated and boldly implemented. Too often, the only operative goals have been the national security benefits that result from debriefing a defector; the defector's personal security against attacks by his or her country's security services; and enabling the defector to survive without continuing U.S. Government intervention. Other goals must be added to that list: to encourage achievement in American society consonant with the defector's talents and accomplishments; and to assist the defector in making a continuing contribution to the United States. While the Executive branch has taken steps to administer its current defector program more effectively, it must also effect this important change in attitude and commitment.

The Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs has begun a major study of the U.S. Government's handling of defectors and other refugees from the Soviet Bloc. This study will focus particular attention on the contributions that defectors can and do make to American society and on the need to encourage that process. The Intelligence Committee supports this PSI study and is cooperating with the Subcommittee in its effort to inform the public regarding the needs of defectors and of the agencies that assist them.

Perhaps the greatest risk in a strategy of penetrating hostile services is that the agent-in-place or defector may be a double agent, pretending to be recruited by or escaping to the United States but actually controlled by a hostile counterintelligence service. Disputes over the *bona fides* of sources have plagued the U.S. intelligence community in the past. Such differences are sometimes unavoidable, but they should not disrupt interagency cooperation. Counterintelligence is not an exact science. The important thing is not to rely on a single source without careful testing and corroboration of his information. In this regard, the Committee has sought and received assurances that intelligence officials are alert to the risk of over-reliance on the polygraph.

The FBI, CIA, and DoD counterintelligence components have made extensive use of double agents, as evidenced in the recent Izmaylov and Zakharov cases. Last June, the Soviet air attache, Col. Vladimir Izmaylov, was expelled after being apprehended by the FBI. On August 23, Gennadiy Zakharov, a Soviet physicist working for the United Nations, was arrested and charged with espionage. Both Soviets had been maintaining clandestine contact with individuals who were cooperating with the FBI.

There is a clear need for these operations to be carefully managed. Counterintelligence managers must also review operations to

ensure that they have not been compromised. The Committee found Executive branch officials sensitive to these and other issues raised by double-agent operations.

The most difficult counterintelligence task is countering the use of "illegals," that is, hostile intelligence service officers who operate under deep cover rather than official cover. Some "illegals" may be used primarily for performing espionage support functions (e.g., clearing drops). The FBI and the Justice Department should consider improved ways to prosecute "illegals" for such espionage support activity.

Findings and Recommendations

18. Finding.—In the aftermath of the Yurchenko re-defection, the CIA has made improvements in its procedures for handling defectors. The Committee will continue to review the implementation of those procedures to ensure that needed resources and personnel, as well as continuing high-level support, are provided. The Administration has commissioned an independent assessment of the CIA defector resettlement program, and the results will be provided to the Committee.

19. Recommendation.—Objectives for the defector resettlement program must include encouraging the fullest possible achievement in American society and assisting defectors to make a continuing contribution to the United States. The Committee strongly supports the efforts of the Permanent Subcommittee on Investigations of the Senate Governmental Affairs Committee to focus public attention on the contributions that defectors can make to American society and on the need to enhance their ability to make such contributions.

20. Finding.—The Executive branch has reassured the Committee regarding the risk of over-reliance on the polygraph in testing sources and defectors and has demonstrated sensitivity to issues concerning the mangement of U.S.-controlled double-agent operations.

21. Recommendation.—The Justice Department and the FBI should work together to develop improved ways to prosecute "illegals" who perform espionage support functions. If further legislation is needed, the Justice Department should so inform the Congress.

3. Espionage Investigations and Prosecutions

Espionage investigations that may lead to criminal prosecution raise delicate issues of interagency cooperation and balancing of interests. Some senior officials support impostition of the most severe penalties on an individual found to have engaged in espionage on behalf of a hostile foreign power. Law enforcement objectives may conflict, however, with counterintelligence requirements and other national security interests.

Espionage cases involving non-Soviet bloc countries raise foreign policy issues, because of the desire of the United States to maintain good relations with particular governments. In the recent Pollard and Chin cases, however, the Executive branch has demonstrated its willingness and ability to investigate and prosecute espionage by agents acting on behalf of friendly countries—in these cases,

Israel and China. The Committee fully supports enforcement of the espionage laws, without regard to the foreign country involved. This policy does not necessarily conflict with other U.S. objectives requiring good relations with such countries, so long as it is applied even-handedly. The United States should make clear to every country that it will not tolerate violation of our espionage laws and that it will investigate the intelligence operations of countries that control or permit the commission of espionage in or against the United States on their behalf. The Committee is pleased with recent assurances of State Department cooperation with enforcement action whenever evidence of espionage is presented.

For many years U.S. counterintelligence officials assumed that information acquired by intelligence techniques could not be used for law enforcement purposes because of legal obstacles and the need to protect sources and methods. The Foreign Intelligence Surveillance Act and the Classified Information Procedures Act have made espionage prosecutions somewhat easier, although other difficulties still remain. These problems include the use of certain investigative techniques, the need for more expertise in handling sensitive espionage matters, and requirements for better cooperation among and within agencies.

One of the principal differences between espionage investigations and other criminal cases is the overriding need for secrecy to protect counterintelligence sources and methods. That is why Presidents have asserted claims of "inherent constitutional power" to authorize the use of intrusive techniques with Attorney General approval rather than a judicial warrant. That is also why Congress has established a special secure court order procedure under the Foreign Intelligence Surveillence Act and exempted counterintelligence from the law enforcement procedures for access to bank records in the Right to Financial Privacy Act. U.S. counterintelligence officials have consistently contended that ordinary judicial procedures do not provide adequate security in dealing with hostile intelligence services. In normal criminal cases the objective—either immediate or long-term—is always prosecution in open court. Counterintelligence operations have other objectives that may be more strategically important, such as learning the methods of the hostile service.

Federal law does not adequately take account of such differences in several areas. The FBI has found that the counterintelligence exemption in the Right to Financial Privacy Act is insufficient to obtain access to bank records when financial institutions refuse to cooperate on a voluntary basis. Consequently, the FBI is requesting legislation to give U.S. intelligence agencies the authority to require financial institutions to provide access to records. Unlike the law enforcement procedures under the Right to Financial Privacy Act, neither a court order nor notice to the subject of the records would be required. The FBI has a strong case for replacing the current voluntary system with a law that provides mandatory access for counterintelligence purposes within a framework of Attorney General guidelines and congressional oversight to provide safeguards against abuses. The Committee, therefore, has included legislation to address this need in the Intelligence Authorization Act for Fiscal Year 1987.

There is a similar problem with access to telephone and other telecommunications records. Paradoxically, it is easier in some states to wiretap an individual than to get the phone company to provide access to his or her billing records. For security reasons, the law enforcement alternative of a grand jury subpoena is usually impractical; and the Foreign Intelligence Surveillance Act does not cover access to records. As with bank records, the FBI is asking for legislation that provides mandatory access for counterintelligence purposes to such telecommunications records as telephone billing records. The Committee has incorporated such legislation in the Intelligence Authorization Act for Fiscal Year 1987.

A third gap in federal law concerns physical searches. The Foreign Intelligence Surveillance Act (FISA) authorizes a special court composed of Federal District Judges to grant orders for electronic surveillance to meet counterintelligence requirements, but the Act does not apply to physical search. The FBI supported broadening the Act to cover searches as part of the intelligence charter legislation considered by the Committee in 1980, but the only provisions of the charter to be enacted were the congressional oversight authorities. Pursuant to Executive Order 12333, the Attorney General authorizes warrantless searches for counterintelligence purposes.

The absence of a statutory court order procedure creates at least two problems. First, as with bank and telephone records, there is no authority to require cooperation from private parties. Second, the Federal appeals court in the *Truong* case ruled that evidence derived from a warrantless counterintelligence search may not be used in court if the search occurs after the Government decides to prosecute. Neither problem exists for wiretaps and other forms of electronic surveillance under the Foreign Intelligence Surveillance Act, which provides a court order procedure to secure the cooperation of private parties and permits the use of information for law enforcement purposes with appropriate security.

In light of this situation, the Committee recommended in 1984 that legislation be developed to establish statutory procedures comparable to FISA for physical search. The Committee is prepared to develop and introduce such legislation in cooperation with the Executive branch.

The President's interim report to the Intelligence Committees comments, "It is imperative that FISA be retained as it now exists." The Committee similarly endorsed FISA in 1984, finding that it has resulted in "enhancement of U.S. intelligence capabilities" and also "contributed directly to the protection of the constitutional rights and privacy interests of U.S. persons." The Committee believes that physical search legislation can be achieved, with Executive branch support, without endangering FISA.

Espionage investigations and prosecutions would also be more successful if greater expertise and resources were brought to bear in certain areas. Since 1985 the Army has reorganized its counterintelligence efforts and instituted a specialized training program to develop greater expertise at the field level in espionage investigations.

The espionage prosecutions in 1985 and 1986 demonstrated the importance of early consultation with Justice Department attorneys in developing tactics that reconcile intelligence and law en-

forcement interests. In the Pelton case, close cooperation between NSA, and the FBI, and the Justice Department resulted in a conviction with minimal disclosure of sensitive information. In the Sharon Scranage case, the combined efforts of the CIA, the FBI, the Justice Department, and the State Department produced a strategy that successfully led both to two convictions and to the exchange of the Ghanaian official convicted in the case for several prisoners in Ghana and their families.

The Committee understands that such consultation is now being instituted in a more timely manner than often occurred in the past. This welcome coordination requires that the Justice Department, in turn, have a sufficient number of attorneys trained and experienced in handling the unique problems in these cases. The Committee is especially concerned that those attorneys learn how to maintain controls on the release of sensitive information. Department attorneys should also work with U.S. counterintelligence agencies in potential espionage cases to ensure that their methods are as consistent as possible with successful prosecution. In this regard, the Justice Department's Criminal Division has begun to build a cadre of experienced personnel and to provide additional training to United States Attorneys.

The Howard case, which is discussed in some detail in the Committee's classified Report, revealed serious shortcomings in CIA performance relating to espionage investigations. The Committee is pleased to learn that the CIA has taken steps to correct problems pinpointed in investigations by its Inspector General and an interagency group. The Committee will monitor the implementation of those changes.

Issues relating to the handling of the Howard case by the FBI and the Justice Department have also been pinpointed and are the subject of continuing consideration. The Committee expects remedial actions to be taken, as appropriate, and will continue to follow this matter.

Findings and Recommendations

22. Recommendation.—The United States should not tolerate violation of our espionage laws by any country and should investigate the intelligence operations of countries that control or permit the commission of espionage in or against the United States on their behalf. The Committee is pleased to learn on their behalf. The Committee is pleased to learn that the State Department has pledged to cooperate with enforcement action whenever evidence of espionage is presented, and the Committee supports efforts to set up a mechanism for regulatory interagency consultation on cases that might warrant action.

23. Finding.—The Foreign Intelligence Surveillance Act continues to be considered by U.S. counterintelligence agencies to be highly beneficial to their efforts. They strongly favor retention of FISA as it now exists.

24. Recommendation.—Congress should enact legislation to give the FBI the authority to require financial institutions and telecommunications carriers to provide access to records, with notice restrictions comparable to FISA. Any such authority should be limited to counterintelligence matters, governed by the current Attor-

ney General's guidelines, and accompanied by improved provisions for congressional oversight.

25. Recommendation.—Congress should enact legislation comparable to FISA to authorize physical search for intelligence purposes, so as to reduce legal uncertainties in counterintelligence investigations that have prosecution as one of their objectives.

26. Recommendation.—U.S. counterintelligence agencies should continue to emphasize, as standard procedure, consultation with the Justice Department at an early stage in potential espionage cases. The Justice Department should provide increased training to Criminal Division attorneys and U.S. Attorneys concerning the prosecution of espionage cases, including the need to protect sensitive information relating to such cases.

27. Finding.—The CIA has taken some steps that are likely to improve counterintelligence investigations and prosecutions, in the wake of investigations of the Howard case. The Committee will monitor implementaton of those improvements.

28. Recommendation.—The FBI and the Justice Department should take actions, as appropriate, to remedy shortcomings exposed by the Howard case.

E. OVERSEAS OPERATIONS

Strategic counterintelligence objectives abroad differ from those in the United States not only because of the different environment, but also because of the added requirements for counterintelligence support in intelligence collection programs. The Committee welcomes recent CIA initiatives to improve both its counterintelligence efforts and its career opportunities in counterintelligence.

The Committee's classified Report discusses further issues regarding CIA and Department of Defense counterintelligence activities overseas.

The investigation of espionage by U.S. civilian and contractor personnel abroad raises jurisdictional questions. The Committee believes that the FBI should be called in and should work closely with agency security officials from the outset.

Findings and Recommendations

29. Finding.—The CIA has begun initiatives to improve its counterintelligence efforts.

30. Recommendation.—U.S. agencies abroad should continue to obtain the timely advice and assistance of the FBI in cases of possible espionage by civilian and contractor personnel.

F. PERSONNEL MANAGEMENT AND TRAINING

Counterintelligence is not the main function of any of the organizations responsible for U.S. counterintelligence programs. The CIA's primary task is collection and analysis of political, economic and military intelligence; the FBI is a law enforcement organization; and each of the service counterintelligence organizations is part of a larger criminal investigative or intelligence agency. This is one reason why there have been less specialized training and fewer incentives for careers in counterintelligence. Personnel are recruited for law enforcement or intelligence positions generally

and are usually not assigned to counterintelligence until they have experience in other fields. The advantage of this practice is that personnel can develop their basic investigative or intelligence skills in less sensitive areas before taking on more important counterintelligence duties. The disadvantage is that specialization and career advancement in counterintelligence may be discouraged because of the organization's emphasis on other functions.

Every agency is taking steps to upgrade counterintelligence training, but the results thus far have been uneven. More should be done to encourage agencies to share their experience with successful methods. While each agency operates in a different environment and with different internal regulations, joint discussion of such topics as the nature of the threat from particular hostile services and the techniques for offensive operations and counter-espionage investigations could be very useful. This would also make more efficient use of expert personnel who assist in other agencies' training. In the CIA and the military services, better training in agency guidelines is also needed.

In the aftermath of the Miller case, the Committee has taken a close look at FBI personnel management policies for counterintelligence. At the Committee's request, the FBI prepared a study reviewing the impact of FBI personnel policies on the Foreign Counterintelligence (FCI) Program in order to determine how the FBI may more effectively recruit, select, assign, train, promote, and retain Special Agents for counterintelligence matters. The FBI study indicated a need for improvements in several areas.

The FBI confronts unusual personnel management problems because of the large hostile intelligence presence in New York City, where the cost of living has discouraged FBI Agents from seeking assignments or pursuing careers. Unlike State Department personnel, FBI Agents in New York do not have a special housing allowance to defray the cost of living in town. The Committee believes that action is needed to improve benefits and incentives in New York and is prepared to develop legislation that may be needed for this purpose.

Another manpower issue is the limited number of FBI senior grade positions in the counterintelligence field, as compared to positions as Special Agent in Charge of a field office and comparable headquarters positions with primarily law enforcement duties. The Committee supports efforts to change this situation, including funds requested in the FY 1987 budget to increase the number of senior grade counterintelligence positions at FBI Headquarters. The Committee also supports the FBI policy requiring that all new Special Agents in Charge of field officers who have not previously served in a full-time counterintelligence position must receive FCI training.

The Committee intends to continue its review of FBI counterintelligence personnel policies as part of a broader ongoing study of intelligence community personnel issues.

DoD counterintelligence components have similar problems and should develop appropriate revisions in personnel policy to encourage specialized counterintelligence career development. In all the DoD counterintelligence units, as well as the FBI, greater efforts are needed to recruit and retain the best possible personnel.

Findings and Recommendations

31. Recommendation.—More should be done to encourage agencies to share their experience with successful CI methods and to make more efficient use of expert training personnel.

32. Recommendation.—Additional measures should be taken to improve benefits and incentives for FBI Agents in New York City, including any legislation needed to give the FBI comparable authority to the State Department.

33. Finding.—The FBI is planning to increase the number of senior grade counterintelligence positions at FBI Headquarters. The Committee supports these efforts.

34. Recommendation.—While each counterintelligence agency must recruit to satisfy its unique needs, greater attention should be given to determining specialized qualifications required for personnel to meet each agency's CI needs as distinct from law enforcement or foreign intelligence needs.

35. Recommendation.—DoD counterintelligence components should continue to develop appropriate revisions in personnel policy to encourage specialized counterintelligence career development.

IV. Security Countermeasures

In 1984–85 the Executive branch conducted seven in-depth studies of security policies and practices for protecting classified information and activities against hostile intelligence collection. The Committee has reviewed findings and recommendations from all of these studies, as well as observations and proposals made by other Congressional committees, by witnesses at the Committee's closed hearings, and by experts inside and outside the Government. Taken together, these reports and recommendations raise grave questions regarding U.S. security programs to protect sensitive information from our adversaries.

The Walker case disaster and the bugging of typewriters in our Moscow embassy were compromises that waited years to be uncovered and that illuminated significant weaknesses in the nation's security. There have been wide disparities in policies and standards for personnel, information, technical and other security measures. Serious imbalances in resource allocation have existed, and in some areas inadequate resources have led to serious gaps in protection. Research and development to improve security has been haphazard at best.

Since the late 1970s, the Committee has worked with the Executive branch and the intelligence community to strengthen counterintelligence throughout the Government, so that the FBI, CIA and DoD counterintelligence components could deal more effectively with the hostile intelligence threat. Until 1985, however, neither this Committee nor any other congressional body had taken a similarly comprehensive look at the defensive security countermeasures that surround the core of classified information and that are supported by counterintelligence. The Committee's closed hearings in the fall of 1985 were the first systematic Congressional review of security programs since the 1957 report of the Commission on Government Security established by Congress (with Senator John Sten-

nis as its Vice Chairman). Although the Committee is encouraged by many of the steps now being taken to remedy serious deficiencies, the continuing fragmentation of security planning and policy requires a substantial reorganization of the way the Government handles its many security programs. Congress has a similar duty to put its own house in order; and the Committee has specific recommendations for that purpose as well.

The Committee has addressed security countermeasures at two levels. First is the national policy level, where government-wide initiatives and programs are developed, approved and overseen. Many of the most serious security weaknesses result from the lack of an effective, national policy that gives high priority to security programs and ensures comprehensive and balanced planning. The second level is the numerous separate security disciplines, which each have their own problems that must be solved within a coherent national policy framework. These disciplines include information security, personnel security, communications security, computer security, emanations security (TEMPEST), technical surveillance countermeasures, physical security, industrial security and operations security. Their variety itself clearly indicates how difficult it is to pull together the necessary expertise and reconcile the interests of different agencies and programs—intelligence, military, diplomatic, industrial, research and budgetary. Nevertheless, the effort must be made if we are to reduce the likelihood of future compromises that repeat the multi-billion dollar damage of the Walker, Pelton, Howard, Harper and Bell cases or the incalculable harm from interception of our communicatins and technical penetration of U.S. facilities.

We would not wish to mislead; in any foreseeable environment, U.S. security countermeasures programs can provide no absolute guarantees against compromises and losses. Our goal is a significant improvement in security, a further limiting of the damage that is wreaked by those compromises and losses. Our belief is that more effective, but not unduly intrusive measures can accomplish this objective.

A. A NATIONAL STRATEGIC SECURITY PROGRAM

In December, 1985, the Committee recommended to the National Security Council that the Excutive branch develop a comprehensive and integrated National Strategic Security Program to coordinate and foster the protection of sensitive information and activities from the efforts of hostile intelligence services. The purpose is three-fold.

First, such a program would give greater visibility, higher priority and increased attention of senior officials to security countermesures. Frequently, security programs have neither an influential voice in government departments and agencies nor adequate funding and career opportunities. Security must be recognized by the Executive branch and Congress as a crucial underpinning to the other basic functions—military, intelligence and diplomatic—that safeguard national security.

Second, the reason for such a program is to provide a coherent structure to address and overcome security deficiencies. As dis-

cussed in the following sections, these problems include underfunding of essential programs, significant gaps in research, inadequate training and career development, insufficient management accountability, uneven national policy guidance, interagency conflicts over new initiatives, and failure to ensure necessary linkages among security disciplines.

Third, the establishment of such a program and structure should provide long-term continuity and consistency through succeeding Administrations. The changing of NSC structures from one Administration to the next does not fill the pressing need for continuity and consistency of policy. When a National Strategic Security Program has taken shape, therefore, the essential features should be promulgated by the President in a formal Executive Order.

At the Committee's closed hearings in late 1985, senior officials were asked to discuss how U.S. counterintelligence and security countermeasures policies are established and coordinated at the national level. The answer for counterintelligence was clear: responsibility is focused on a single NSC committee process (the Interagency Group for Counterintelligence (IG–CI) and the Senior Interdepartmental Group for Intelligence (SIG–I)), with support from an interagency staff which assists the NSC staff in coordinating policy initiatives and overseeing their implementation. Much progress has been made in developing a coherent process for counterintelligence policy. The same cannot be said for security countermeasures, where responsibilities have been widely diffused and the Executive branch has only begun to develop a coherent policy review structure.

The DCI testsified that the SIG–I is "the principal forum where the national perspective can be brought to CI [counterintelligence] and CM [countermeasures] policy," with countermeasures handled by an Interagency Group (IG–CM) chaired by the Deputy Undersecretary of Defense for Policy. At the same time, however, the DCI acknowledged the existence of "other Executive branch policy recommending and implementing entities such as the DCI Security Committee, the National Telecommunications and Information Systems Security Committee, the SIG for Technology Transfer, etc." While the DCI said the SIG–I system has " the capability for and mission for ensuring proper national-level coordination of all CI and CM matters," this has not in fact been the case for security countermeasures.

Recently, the DCI, acting in his capacity as Chairman of the SIG–I divided the Interagency Group for Countermeasures into separate groups for Technical matters (IG–CM(T)) and for Policy and other non-technical issues (IG–CM(P)). The new IG–CM(T), headed by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, is intended in part to serve as a bridge between the intelligence world of the SIG–I and the world of the National Telecommunications and Information Systems Security Committee (NTISSC). The NTISSC is chaired by the same Assistant Secretary and has a presidential mandate under NSDD–145 to develop communications, computer and emanations security policy for the whole government.

The DCI also abolished the DCI's Security Committee (SECOM), which had been a working-level intelligence community group out-

Page 488 of 3957

side the IG–CM but covering some of the same issues. The two new IG–CMs are to have subcommittees that will handle many of the former SECOM functions, but with more senior members than was the case with SECOM, so that subcommittee members can actually commit their agencies to act upon group recommendations. Staffing is to be achieved through an up-graded interagency staff.

These structural changes are very welcome signs of the seriousness with which the Executive branch is approaching the need to improve the security policy process. The Committee does not believe, however, that they go far enough in establishing a forum in which all the many security interests can be surfaced and reconciled. It is uncertain, moreover, whether the IG–CM subcommittee will be sufficient improvements on the SECOM structure to overcome the bottlenecks that too often have stifled progress on security issues. The Committee continues to believe, therefore, that a comprehensive National Strategic Security Program must be developed, through whatever structures the Executive branch finds best suited to that task.

In recommending establishment of a comprehensive National Strategic Security Program, a Committee does not intend to create a "czar" or to take from individual agencies their responsibility for implementing national policies that affect their work. If there is no national policy, however, there is no standard against which to hold each department accountable. If national policies are fragmented, outdated or unbalanced, security becomes subordinated to other departmental priorities and interagency disputes. This has occured far too often in recent years. Later sections of this Report give examples: the inability to reach agreement on a "single scope" background investigation for Top Secret and SCI clearances; the proliferation of special access programs without sufficient controls and standards; the imbalance in resources between expensive technical safeguards and the personnel and information security measures needed for effective computer security; and, at least until very recently, interagency conflicts over how to deal with some technical security issues.

As important as it is to remedy these problems, the greatest value of a National Strategic Security Program should be to promote innovative solutions to new and emerging hostile intelligence threats. This requires collaboration with counterintelligence agencies to identify such threats, as well as recruitment and training of top-quality security specialists with wide-ranging operational, technical, analytical, and managerial skills. At the core must be a commitment at top management levels within each department and agency to setting clear security objectives, providing adequate resources, and devising effective oversight and inspection procedures for holding managers and commanders accountable for their performance. This commitment will be forthcoming only if Congress and the President make clear they expect it and establish their own systematic means to assess government-wide progress in meeting national goals.

A National Strategic Security Program should provide policy direction and oversee implementation for all security disciplines:

Personnel security;
Information security;

64-268 O - 86 - 3

Page 488 of 3957

Communications, computer and emanations security;
Technical surveillance countermeasures;
Physical security;
Industrial security;
Operations security.

To assist the NSC, a single body shoud be assinged responsibility for policy planning and analysis of all aspects of security countermeasures for protection of sensitive information against hostile intelligence efforts. It should ensure effective coordination among the other interagency forums that address particular problems. It should have the task of putting together for the NSC and the Congress a fully balanced and coordinated government-wide program. A senior official should be designated to testify on the National Strategic Security Program before the appropriate Congressional committees.

During 1985, the CIA and the State Department took significant steps to achieve the same objectives on a departmental level. The CIA reorganized and expanded its Office of Security to integrate all its security functions. Similarly, as recommended by the Inman Panel on Overseas Security, the State Department established a new Diplomatic Security Service with higher status and wider responsibilities, including a high-priority effort to upgrade technical security. The Stilwell Commission has recommended a similar action by the Defense Department, stressing "that all security disciplines have as their fundamental purpose the protection of classified information and must be applied in a fully balanced and coordinated way." The Committee urges that resources be allocated to enhance security policy and oversight in the Office of the Secretary of Defense (OSD), so as to make the policy-level integration of the various security programs in DoD a viable option.

A significant aspect of the National Strategic Security Program should be to assist the NSC on resource priorities. The current budgetary arrangements are fragmented and inadequate. To consider ways to improve the resource allocation process, the Committee held a closed hearing on June 4, 1986, on principal security programs outside the NFIP, as well as those in the CIA Office of Security. The ultimate goal of the Committee is to have each department and agency identify its security resources by function and program and include these resources in their congressional budget justification submissions. The National Strategic Security Program should give the NSC and Office of Management and Budget a similar opportunity to evaluate the resource priorities of these and other security countermeasures programs.

Another high priority for the National Strategic Security Program should be an assessment of requirements for research and analysis, especially on personnel security and the interfaces between personnel, communications and computer security. The greatest imbalance in security resources is between costly projects on technical safeguards and the meager efforts to look into personnel security issues. Not until January, 1986, was DoD able to get the necessary concurrences for a modest personnel security research program in DoD to be administered by the Navy. Current arrangements for intergency assessment of security research needs have been insufficient to identify and promote aggressive and bal-

Page 490 of 3957

anced government-wide efforts, even though particular agencies have taken valuable initiatives in areas of concern to themselves.

Special emphasis should also be placed on commander and manager responsiblity for security within their respective organizations. The recent action of the Deputy Secretary of Defense ordering the incorporation of security management as a criterion in military and civilian performance and fitness reports is a step in right direction. Such a requirement should be extended government-wide and apply to all contractors as a condition for inclusion on a bidders list. Other realistic sanctions are needed, as well as greater consistency in the government and among contractors on the severity and application of such sanctions as fines, relief for cause, debarment and suspension, for knowing or negligent security violations both by managers and by subordinates. The National Strategic Security Program should supply the necessary policy direction.

Security normally ranks well below other careers in most agencies; the National Strategic Security Program must change the status of the security profession. Security specialists should match other professionals in terms of their qualifications, training, compensation and career opportunities. There should be an independent evaluation of the recruitment, training, pay, status, professional development and retention of federal security officers in all departments and agencies. As recommended by the Information Security Oversight Office and the Stilwell Commission, the OPM job classification standards for security should be revised immediately to ensure comprehensive and accurately graded descriptions of modern security disciplines.

One of the common themes in all recent studies of security countermeasures—the Information Security Oversight Office (ISOO) task force, the Stilwell Commission, and the Inman Panel—is the need for better training not only for security professionals, but also for managers and other officials having security responsibilities. In the near-term, the quality of training for new security personnel must have special attention. Through the government, security initiatives are providing funds for new personnel. Agencies should be held accountable for ensuring that the most qualified personnel are recruited and that their training meets high standards.

The National Strategic Security Program should establish government-wide security training objectives for managers, security professionals, personnel security clearance adjudicators, and industrial security officiers. Minimum levels of training and certification should be established for industrial security personnel, clearance adjudicators, and other positions requiring consistent standards. Because the Defense Investigative Service and the Defense Security Institute (DSI) have crucial roles in the development and implementation of security training programs and industrial security generally, an expanded government-wide training role for DSI should be considered. The Information Security Oversight Office has made a similar recommendation. DSI could serve as a national security training and education center serving all federal departments and agencies. Consideration should also be given to forming under DSI an interagency group, with counterintelligence agency participation, to develop and review effective security awareness

Page 490 of 3957

educational material and techniques. Given the concentration of sensitive facilities on the West Coast, establishment of a permanent West Coast security training facility for government and contractor personnel should be considered.

One of the most challenging and difficult tasks that a National Strategic Security Program must address is the development of coherent and effective policy for operations security (OPSEC). OPSEC has many definitions amoung the various departments and agencies. It can include the implementation and assessment of U.S. efforts to frustrate hostile intelligence collection. Another element is the careful design of particular unclassified activities or information to keep hostile intelligence services from putting together bits and pieces of information to detect classified missions or the presence of sensitive installations.

Equally important is the assessment of government practices outside the national security field that could help or hinder hostile intelligence collection efforts. The recently established National Operations Security Advisory Committee of the IG-CM(P) has taken several valuable initiatives in restricting public availability of sensitive data.

A 1985 interagency assessment identified serious OPSEC weaknesses. The National Strategic Security Program should develop government-wide OPSEC objectives and ensure that relevant agencies have the necessary resources and programs to achieve these goals. Just as sensitive military units take care to ensure that changes in routine activity will not provide our enemies indications and warning of their operations, so must agencies and contractors involved with sensitive agencies or programs incorporate OPSEC in their overall security philosophy and programs.

These are some of the government-wide security issues that should be addressed by a National Strategic Security Program. Others are detailed in the sections below on personnel security; information security; communications, computer and emanations security; technical and physical security; and industrial security.

Findings and Recommendations

36. Recommendation.—The Executive branch should develop and implement a comprehensive National Strategic Security Program which would provide:

a. NSC-approved objectives and policy direction;

b. A broad master plan faithful to the objectives and policies, and both based upon and prioritized in light of the threat;

c. Close coordination of implementing programs;

d. Assessment and allocation of resource requirements for all areas of common concern—such as, but not limited to: R&D; computer security; TEMPEST and personnel security; and core training for technical security countermeasures;

e. Oversight of implementation of national policy; and

f. A review of total resources planning.

This program, although within the NSC, should be structured so as to provide long-term continuity and consistency through succeeding Administrations. Accordingly the program and the essential structure for its maintenance should be promulgated by the President in an Executive Order.

37. Finding.—Recent IG-CM changes promulgated by the DCI, although not sufficient, in the Committee's view, to solve the problem, are a welcome sign of the seriousness with which officials are addressing the need to improve the security process.

38. Recommendation.—The Defense Department should enhance its security policy and oversight capabilities in the Office of the Secretary of Defense so as to ensure integration of policies for the various DoD security programs

39. Recommendation.—The National Strategic Security Program should evaluate security countermeasures resource priorities for the NSC and OMB on an annual basis. Security resources should be identified by function and program in departmental and agency budget justifications. The Administration and the Congress should consider additional ways to implement a more coherent budget process for security programs.

40. Recommendation.—The National Strategic Security Program should assess requirements for research and analysis on security countermeasures to promote aggressive and balanced efforts government-wide, especially on personnel security.

41. Recommendation.—The National Strategic Security Program should emphasize commander and manager responsibility for security, including government-wide application of the recent DoD action to incorporate security into performance evaluations and development of more realistic and consistent policies for disciplinary sanctions.

42. Recommendation.—The National Strategic Security Program should commission an independent evaluation of the recruitment, training, pay, status, professional development and retention of federal security personnel. Relevant OPM job classifications should be revised and modernized.

43. Recommendation.—The National Strategic Security Program should establish government-wide security training objectives and should require minimum levels of training and certification for industrial security officers, clearance adjudicators, and other positions requiring consistent standards.

44. Recommendation.—The National Strategic Security Program should consider phased assignment of national responsibilities for security training to the Defense Security Institute (DSI), with an interagency group including representation from U.S. counterintelligence agencies to develop security awareness materials. DSI should establish a West Coast annex.

45. Recommendation.—The National Strategic Security Program should develop government-wide operations security (OPSEC) objectives and ensure that relevant agencies have the necessary resources and programs to achieve those goals.

B. PERSONNEL SECURITY

The most important barrier to the hostile intelligence threat and the growing willingness of Americans to divulge classified information for financial gain is a sound personnel security program. Unfortunately, recent Executive branch and congressional studies have identified significant weaknesses in U.S. Government personnel security practices. Many of the issues raised by the Report of

the Commission on Government Security in 1957 remain unresolved today, particularly the need for national policy guidance and oversight. The Stilwell Commission, the DoD Industrial Security Review Committee (formed after the Harper espionage case), the Permanent Subcommittee on Investigations of the Senate Governmental Affairs Committee, other interagency assessments, and investigations of agency performance prompted by recent espionage cases have all addressed deficiencies, inconsistencies and ineffectiveness in the administration of personnel security policies and programs. Development of a more coherent and effective personnel security policy should have the highest priority in a National Strategic Security Program.

The Stilwell Commission, while finding the DoD security program "reasonably effective," made the following critique:

> Clearly there is room for improvement. Many people are cleared who do not need access to classified information. Background investigations yield relatively little derogatory information on those being cleared, and under the existing adjudication process, far fewer still are actually denied a clearance. Once cleared, very little reevaluation or reinvestigation actually occurs, and relatively few indications of security problems are surfaced. The principle that a cleared individual is authorized access only to that information he "needs to know" is generally not enforced.

The Commission attributed these problems to insufficient resources and the desire not to let security interfere with mission accomplishment.

The Committee endorses vigorous implementation of most of the Stilwell Commission's recommendations on gaining and maintaining access to classified information and on detecting and investigating security violations. They should be reviewed at the NSC level and adopted for government-wide application. In summary, the Commission proposes:

For Secret clearances, better background checks, an eventual reinvestigation system, and better workplace controls (document logs and briefcase searches).

For Top Secret information, many more reinvestigations, more polygraphs primarily for reinvestigations, better workplace controls (a personal reliability program and a ban on one-man access), and a special crypto-access compartment.

More inspections and management responsibility.

Not issuing clearances for information to personnel who require only access to the workplace.

Measures to reduce the number of clearances and streamline security requirements for contractors, including a billet system to cut the number of Top Secret clearances, justification for each contractor clearance (with periodic rejustification for overseas positions), and a single scope for Top Secret and SCI background investigations.

To free resources to cover other costs, the easing of reinstatement procedures for contractors whose clearances lapse for a short time and the routine granting of interim Secret clearances while initial investigations are conducted.

These recommendations reflect the most comprehensive and detailed analysis of DoD personnel security requirements that has been conducted in decades. Nevertheless, in some respects they fall short of meeting current needs.

The first requirement is resources. Personnel security is seriously underfunded, especially in comparison to the technical programs for communications and computer hardware and software. Redressing this imbalance should be one of the highest priorities for a National Strategic Security Program. Congress added $25 million for the Defense Department in FY 1986 to reduce the backlog of investigations and, especially, of reinvestigations of persons with Top Secret clearances. The Committee has recommended, and the Senate has passed, an additional $22 million authorization and 358 positions for FY 1987 to accelerate implementation of Stilwell Commission recommendations, primarily regarding more detailed investigations for Secret clearances. Intelligence elements have also regularly fallen short of meeting periodic reinvestigation goals because of inadequate funding. This is true as well for the FY 1987 budget. The basic problem is that personnel security has had relatively low priority in the Executive branch budget process. The Committee welcomes recent testimony by the DDCI that the CIA will give much higher priority to reinvestigations.

Nowhere is the adage "penny wise, pound foolish" more apt, yet even the Stilwell Commission had to confront serious resource constraints. Its goal is to reduce the DoD backlog of reinvestigations for persons holding Top Secret clearances to manageable levels within four years and to conduct periodic reinvestigations of all persons holding Secret clearances and above by 1995. Efforts to reduce the number of positions requiring background investigations can alleviate some of the pressure, but the technological sophistication of modern military systems and the need for widespread access to intelligence products requires that large numbers of DoD personnel have at least Secret-level clearances. On the civilian side, the work of Departments such as State, Energy, Justice and Treasury will continue to require that many employees have background investigations and reinvestigations.

Over the years, resource constraints have prevented any serious consideration of field investigations for Secret clearances, which have been based on name and fingerprint checks of law enforcement and counterintelligence files. Some of the most sensitive information in the U.S. Government is classified at the Secret level, and sustained passage of Secret information to hostile countries would do grave damage to national security in many areas. The Harper case is a good example where compromise of a substantial amount of Secret information from a defense contractor's office did great harm. The current requirements for Secret clearance investigations are too low, and the proposals for wider checks are too modest.

At a minimum, the investigative requirements for a Secret clearance should include, in addition to file checks: a credit check; inquires to present and past employers; more documentation of identity; other field inquiries on recent life history; and a subject interview. The key is the interview, to surface issues that may merit further investigation. This recommendation requires a substantial

increase in manpower and funds, but the cost is reasonable in light of the Soviet bloc intelligence emphasis on acquisition of Secret-level technological data.

Overall, the Stilwell Commission goal of eliminating the reinvestigation backlog within four years should be extended government-wide and to contractor employees. In addition, a government-wide plan for Secret clearances should be developed and submitted to the Committee, with a target of implementation in less than the ten years proposed by the Stilwell Commission. A government-wide funding plan to achieve all these objectives should be submitted to Congress as soon as possible.

Another resource problem results from the resistance of some authorities to modification of Top Secret and SCI background investigation requirements that Defense Department officials have concluded are not cost-effective. Because the Defense Investigative Service, CIA and OPM have different policies on the scope of those investigations, it is not unusual for individuals, particularly in industry, to have two or more background investigations in the same year for Top Secret and SCI access. Moreover, some agencies appear unwilling to simplify their background investigation procedures in the light of cost-effectiveness studies. While the Committee has not attempted to evaluate alternative procedures in detail, it strongly recommends that a uniform policy be established to achieve less costly and more timely background investigations and clearances and to eliminate redundant investigations.

Another factor that should guide development of a "single scope" investigation is the high priority for reinvestigations. Recent espionage investigations indicate that none of the current approaches to initial clearance is infallible. Espionage-related issues rarely surface during initial background checks. Streamlining the procedures for initial investigations would release manpower for use in meeting the five-year reinvestigation requirement that all agencies agree should apply to Top Secret and SCI Clearances.

The Committee also believes that a "single scope" background investigation for Top Secret and SCI clearance should include an in-depth interview of each subject by a trained and experienced security officer. The record indicates that such interviews are often effective in surfacing issues not uncovered by a field investigation that bear on the ability of an individual to handle sensitive information.

Several Stilwell Commission proposals deserve special emphasis. A reliability clearance for persons needing access to a site, but not to classified information, would underscore the importance of "need to know." There are no figures on the number of people with clearances where the intent is solely to determine their reliability. Included in this category are guards, char force, maintenance personnel, etc. Implementation of this measure would set the stage for carrying out such other measures as a "billet control system" describing which positions require access to classified information. This action will help revive the need-to-know rule by drawing a clear distinction between clearance for one purpose and clearance for other purposes.

The Committee shares a concern, expressed initially by the Permanent Subcommittee on Investigations, about the potentially seri-

ous risks in issuing security clearances to foreign-born individuals whose background cannot be verified adequately. The Stilwell Commission's proposal for use of the polygraph in such cases is comparable to the FBI's policy of polygraphing foreign nationals employed for specialized purposes. Agencies must guard against overreliance on the polygraph, of course, especially when independent corroboration is so difficult to obtain. Other approaches tailored to particular agency needs should also be considered. A government-wide minimum standard is needed, however, in order to ensure cross-agency acceptance of clearances.

One Stilwell Commission recommendation that should be reconsidered is the proposal for one-time, short duration (read on, read off) access by cleared personnel to the next higher level of classified information when necessary to meet operational or contractual exigencies. Given the vast differences between investigative standards for Secret and Top Secret, there is too great a risk in giving an individual with only a Secret clearance access to Top Secret information. If the requirements for Secret clearances are substantially upgraded, this proposal could be reconsidered as a means to conserve security resources. As the Stilwell Commission recognized, administrative oversight is essential to ensure that repeated read on, read off access does not become a loophole for semipermanent access.

Several areas of concern not mentioned by the Stilwell Commission deserves serious consideration. One is the need for relevant data on persons who leave positions with Top Secret or sensitive compartmented accesses. Pelton, Howard and, for the most part, Walker committed espionage after each had lost his clearances.

Walker's greed and his aberrant conduct as a private investigator could have alerted a Navy system tasked to continue oversight of individuals with previous high clearances. No such system effectively exists. Pelton's bankruptcy should have served as the indicator for further NSA review, particularly in view of Pelton's access to very sensitive information. Had Howard's travels and finances been known, the FBI might have been brought into that case much sooner.

The Executive branch should consider requiring as a precondition for clearance, that those who receive access to the most sensitive information agree to permit, for a period of years after their clearance ends, access to relevant financial and foreign travel records. In practice, for example, this would mean that agency security officials could access credit bureau information on former employees, as DoD agencies are now doing on background investigations and reinvestigations pursuant to the Stilwell Commission's recommendation.

Such a system could be abused if not clearly limited to persons with access to especially sensitive information and properly administered under stringent safeguards for privacy and civil liberties. It would be important to establish clearly, for example, that the examination of these records would not imply suspicion regarding a person. Another useful safeguard might be to limit the information gained from these records to an employee's security file unless the Director of Security certified that it warranted the attention of another office or the FBI. Other minimization procedures, perhaps based upon those in the Foreign Intelligence Surveillance Act,

could also be applied. In addition to providing better means to detect suspicious behavior, records access procedures could enable security offices to respond in a timely and helpful fashion to evidence of financial problems among personnel whose recent sensitive accesses would make them lucrative intelligence targets.

The Committee recommends that the Executive branch study the possibility, in consultation with appropriate congressional committee and civil liberties experts, of a program of expanded post-access foreign travel reporting obligations and/or agency access to relevant financial and travel records. The Committee believes that such a program, if combined with proper safeguards and limited to those persons whose access to the most sensitive information clearly warrants special measures, might be acceptable from a civil liberties standpoint. A similar view has been expressed by a ranking ACLU official at a recent conference sponsored by the Congressional Research Service of the Library of Congress.

Another initiative, relevant to the role of a National Strategic Security Program in fostering and coordinating research, is examination of the value of psychological testing in the security clearance process. Some authorities contend that such testing can help identify persons disposed to disregard their obligations for the sake of self-gratification. Any use of psychological testing, however, should take full account of the need for test reliability, trained personnel to interpret results, and protection of individual rights. Psychological testing can supplement, but not replace other screening devices.

The Stilwell Commission urged the Secretary of Defense, although not in a formal recommendation, to press for revival of the interagency effort chaired by the Justice Department in 1983–84 to draft a new Executive Order on personnel security. While drafting such an order may be a lengthy process and must not be an excuse for inaction on the specific national policy issues discussed above, a new Executive Order would make an important contribution to better personnel security. Such an order should provide a formal Presidential mandate for minimum government-wide standards and procedures that incorporate the essential elements of national policy on key topics, with details to be spelled out in an implementing directive that can be updated periodically in light of experience and research. Second, it should establish an office similar to the Information Security Oversight Office to provide the kind of policy guidance and oversight of implementation that ISOO has supplied for information security. The absence of such an office makes it extremely difficult for the National Security Council to address personnel security policy issues government-wide. Third, a new Executive Order should focus exclusively on policies and procedures for access to classified information and to facilities where classified information is maintained. Experienced Justice Department officials believe that such an order would make it easier to defend in court decisions to deny or remove security clearances.

More extensive and timely background investigations and reinvestigations, with streamlined government-wide standards and procedures, must feed into an adjudication system with rigorous but realistic criteria for granting or denying clearances. There is currently no uniform requirement to deny a clearance to a person who

Page 498 of 3957

has been convicted of a felony or has admitted to conduct which constitutes a felony under state or local law. There is no requirement for follow-up inquiries in cases where clearances are granted to persons admitting problems like drug use. (The FBI has expressed particular concern about this problem in contractor facilities, where habitual drug users have posed real threats to sensitive research and development programs.) There is no government-wide requirement for training of persons who adjudicate security clearance cases. (Only one agency currently has a formal adjudicator training school and individual services tend to have too few adjudicators to justify their own training programs.) The lack of training and experience among adjudicators causes delays and inconsistencies within and among agencies.

Agency and interagency investigations of such recent espionage cases as Edward Lee Howard and Jonathan Pollard have highlighted serious flaws in agency hiring, assignment and termination practices. The CIA and DoD have moved to rectify problems, and there will probably be interagency consideration of adopting similar corrective measures. The CIA and other agencies have also become more sensitized to the risks inherent in decisions to give sensitive assignments to persons with a history of personal problems. While there is a balancing need not to do away with necessary managerial flexibility, these corrective steps are basically much needed and long overdue.

Underlying these specific problems is a general attitude that the purpose of the clearance process is simply to wed out those individuals most obviously likely to pose a threat to security. Wider background checks will have little impact if the results are not used effectively. Especially for Top Secret clearances and for the most sensitive Secret clearances, the policy should be reversed. Clearances should go to individuals whose records demonstrate a clear aptitude for security. That is, their background and personal qualities should show a high sense of responsibility—not just the absence of proved disqualifying factors. At the same time, denial of such highly sensitive clearances should not affect the ability to pursue careers in other areas.

A final personnel security issue is the use of polygraph examinations as part of the initial clearance process or in reinvestigations. Since 1983, the Committee has followed closely the various attempts in the Executive branch to widen use of polygraphing for personnel security purposes and congressional efforts to control such practices by statute. The Committee has consistently supported the approach taken by the Senate Armed Services Committee in approving a personnel screening polygraph test program for the Defense Department. That test program is limited to counterintelligence-related questions and has very stringent quality controls and safeguards for individual rights. The same limitation, controls and safeguards should apply to any expansion of polygraphing in other departments and agencies. The National Strategic Security Program should ensure full coordination of departmental policies and practices for this purpose.

The Committee is concerned about the tendency to place an overreliance on the polygraph, thereby allowing apparent passage of an examination to validate the reliability of an individual who may be

Page 498 of 3957

intent on espionage. Other concerns are the persistent underfunding for implementation of some high-quality polygraph programs and the risks that incompetent or improper use of the polygraph may harm the careers, reputations or well-being of loyal Americans. Adequate research on personnel screening polygraph practices is also lacking.

An essential prerequisite for any wider polygraph program in DoD or other agencies is a significant upgrading of the national polygraph training school managed by the Army. This training program should be the focal point for development of a government-wide approach to personnel security polygraph examinations, including equipment requirements, question format, quality controls, and use of individuals as training subjects. A model that should be studied is the Air Force Seven Screens program, which is described in a recent report to the Senate Armed Services Committee. This is a screening program that uses only counterintelligence-related questions and is designed to establish and maintain strict quality controls and respect for individual rights. The establishment of an Oversight and Review Committee and the conduct of regular inspections are especially valuable features of Seven Screens that should be considered for use in other polygraph programs. The Committee is pleased that other sensitive DoD programs are adopting the Seven Screens approach.

The Stilwell Commission recommended that Congress replace the current statutory authority for a limited DoD "test program" with permanent legislation authorizing the use of polygraph examinations for personnel screening with counterintelligence-related questions for DoD personnel. Any such legislation should incorporate standards for quality control and respect for individual rights and should provide a means whereby those standards can be enforced. DoD has prepared draft legislation for this purpose. The legislation deserves serious consideration in the next Congress, after thorough review of the current test program. If Congress does not yet have sufficient test data to decide this issue, then the current test program should be extended for a specific period, at the end of which a decision on permanent authority will be made.

The DoD-proposed polygraph legislation would apply only to the most sensitive positions and would include both quality control and oversight requirements. The Secretary of Defense and the Armed Services Committees would agree in advance to an annual numerical ceiling on examinations to be given, and no adverse action could be taken soley on the basis of polygraph results except with approval at the highest levels in special circumstances. In reviewing this proposed legislation, Congress should consider the adequacy of DoD policy oversight and inspection arrangements to ensure consistent implementation and quality control for all DoD compenents. As recommended elsewhere, this requires augmentation of OSD security policy staff personnel. An oversight and review committee comparable to SEVEN SCREENS should also be considered.

The difficulties with expanding the use of polygraph examinations in DoD and other departments suggest a need for caution at the national policy level. There is widespread misunderstanding about the use of polygraphs for personnel security screening with CI-related questions and strict quality controls. While a uniform

national policy for access to certain types of highly sensitive data is desirable in theory, more needs to be done to explain the procedures and safeguards to federal employees, the Congress and the public and to compile data on employee reactions to such examinations before a government-wide policy is implemented.

Findings and Recommendations

46. Finding.—Defense Department adoption of Stilwell Commission recommendations is a major step forward. The Committee has supported additional funding in FY 1986 and 1987 to accelerate implementation of recommendations regarding clearance investigations.

47. Recommendation.—The National Strategic Security Program should ensure substantially increased funding for personnel security in all relevant departments and agencies. A Government-wide plan should be submitted to Congress to achieve the following goals: (a) elimination of the reinvestigation backlog for Top Secret (including SCI) within four years; and (b) implementation within less than ten years of a program for intensified investigation and reinvestigation for Secret clearances.

48. Recommendation.—Agreement should be reached as soon as possible on a "single scope" background investigation for all Top Secret and SCI clearances. The uniform policy should provide for: (a) less costly and more timely background investigations and clearances; (b) highest priority for meeting the five-year reinvestigation requirement; and (c) a subject interview in all cases.

49. Recommendation.—Government-wide adoption should be considered for the Stilwell Commission recommendations to prohibit the practice of requesting security clearances solely to provide access to a controlled area, where there is no need to know or even to be exposed to classified information. Reliability investigations should still be conducted in such cases, with standards equal to those proposed by this report for Secret clearances.

50. Recommendation.—More effective means should be established for investigating and clearing immigrant aliens and foreign nationals overseas who are granted access to classified information.

51. Recommendation.—Implementation of the proposal for one-time, short duration access by cleared personnel to the next higher level of classified information should be postponed until Secret clearance requirements and investigations are upgraded and the IG–CM(P) has reviewed the issue.

52. Recommendation.—The Executive branch should study the possibility, in consultation with appropriate congressional committees and civil liberties experts, of a program for requiring those who receive access to the most sensitive information to agree to expanded post-access foreign travel reporting obligations and/or agency access to relevant financial and travel records. Such a program would need to be clearly limited and to incorporate proper safeguards regarding the use of the information obtained.

53. Recommendation.—The National Strategic Security Program should increase personnel security research, including expanded research and evaluation on the wider use of psychological testing in the clearance process, taking full account of individual rights, as well as the implications of recent espionage cases.

54. Recommendation.—The President should issue a new Executive Order on personnel security. The order should provide for government-wide minimum standards and procedures and a policy oversight office similar to the Information Security Oversight Office. It should focus exclusively on personnel security programs regarding access to classified information and to sites where classified information is maintained. Drafting of this order should not delay action on other recommendations.

55. Recommendation.—The National Strategic Security Program should improve the adjudication process for granting or denying security clearances, with more rigorous standards regarding persons who have committed felony offenses; follow-up measures where persons with admitted problems like drug use are cleared; and a government-wide requirement for training of adjudicators. For the most sensitive positions, a "select in" policy based on demonstrated aptitude for security should be adopted in place of the current "select out" policy based on the absence of proved disqualifying factors.

56. Finding.—Agency and interagency investigations of recent espionage cases have highlighted flaws in hiring, assignment and termination practices. Recent corrective efforts in CIA and DoD and proposed government-wide consideration of similar measures should be very useful. The Committee will continue to monitor these efforts to achieve needed corrective action without destroying necessary managerial flexibility.

57. Recommendation.—The national Strategic Security Program should ensure full coordination of departmental policies and practices for the use of polygraphing in personnel security screening so as to maintain stringent quality controls and safeguards for individual rights, to prevent over-reliance on this technique, to provide for necessary research and funding, and to improve understanding of the procedures.

58. Recommendation.—Congress should consider permanent legislation authorizing DoD to use polygraph examinations for personnel security screening with CI-related questions, based on the most recent DoD proposal. If a decision cannot be reached in 1987 because of insufficient test data, then Congress should extend the current test program for a fixed period.

59. Recommendation.—The other Stilwell Commission recommendations on personnel security should be implemented vigorously in DoD with augmented OSD policy oversight, and they should be reviewed at the NSC level for adoption government-wide.

C. INFORMATION SECURITY

In December, 1985, the Committee submitted to the National Security Council a series of recommendations on information security, in response to a request for input on proposals developed by the Information Security Oversight Office (ISOO). In addition to calling for a National Strategic Security Program, as discussed above, the Committee urged immediate implementation of the ISOO proposals with strong, public endorsement of the President and the principal members of the National Security Council. The ISOO proposals would establish new information security policies for curbing over-

classification and over-distribution, improving classification management, enforcing the need-to-know principle, and improving security awareness and investigations of unauthorized disclosures. The Committee recommended that senior executives and program managers be held personally responsible for effective implementation of these policies.

Although the ISOO proposals are an excellent agenda for near-term actions, the Committee made several other recommendations for long-term decisions. First, there is a fundamental problem with the classification system because of its complexity. The Committee recommended consideration of a two-level system, based essentially on the current Secret standard and the Sensitive Compartmented Information model used in the Intelligence Community. A two-tier system offers a better chance of enforcing the need-to-know principle and reversing the natural incentives to over-classification.

The Confidential classification should be dropped, with such information either kept unclassified or protected at the Secret level. The initial decision should be whether the information requires protection in order to prevent substantial harm to identifiable national security interests.

The classification threshold should reflect a policy that classifies information only where truly necessary to maintain the national security. The report on Scientific Communication and National Security, issued in 1982 by a panel of the National Academy of Sciences, warned that undue controls can "weaken both military and economic capabilities by restricting the mutually beneficial interaction of scientific investigators, inhibiting the flow of research results into military and civilian technology, and lessening the capacity of universities to train advanced researchers." The 1985 interagency report on Soviet Acquisition of Military Significant Western Technology reiterated the warning that restricting access to scientific data "may also inhibit the United States' own national research effort." As stated recently by former DIA Director Eugene F. Tighe, "[I]f the U.S. security system for handling classified material is to be useful, only data that are critical to the United States' status as a political, economic and military power should be classified." The assumption should be that information is unclassified, unless there is a specific reason for maintaining secrecy.

The higher of the two classification standards should focus on the much smaller universe of data that require special protective measures above and beyond the normal safeguards for classified information. As is the case with intelligence data designated SCI, classification at the second level should be based on a full analysis of the risks of compromise. Such analysis should ensure that special protective measures are imposed only where necessary and are not diluted by applying them too widely. Careful analysis should also provide the elements for more effective security briefings that help senior policy-makers as well as lower level employees understand the consequences of a security breach.

Executive branch officials have noted that many bilateral and multilateral national security agreements are linked to the current system, and that the handling of Confidential-level foreign material at the Secret level will require some investment. The Committee recognizes that this change must be gradual. It is confident, howev-

er, that the declassification of many U.S.-generated documents that do not merit serious protective efforts will result in significant overall savings that can be devoted to better protection of Secret and Top Secret information.

Another concern is that a higher classification threshold would make more documents accessible to people who request them, either directly or under the Freedom of Information Act. However, unclassified information of a sensitive character can be marked "For Official Use Only" to maintain a policy of not releasing such materials routinely or in response to non-FOIA requests. Concern about FOIA, moreover, should not dictate classification management policy, which should be geared to the most efficient protection against hostile intelligence access to truly important secrets. If a case can be made that specific types of unclassified, but sensitive, information should be exempted from the FOIA, Congress should consider appropriate legislation as has been done for certain kinds of Defense Department technical data. This would be in keeping with the report on Scientific Communication and National Security, which called for development of specific criteria to determine whether unclassified scientific research should be protected by means short of classification.

The other information security recommendations sent to the NSC by the Committee addressed the problem of disclosure of classified information to the news media. The Committee is especially concerned about leaks that compromise sensitive intelligence sources and methods. The Committee emphasized the ISOO recommendation that more effective, unclassified educational materials be developed to explain the damage caused by unauthorized disclosures. The more important recommendation was for new procedures for authorized disclosure of classified information to the news media.

The Committee recommended that the NSC confront the pervasive practice of authorized disclosure of classified information on background, without permitting attribution to the source. By executive order, the President should require each agency to establish procedures to be followed whenever an official authorizes the disclosure of classified information to the news media or in any other public forum. The procedures should apply not only to formal statements for attribution, but also to disclosures on background. They should require that a decision be made to declassify the exposed information or that a record be maintained for purposes of accountability when authority is exercised or granted to disclose information that remains classified. The procedures should require consultation with the agency that originated the information and written designation of the officials in each agency who are authorized to communicate classified information to the media, either in person or through an authorized representative.

Some Executive branch officials oppose such procedures as likely to open the floodgates for "authorized leaks." Others want strict enforcement of a policy that any classified information disclosed to the media be officially declassified. The Committee strongly encourages adherence to a policy that officials speak on the record to the maximum extent. Nevertheless, there may well be valid reasons for retaining a background briefing's classified character. Any serious

effort to address the problem of leaks must face the realities of press-government relations. More leak investigations may accomplish little, moreover, so long as authorized background disclosures continue to divert investigators from cases in which administrative discipline, dismissal or legal action is possible. Policies that ignore "authorized leaks" simply reinforce the climate of cynicism that has fostered disrespect for security.

In addition to the recommendations submitted to the NSC in December, 1985, the Committee has several other information security recommendations. Many proposals of the Stilwell Commission on managing and controlling classified information should be considered government-wide. These include recommendations to:

Require, rather than simply permit, challenges to classifications believed to be improper.

Require a higher minimum degree of accountability for Secret documents.

Impose better controls over reproduction equipment used to copy classified information.

Initiate long-term action to develop technical or mechanical controls over unauthorized reproduction.

Reduce unnecessary retention and storage of classified documents.

Prohibit employees from working alone in areas where Top Secret or similarly sensitive materials are in use or stored.

The Stilwell Commission recommendations on special access programs and on National Disclosure Policy for transfers of classified information to foreign governments are particularly important.

The proliferation of special access programs is testimony to the failure of the current security system. ISOO Director Steven Garfinkel testified that "a number of these programs are probably unnecessary," and the Stilwell Commission reported that some actually afford less security protection than ordinary classification requirements. This situation reflects the fact that, too often, there is no real analysis of the hostile intelligence threat to special access programs or of the reasons why normal security standards and procedures offer inadequate protection. As the Stilwell Commission comments:

> [A]lthough the sole rationale for the creation of Special Access Programs under Executive Order 12356 is to provide enhanced security, there is sometimes too little scrutiny of this determination at the time such programs are created. Unless an objective inquiry of each case is made by the appropriate authorities, the possibility exists that such programs could be established for other than security reasons, e.g., to avoid competitive procurement processes, normal inspections and oversight, or to expedite procurement actions.

The Stilwell Commission's proposed policies, standards and controls for special access programs should be adopted government-wide. The development of minimum security standards for all DoD-established special access programs, which was recommended by the Stilwell Commission and has now begun, should end the temptation to use SAPs as a way to avoid normal security requirements.

The assignment of Defense Investigative Service personnel to work full-time at major contractor facilities may reduce the likelihood of problems like those recently revealed at Lockheed regarding protection of information on stealth technology.

Executive Order 12356 on National Security Information should be modified, moreover, to place more controls on the establishment of special access programs and to give the ISOO Director greater authority to conduct oversight and ensure accountability of special access programs. A revised executive order should designate the Secretary of Defense as the sole official entitled to create or continue defense-related, non-intelligence special access programs. There should also be a comprehensive, one-time review and revalidation of all existing special access programs and associated contracts, with each department and agency reporting the results to the ISOO Director who should make an independent assessment for the NSC.

The Committee believes ISOO has made a valuable contribution to better information security, but its small size (10 professionals) unduly limits its ability to conduct oversight inspections and other in-depth evaluations. ISOO's staff should be expanded to include a permanent element to inspect agency practices at all levels of command and management. While ISOO cannot replace internal inspections, it should do more to ensure the effectiveness of agency inspections by sampling on a periodic basis. ISOO should also work closely with the Defense Security Institute to implement the government-wide policy (proposed by ISOO) requiring seminars and training courses for all levels of commanders and managers, in government and industry, to understand information security policy and procedures, especially classification management.

Classification management training should focus, in part, on the fact that the only valid national security reason for classifying information is that a hostile element whose goal is to damage the interests of the United States should not have use of the information. Throughout the government, most classification judgments are made by the "proponent," i.e., the originator or functional manager responsible for the substance of the information. Few classification authorities consider or have a good knowledge of how a hostile element, government or otherwise, would use a particular piece of information to damage U.S. national security interests.

An informal query of government and industrial managers by Committee staff tends to validate the report that managers are often deficient in their knowledge of classification management requirements and procedures. The proliferation of classified documents and the need for greater security has sprawned an entire dictionary of special classification markings and control systems. The rise of these special markings and control systems has tended to generate a false sense of security and also to confuse those who do not fully understand their meanings. ISOO and the DCI should undertake a thorough reassessment of these practices with a view to simplifying the special markings systems.

Special markings help to enforce need-to-know restrictions by warning a reader what accesses are required to read a document. Equally important, however, is a need for clear assignment of responsibility for determining whether someone has a requirement

for access to information about a particular program. ISOO should review current directives and regulations to ensure that such responsibilities are pinpointed and that compliance is audited regularly.

Finally, the Committee does not believe that legislation to enhance criminal enforcement remedies for unauthorized disclosure of classified information would be appropriate this year. After completion of the appeals in the *Morison* case, a reassessment by both Congress and the Executive branch might be in order. The Committee does, however, support continued investigation of unauthorized disclosures within agencies and by the FBI for purposes of administrative discipline as well as criminal prosecution. When Department of Justice guidelines for leak investigations are reviewed pursuant to ISOO's proposal, they should be revised to reflect this policy. Polygraph examinations should also continue to be used in leak investigations on a voluntary basis in accordance with procedures followed in other types of criminal investigations.

Findings and Recommendations

60. Recommendation.—The Executive branch should immediately implement the Information Security Oversight Office (ISOO) proposals, with strong public endorsement by the President and the principal members of the National Security Council.

61. Finding.—The complexity of the current information security system has led to overclassification, employee confusion and ignorance, inability to protect all the information earmarked for protection, and, at least at times, cynical disregard for security.

62. Recommendation.—The Executive branch should consider simplifying the classification system by establishing two levels, eliminating the current Confidential classification. This streamlining should be preceded by consultation with other countries with whom the United States shares security classification agreements.

63. Recommendation.—An Executive Order should be promulgated requiring each agency to establish procedures governing authorized disclosure of classified information to the news media, including background disclosures of information that remains classified. Such procedures should require records for accountability, consultation with originating agencies, and designation of officials authorized to disclose classified information to the media.

64. Recommendation.—The Executive branch should review the Stilwell Commission proposals on managing and controlling classified information for possible government-wide implementation as part of the National Strategic Security Program.

65. Recommendation.—Executive Order 12356 should be modified to require greater controls on special access programs and to give the ISOO Director greater authority to oversee such programs. The Secretary of Defense should have sole authority to approve defense-related, non-intelligence special access programs. The whole government should conduct a comprehensive review and revalidation of all existing special access programs and associated contracts, with an independent assessment by the ISOO Director. Such reviews should be repeated on a periodic basis.

66. Recommendation.—ISOO's staff should be expanded to include a permanent inspection element. ISOO should work with the

Defense Investigative Service to implement improved training courses on information security and classification management. ISOO and the DCI should also reassess special markings with a view to simplification. ISOO should ensure that agencies designate individuals/positions with responsibility for determining need-to-know access.

67. Recommendation.—The Executive branch should postpone consideration of new criminal penalties for unauthorized disclosure until after the appeals in the *Morison* case. The Committee supports continued internal agency and FBI investigations for purposes of administrative discipline as well as prosecution, including use of voluntary polygraph examinations under criminal investigative procedures. Justice Department guidelines for leak investigations should be revised to reflect current policy of using administrative sanctions when prosecution is not pursued.

D. COMMUNICATIONS, COMPUTER, AND EMANATIONS SECURITY

The rapid expansion of electronic systems and equipment capable of very high-speed transmission and storage of large volumes of information offers striking capabilities and opportunities for the United States, particularly in the areas of national defense and intelligence. Equally striking are the security vulnerabilities of such systems, for which Executive branch efforts to develop and implement countermeasures are in their embryonic stage. The Defense Department and NSA have been given the lead in developing national policy for security countermeasures against hostile intelligence efforts to intercept communications, penetrate computer systems, and monitor the emanations from communications and information processing equipment.

Traditionally, communications security meant the encryption of classified communications and the maintenance of discipline to ensure that classified information was not discussed on open lines. In the 1970s, two weaknesses with this approach came to be recognized. First, it was discovered that the Soviets had a massive capability to intercept communications that could be exploited for significant intelligence value, even if the discussions were unclassified.

The second factor was the inherent human weakness of government and contractor officials, at all levels, who inevitably fail to follow strict security rules. The inaccessibility or inconvenience of secure phones, and the ease of slipping into or "around" sensitive topics, meant that security briefings and penalties were simply not adequate to prevent discussion of classified information on open lines.

Congressional concern about communications security has increased with growing public awareness of the threat. In 1985, Congress enacted Senator Moynihan's proposal that the FBI submit a report to Congress on the measures needed to counter the Soviet surveillance threat to domestic communications. This report was submitted in June, 1986, but was limited to the FBI's counterintelligence support role without discussing steps being taken or planned by the National Security Agency's Information Security Directorate to deny the Soviets access to domestic communications.

The NSA communcations security program is described in detail in the annual budget justification submitted to the Intelligence Committee for the first time in 1985. NSA has recently initiated a major program to upgrade communcations security by developing a low-cost, user-friendly secure telephone system. NSA's leadership in working with private industry to develop such a system may lead to a significant security breakthrough. NSA's plans to work with the private sector by licensing use of essential cryptographic techniques in equipment marketed to the public are unprecedented, and the Committee is satisfied with the efforts to take all equities into account. The Committee supports NSA's plans for secure telecommunications equipment, including the idea of making the equipment available to the private sector; it recommends attention at the highest levels to the need for agencies outside the traditional national security arena to join in this program as appropriate. The Committee will continue to exercise budgetary and policy oversight of NSA's communications security program.

In this regard, the NSA is concerned that current plans do not fully respond to the threat to long-distance communications relayed over satellite links and intercepted from sites like the one in Cuba. While the low-cost secure equipment developed under NSA's leadership may solve much of the problem for government agencies and private firms that can afford the cost, many organizations are much less likely to be able to pay the price. Efforts to neutralize the Soviet intercept operations that damage national security should not depend so heavily on the marketplace. Senator Moynihan, former Vice Chairman of the Intelligence Committee, has proposed a $1 billion program to encrypt all domestic communications satellite links. The Committee has asked for and received a five-year NSA plan to protect the most sensitive links that the Soviets could exploit to damage U.S. security interests. This less expensive proposal is to encrypt all dedicated channels leased by federal government agencies, by private firms with government contracts, and by private firms that communicate large financial transactions and economic forecasts. The Soviet could exploit these unclassified links by piecing together information that, taken in aggregate, is highly damaging to the United States. In the Intelligence Authorization Act for FY 1987, the Committee recommends an increase of $129 million for the communications security program above the funds requested by the Administration. More than half of this increase is to begin implementation of the domestic satellite protection plan.

Another threat comes from hostile intelligence efforts to monitor emanations from equipment and/or electrical lines. This problem generally bears the label Tempest, from the term used for the costly shielding and equipment design measures sometimes needed to ensure against compromising emanations. Improvements are being made in definition of the threat and the most cost-effective countermeasures. The initial security standards developed by the Defense Department and the Intelligence Community were based primarily on the theoretical possibility of compromise. A 1983 interagency assessment of actual and probable threats led to refinement of the threat assessment, since the current threat appears much greater abroad than in the United States. The bulk of Tem-

pest expenditures, however, is still being made in the United States.

On June 27, 1986, the General Accounting Office completed a review of domestic DoD and military service adherence to national Tempest policy for the House Committee on Government Operations. The GAO concluded that more than a year after the issuance of the new January, 1984, Tempest policy, the services all continued to follow their older internal Tempest guidance.

The GAO is of the view that the imposition of "Tempest countermeasures on industry should be controlled from a central point within DoD." Also in order to minimize unnecessary Tempest-related expenditures, the report recommends that the Secretary of Defense require all DoD components to conduct Tempest evaluations before implementing Tempest countermeasures in the United States to protect non-SCI information. Both the Stilwell Commission and an interagency body have recommended increased efforts to relate more closely the extent of the Tempest protective effort in the U.S. to the identified hostile collection threat. The expenditure of funds and effort for unnecessary Tempest protection clearly shows the need for better threat analysis and interagency collaboration in developing the communications and computer security aspects of a National Strategic Security Program.

The Committee sees a similar imbalance in resource allocation in the computer security field. Testimony at Committee hearings indicates a disparity in resources between the technological and human sides of the computer security problem. The overwhelming emphasis today is on increasing expenditures for development of more secure equipment and software, rather than on the personnel and information security measures needed to deal with the human side of the problem. The DCI testified that personnel security is "the most important part of any effective security program," yet the Computer Security Center at NSA and the interagency computer security committee (under the National Telecommunications and Information Systems Security Committee chaired by the Assistant Secretary of Defense for C^3I) have focused mainly on hardware and systems design.

The Stilwell Commission, citing the estimate that redressing the damage from the Walker-Whitworth case could cost several billion dolars, went on to warn:

> Given the range of density of information housed in major DoD computer-based systems, the possibility of remotely accessing terminals over great distance, and the difficulty of detecting exploitation by a trusted person, it is entirely conceivable that a computer-wise traitor could cause catastrophic loss of resources and military advantage.

The security officer for one of the larger military logistics computer systems sites expressed the same concern to Committee staff. The Committee is also concerned about the apparent use of a DoD computer system in a scheme to divert parts to Iran.

The trusted-person threat to computer security is not limited to the Defense Department. The State Department has a problem due to the fact that many embassy computer system managers and operators are foreign nationals. In light of the sensitivity of even un-

classified State Department systems, Members of the Committee sponsored an amendment to the Diplomatic Security Act to protect funding for State Department initiatives to replace those personnel with U.S. citizens.

Because of the seriousness of the computer security threat, the Committee urges consideration of the option suggested in a 1985 interagency assessment: "The only recourse may be for the United States to exclude from these data bases the types of science and technology information that are likely to be used against U.S. interests." The National Strategic Security Program should ensure that the computer security and information security communities jointly develop procedures requiring analysis of computer system vulnerabilities before sensitive material is approved for storage in those systems.

Given the gravity of the personnel security problem, the National Strategic Security Program should address the need for more stringent controls on personnel with access to sensitive computer data bases. As a result of the Walker-Whitworth case, special "crypto-access" controls have been approved for personnel with extensive access to classified cryptographic information. Similar controls should be considered for access to the most vital data bases and networks. Furthermore, such positions should have top priority for institution of personnel reliability program measures, as recommended by the Stilwell Commission for DoD personnel involved in especially sensitive programs.

One reason for the apparent imbalance in attention to technological and human aspects of the computer security problem may be the national policy structure that separates communications and computer security from other security functions. In 1984 the President issued NSDD–145, which made NSA the "national manager" for communications and computer security under a new National Telecommunications and Information Systems Security Committee (NTISSC) chaired by the Assistant Secretary of Defense for C3I. NSDD–145 was an important effort to update national policy, because it recognized the close connections between computer and communications security. The Committee endorses the assignment of NSA, working through its National Computer Security Center, to conduct research and develop computer security hardware, systems and standards not only for DoD, but also for the federal civilian establishment and segments of the private sector. The National Bureau of Standards Institute for Computer Science and Technology is cooperating with NSA in transmitting research results throughout the government and to private industry. These efforts should increase.

Computer security is, however, one of the best examples of why a still broader national policy structure is essential to ensure full attention to all aspects of security counter-measures. While NSA has unique technical capabilities, computer security priorities should be addressed as part of the National Strategic Security Program to ensure that research efforts and resource allocation respond to the most serious actual and probable threats. (Another reason for a framework spanning current jurisdictional divisions is that TEMPEST issues relate closely to technical surveillance countermeasrues, as discussed below.)

Recently, fears have been expressed regarding a "big brother" role in NSA's growing involvement with the civilian and private sectors. The Committee believes that NSA is best equipped to develop technical measures needed to remedy serious vulnerabilities in a timely manner. The Committee also recognizes that both the Executive and Legislative branches must continue to exercise oversight to ensure that the Government does not impose technical solutions that impinge on individual privacy, civil liberties or public confidence.

To improve congressional oversight of resource allocation, program priorities and privacy concerns, the Committee instituted a review of the NSA communications and computer security budget requests beginning with FY 1987. The House Intelligence Committee began this practice last year, and the funds were included for the first time in the Intelligence Authorization Act for FY 1986. While these NSA programs are not part of the National Foreign Intelligence Program and thus are within the concurrent jurisdiction of the Armed Services Committee, they also fall under the Intelligence Committee's general mandate in Senate Resolution 400 for oversight of measures taken to protest against the hostile intelligence threat.

Findings and Recommendations

68. Recommendation.—The National Strategic Security Program should ensure that NSA's plan for low-cost, secure voice telephone equipment is implemented by all government agencies, contractors and offices involved with national security information and other technological, political and economic information of significant value to adversaries.

69. Finding.—A program for encryption of domestic commercial communications satellite links that would be the most lucrative targets for hostile interception of private communications is a worthwhile supplement to the secure phone program. The Committee has recommended FY 1987 funding to begin this program.

70. Recommendation.—The National Strategic Security Program should enforce current national TEMPEST policy for all government agencies, so that decisions to buy TEMPEST equipment are based on the best counterintelligence estimates of actual and probable threats.

71. Recommendation.—The National Strategic Security Program should place greater emphasis on personnel, physical and information security aspects of computer security, including research efforts, and should establish relative priorities for all aspects of computer security countermeasures.

72. Finding.—Because U.S. embassy computers and word processing systems may contain sensitive information, Committee Members sponsored an amendment to the Diplomatic Security Act to protect State Department funds to place U.S. citizens in charge of embassy computers.

73. Recommendation.—The computer security and information security communities should review and improve current procedures for analysis of information system vulnerabilities before sensitive material is approved for storage in such systems.

Page 512 of 3957

74. Recommendation.—Given the gravity of the threat, high priority should be given to strict personnel security controls, comparable to the reinstituted crypto-access program and incorporating personnel reliability programs, for persons with extensive access or potential access to sensitive computer systems.

75. Recommendation.—The National Strategic Security Program should provide for national-level review of communication, computer and emanations security resource requirements, with NSA continuing to be responsible for development of technical measures and standards needed to remedy vulnerabilities. The Committee will continue to oversee the level of effort and to ensure that technical measures are not imposed in a manner that impinges on individual privacy, civil liberties or public confidence.

E. TECHNICAL AND PHYSICAL SECURITY

In June, 1985, the Committee heard detailed testimony on the bugging of typewriters at our Moscow embassy and other Soviet technical surveillance operations. This testimony vividly demonstrated the Soviets' strong technical surveillance capabilities and U.S. vulnerability to sophisticated electronic penetration and eavesdropping techniques. Shortly thereafter, the Inman Panel on Overseas Security submitted to the Committee a compartmented annex to its report to the Secretary of State, showing that the technical security threat is a formidable challenge. The Inman Panel stressed fundamental problems for the State Department and recommended both a reorganization of State Department security operations into a new Diplomatic Security Service and a massive rebuilding program for overseas missions. The Moscow embassy discovery and the Inman Panel report have reawakened the intelligence community and the State Department to the threat of hostile technical surveillance.

The Committee recognized after the June, 1985, hearing that U.S. technical surveillance countermeasures (TSCM) had been seriously underfunded in recent years. Consequently, the Committee proposed what became a $35 million FY 1985–86 supplemental appropriation to enhance security countermeasures at U.S. facilities abroad.

The physical security lapses that allowed Soviet access to State Department equipment and the low funding for technical surveillance countermeasures are matters of grave concern to the Committee. As a result, the Committee accompanied its proposal for a supplemental appropriation with a request for a comprehensive long-range plan for upgrading technical security at U.S. facilities abroad. The outlines of such a plan are beginning to take shape.

The Committee is pleased to note the cooperation and progress achieved in this area by Executive branch agencies in 1986. The best way to marshal their energies is, however, to establish a National Strategic Security Program that can take all interests and disciplines into account. Current interagency mechanisms will benefit from being incorporated in this broader and more formal framework. This recommendation is consistent with an interagency assessment that emphasizes the necessity for total protection of information and telecommunications equipment and with the testi-

Page 512 of 3957

mony of CIA's Security Director that "the best security will be achieved through a program that integrates technical security with other security disciplines."

Many agencies play R&D or operational roles in detecting and denying technical penetration by hostile intelligence services. Adequate TSCM planning must do more than just provide an organizational framework and philosophy. It should outline explicitly the vulnerabilities, requirements, objectives, responsibilities, resources and schedule for short and long-term R&D, training, personnel, inspection and other needs. The Committee looks forward to this level of effort in the future.

Implementing the Inman Panel recommendations, the State Department has established a new Diplomatic Security Service so as to give those who manage its security functions higher status, increased resources and a greater voice in Department management. State has also developed a $285 million construction plan to build more secure facilities in Eastern Europe. The State Department is establishing programs, moreover, to ensure that all information processing equipment sent abroad is under strict security controls. These efforts are a sensible response to the vulnerabilities uncovered by the discovery of the bugged typewriters. The Committee has encouraged development of this program, and Members sponsored an amendment to the Diplomatic Security Act that protects funds for it.

Congress should also support the substantial, multi-year expenditures that will be required to implement Inman Panel recommendations for enhanced physical security at U.S. facilities overseas. Congress funded initial requests to improve embassy security against terrorism, including President Reagan's request for a $110.2 million supplemental appropriation for FY 1985 and the Act to Combat International Terrorism (P.L. 98-533), which authorized $366.3 million for embassy security. The urgent supplemental for FY 1987 appropriates over $700 million to begin the new construction and other security enhancements.

The Committee understands that there must be a "rule of reasonableness" in embassy physical security that takes into account the need for openness and the negative effect of a "fortress" image. Nevertheless, policy and design should be flexible enough to respond not only to the terrorism threat, but also to the hostile intelligence threat.

Security expertise in other agencies can contribute significantly to the success of the embassy construction program and it will be important to factor technical security requirements into both the planning and the construction of new facilities. This Committee has worked closely with the Senate Appropriations Committee to provide funds and positions in the FY 1987 urgent supplemental for such assistance to the Foreign Buildings Office of the State Department.

The State Department advises that budget constraints have required modification of the plans for certain construction which originally would have made necessary security improvements in FY 1988. The revised plan stretches out construction work through FY 1990. The Committee urges the Administration to accelerate its

decisions in light of long-range, tailored security plans for each of these missions.

Findings and Recommendations

76. Recommendation.—The Executive branch should continue to place greater emphasis on the development of means and the implementation of actions to detect and defeat technical penetrations of sensitive facilities. The National Strategic Security Program should reconcile the various technical security interests and integrate them with other security disciplines.

77. Finding.—Executive branch actions in 1986 to upgrade security functions and to coordinate technical security efforts have been a notable step forward. They deserve continuing high-level support and resource commitments.

78. Finding.—State Department plans to improve the security of information processing equipment constitute a reasonable approach to the technical penetration problems. Committee Members have moved to ensure that the needed funds to begin these programs are available.

79. Recommendation.—Congress and the Executive branch should support implementation of the Inman Panel recommendations for major site and/or physical changes to U.S. facilities abroad to enhance security, minimize acts of terrorism and prevent hostile intelligence penetration.

80. Recommendation.—The State Department should ensure that security experts in other agencies are given full opportunity to participate in the planning and oversight of new embassy construction efforts to achieve a comprehensive security system. Decisions on long-range, tailored security plans for overseas missions should be accelerated.

F. INDUSTRIAL SECURITY

Espionage cases of the past ten years, involving such industry personnel as Boyce, Lee, Bell, Schuler, Harper and Cavanagh and the loss of sensitive technological information through increasing levels of espionage and illicit transfer, have highlighted the priority that hostile intelligence services attach to U.S. technology. The interagency report in 1985 on Soviet Acquisition of Militarily Significant Technology described the threat, and its findings are confirmed both by Soviet documents obtained by the French and by the testimony of Soviet bloc defectors. Industry is vulnerable to recruitments by hostile services and to employees who volunteer their information for pay. Industrial communications are vulnerable to Soviet interception; and industrial facilities are susceptible to technical penetration, especially overseas. Co-production agreements with foreign firms compound the difficulties.

Hostile intelligence successes in penetrating U.S. industry, culminating in the Harper case, triggered an in-depth review of industrial security programs and policies in 1984 by a DoD Industrial Security Review Committee (also known as the "Harper Committee"). This review was particularly important because DoD has been delegated industrial security responsibility for eighteen federal departments and agencies. The Harper Committee's 25 recommendations

are designed to enhance industrial security dramatically. While not all have been adopted by DoD, the majority are being implemented as proposed or with some revisions. The Committee urges prompt action on the Harper Committee reforms that have been approved for implementation. The National Strategic Security Program should also review those recommendations for government-wide implementation.

Several Harper Committee proposals deserve special emphasis. First is better integration between counterintelligence and industrial security. In the past, there has been a reluctance on the part of the counterintelligence community to communicate with industrial security officers. While such communication is improving, particularly in security awareness programs such as the FBI's DECA program, there is ample room for closer cooperation. There should be a continous two-way sharing among counterintelligence agencies and government and industrial security officers. Counterintelligence agencies should provide more tailored information on the hostile intelligence threat to particular programs or types of programs, as well as in particular geographical areas, for use in security awareness efforts and the design of security measures.

A pilot program should be initiated for assignment of Defense Investigative Service personnel to large sensitive contractor facilities on a full-time basis, and the National Strategic Security Program should review the results as a basis for considering a similar government-wide practice. With 95 percent of all classified documents (an estimated 15 million out of 16 million) residing with only 4 percent of the cleared industrial contractors, the case for a continuing government security presence at those facilities is strong. It is further enhanced by the admissions of the Chairman of the Board of Lockheed regarding the sloppiness of the company in accounting for classfied documents. A GAO investigation had revealed that Lockheed was unable to account for nearly 1,500 documents due to inadequate controls. A reordering of priorities to concentrate on major contractors will not result in the government taking over contractor security functions, but rather will permit timely audits of security functions and correction of problems in primary facilities.

As discussed in the section on personnel security, a single-scope background investigation for Top Secret and SCI clearances would especially benefit industrial security. The five-year goal for clearing up the backlog of periodic reinvestigation for Top Secret and SCI, if applied government-wide, would similarly benefit contractors who are on the leading edge of U.S. intelligence technology. The Committee has added funds to agency budgets for this purpose on more than one occasion.

Industrial security managers have had to cope with tremendous needs for, and resultant delays in, clearance investigations for industry. With the large defense buildup in recent years has come a dramatic rise in the number of contractor personnel holding security clearances. Between FY 1978 and the end of FY 1985, the number of such clearance investigations per year increased from 28,000 to 75,000. The Defense Department's recent twenty-percent reduction in clearances should help ease this burden.

Page 516 of 3957

Federal Acquisition Regulations should be changed to designate security requirements for classified contracts as a direct cost. When security is designated as a direct cost instead of an overhead cost, industrial security officers are relieved of the opposing pressures of the government-customer who demands more and better security and the company officials who see security as a drain on profitability. In addition, the designation of security as a direct contract cost will force the customer to more precisely define his security requirements in the Request for Proposals (RFP) and in security deliverables. While this approach may appear more costly to the taxpayer, in the long run it will result in greater cost savings through effective planning and cost controls.

Consideration should also be given to the greater use of Cost Plus Award Fee (CPAF) contracts as an incentive for fulfilling contract security requirements and specifications on time, within cost and without security violations. Making security a major award fee determinant along with the other award fee elements will give contractors for classified contracts the motivation for ensuring that more and better-qualified security planning and operations personnel are assigned and retained on contracts.

Training and government certification of all current and planned contractor security officers should be required in each classified contract. As pointed out in the Harper Committee report, the intense targeting by hostile intelligence services of the large amount of classified data entrusted to contractors, as well as the absence of a formal training program for industrial security officers, justifies the government's establishment of this requirement. The requirement for training and certification should also apply to personnel with security responsibilities for special access program contracts.

A final and most disturbing concern is the hostile intelligence threat to foreign subsidiaries of U.S. firms and to foreign firms that have co-production agreements with the United States. Although U.S. counterintelligence efforts abroad, both unilateral and in concert with our allies, can help deal with this problem, it also requires national policymaker attention. The Stilwell Commission warned specifically of the critical problem with co-production arrangements, "where losses could entail not only the end-item being produced but also the technical 'know-how' necessary to manufacture it in large quantities." Other weaknesses identified by the Commission include insufficient controls in the sale of classified weapons systems and ineffective security surveys. The Committee fully endorses the Stilwell Commission's recommendations for improving the National Disclosure Policy, which governs transfer of classified military information to foreign recipients. The following approach would be required in approving classified transfers:

(1) requiring a determination that the need of the recipient cannot be satisfied by unclassified systems or data;

(2) if classified systems or data are required, then requiring selection of a model or type of such system that minimizes the need to transfer classified information;

(3) requiring phasing in of the most sensitive classified information over time, if feasible;

Page 516 of 3957

Page 517 of 3957

(4) avoiding co-production of military systems which involve the manufacture of the most advanced version of classifed components or end-items.

In addition, security surveys would be conducted by a permanent professional staff with flexibility to meet pressing needs for in-country security assessments. The National Strategic Security Program should ensure that such improvements are implemented not only for military information, but for sensitive intelligence and nuclear matters as well.

Findings and Recommendations

81. Recommendation.—The National Strategic Security Program should foster better communication between U.S. counterintelligence agencies and industrial security officials and provide more tailored information on the hostile intelligence threats to particular programs or areas.

82. Recommendation.—DIS should initiate a pilot program for assignment of its personnel to large sensitive contractor facilities on a full-time basis, and the results should be reviewed as a basis for a similar government-wide practice.

83. Finding.—Recently adopted goals for ending the reinvestigation backlog for contractors holding Top Secret and SCI clearances who are currently involved in sensitive classified contracts merit high-level commitment and support.

84. Recommendation.—Federal Acquisition Regulations should be changed to designate industrial security for classified contracts as a direct cost. The primary intent of this proposal is to identify and monitor security costs associated with particular contracts.

85. Recommendation.—Consideration should be given to greater use of Cost Plus Award Fee contracts as an incentive for fulfilling contract security requirements.

86. Recommendation.—Trained and government-certified security officers should be required in each classified contract, including those for special access programs.

87. Recommendation.—The National Strategic Security Program should ensure implementation of the Stilwell Commission recommendations on National Disclosure Policy not only for military information, but for sensitive intelligence and nuclear matters as well.

88. Recommendation.—Other Harper Committee recommendations approved by DoD should be implemented promptly and reviewed for government-wide application.

G. CONGRESSIONAL SECURITY

In December, 1985, Randy Jeffries, an employee of a private firm that transcribed classified hearing transcripts for congressional committees, was arrested for attempting to sell classified material to Soviet intelligence. The FBI detected the employee making contact with the Soviet Military Office in Washington. The employee admitted giving the Soviets excerpts from a classified transcript of a House Armed Services Subcommittee hearing on Defense Department command, control, communications and intelligence programs. The subsequent FBI investigation revealed that the employ-

Page 517 of 3957

Page 518 of 3957

ee had been observed by a co-worker removing classified documents from the firm under his coat and that a friend of his had destroyed a locked briefcase given to him that possibly contained classified documents. Jeffries pleaded guilty in January, 1986, to a charge of supplying national security documents to a person not entitled to receive them. This offense carries a maximum sentence of ten years in prison.

The case highlights the fact that Congress is not immune from the espionage problems that have surfaced throughout the government in recent years. Both Executive branch and congressional inquiries have emphasized the need to enhance congressional security in response to espionage threats. In November, 1985, the Stilwell Commission expressed the following concerns about the handling of classified information by Congress:

> [A]lthough Executive Order 12356 provides that departments and agencies may disseminate classified information to persons outside the Executive branch provided such information is given "equivalent protection" by the recipient, DoD elements frequently provide classified information to the Congress without any understanding of how such information will be protected. While all congressional staff members who receive access to classified DoD information are, in theory, cleared by DoD, little attention is given the handling and storage of such information by congressional staffs, who are not, in fact, bound by the safeguarding requirements of Executive Order 12356.

The Stilwell Commission recommended that the Secretary of Defense take the following actions:

> Urge the President of the Senate and Speaker of the House of Representatives to adopt, for each House of Congress, rules to provide uniform minimum control over classified information provided by departments and agencies of the Executive Branch. Volunteer to provide DoD resources and assistance to Congress to achieve this goal.

In January, 1986, the Report on the Federal Government's Security Clearance Programs by the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs addressed this subject in the following observation:

> Congress must also focus on problems dealing with classified information in the legislative branch. For the most part, there are no established standards and procedures. Personal offices and Committee practices vary widely in terms of their handling of clearances and classified material. There are few, if any, checks in this system. We believe an overall review of security procedures in the legislative branch should be conducted by the Rules Committee, in consultation with the Intelligence Committee, with a goal of recommending improvements where needed.

The Chairman and Ranking Minority Member of the Subcommittee, Senators Roth and Nunn, addressed this issue through preliminary letters to the Senate leadership.

Page 518 of 3957

The Senate Intelligence Committee has received information from the FBI and other U.S intelligence agencies regarding the operations of the intelligence services of Communist countries directed at Members of Congress and their staffs, including attempts to recruit or place agents in Congressional offices. Electronic surveillance of domestic communications by foreign countries also poses threats to Congress. Only a few congressional offices have secure telephones linked through the Executive branch system.

The information provided to the Intelligence Committee about the espionage threat to Congress indicates a continuing pattern of activity designed to exploit vulnerabilities in security. In three cases over the past ten years, the FBI has uncovered and disclosed publicly Soviet bloc attempts to recruit and place American citizens as agents inside Congressional offices. U.S. counterintelligence successfully prevented any damage in the following cases:

In 1976 a political scientist employed by the Atlantic Council, James Frederick Sattler, was revealed to be attempting to secure a position with a House Foreign Affairs Subcommittee, after being recruited and trained as an espionage agent by East German intelligence.

In 1980 a former CIA case officer, David Barnett, was prosecuted for espionage based on evidence that he had sold CIA information to Soviet intelligence and had attempted to gain employment with the Senate and House Intelligence Committees on the instructions of Soviet intelligence.

In 1982 a staff assistant to a House Member reported to the FBI an effort by Soviet intelligence to recruit him as an agent. At the FBI's request, the staff member became a "double agent" to learn more about Soviet intelligence techniques and aid U.S. counterintelligence.

In other cases, which have not been disclosed by the FBI, there is additional evidence of espionage targeting of Congress by Communist intelligence services.

In more general terms, the FBI has described the techniques used to penetrate the Congress. Communist countries assign intelligence officers to the United States as diplomats, journalists, trade representatives, and in similar capacities. Some of these intelligence officers are instructed to cultivate associations with Members of Congress and congressional staff for the purpose of developing confidential relationships. A well-trained intelligence officer knows how to approach individuals so as not to appear in any way hostile or threatening. Sophisticated and skillful intelligence officers can establish relationships that seem entirely innocent. Professional, academic or social contacts lead to friendships without any suggestion by the intelligence officer of anything illegal or improper. Only when the intelligence officer has learned enough about an individual's vulnerabilities will an effort be made to exploit the relationship.

Lax security practices offer greater opportunities for an intelligence officer to succeed in compromising a congressional staff member. Unlike Executive branch personnel, congressional staff have no requirement or established procedure for reporting contacts with representatives of Communist countries. In some cases,

Members or their staff do report such contacts to the FBI, but the record is very uneven.

The purpose of contact reports is to assist the FBI's investigations of suspected foreign intelligence officers. The FBI has advised the Intelligence Committee that its investigations of suspected intelligence officers disclose many contacts with individuals who, after further inquiries, are found to be congressional staff. Contact reports save the FBI much time and effort, as well as enabling it to advise staffers on how to handle such contacts. That agency has raised with the Intelligence Committee the need for a more formalized procedure in the Senate for briefing staff on the espionage threat and for reporting contacts with representatives of Communist countries.

Another matter that the FBI has discussed with the Intelligence Committee is the handling of classified documents in the personal offices of Members. The FBI has offered to develop both classified and unclassified briefings on the espionage threat to Congress from the intelligence services of Communist countries. The Defense Department, which is responsible for most of the security clearances for congressional staff, might be an appropriate source of assistance in briefing staff on the handling of classified materials.

In an effort to address issues related to Senate classified information security, the Senate Sergeant at Arms, in November, 1985, circulated a Senate Select Committee on Intelligence questionnaire to all Members' personal offices and Committees of the Senate. The results of that questionnaire were not encouraging. Based on responses from 60 Senators' offices, the following conclusions can be drawn:

There is confusion about the levels and sensitivity of the classified information received in personal offices.

There is no uniform procedure followed for storage or control of classified information in personal offices.

Staff with clearances in personal offices rarely receive security indoctrinations or other security education.

As a result of the security survey and the foreign intelligence threat to the Congress, the Senate Select Committee on Intelligence, together with the leaders of the Committee on Rules and Administration and the Committee on Governmental Affairs, determined that the key to addressing the Senate's information security problems lies in the creation of a central office within the Senate to develop and oversee much-needed standards and procedures on important personnel security and information security issues.

The security assistance that a central office would provide includes:

Receiving, controlling, transmitting, storing and destroying classified material.

Processing clearance requests for personnel of the Senate.

Maintaining a centralized record of clearances held by personnel of the Senate.

Presenting security briefings and debriefings for the benefit of Senate personnel.

Consulting on security issues with the personal offices and committees.

64-268 O - 86 - 4

Conducting administrative liaison with other U.S. Government agencies on behalf of the Senate.

A particularly troublesome question relating to classified information security is the large number of Senate staff having access to classified material. The Senate security office should be required by resolution to conduct a comprehensive survey of all Senate offices to determine which officers and employees hold security clearances. The director would report this information within 90 days to the Majority and Minority Leaders along with comments and/or recommendations as to the feasibility of reducing the number of Senate staff with security clearances.

Another early task of the proposed office should be to devise a Senate Security Manual whose provisions, if approved by an oversight group and the full Senate, would be binding on all Members, Officers and employees. The Committee has provided to the Senate leadership a draft Senate security manual to serve as a basis for discussion which is reprinted in Appendix G to this Report. The draft security manual contains standards and procedures both for the handling of classified information and for personnel security.

Findings and Recommendations

89. Finding.—Hostile intelligence services have attempted to penetrate the staffs of Senate and House Members and Committees. Hostile services use sophisticated techniques to develop contacts that can lead to intelligence recruitments.

90. Finding.—Lax security practices in the Senate increase the risk of compromising sensitive information. There is no requirement or procedure for reporting contacts with representatives of Communist countries. There are no established procedures for handling classified information, especially in Member offices. There is no accountability for the handling of such information, and there is great confusion about the sensitivity of the information and what should be done with it. There is no central point where the number of Senate employees with security clearances is tallied or where such services of common concern as security briefings and day-to-day information security assistance are provided.

91. Recommendation.—The Senate should establish a central security office to develop and oversee standards and procedures on important personnel security and information security issues.

92. Recommendation.—A central security office, once established, should immediately survey all Senate offices to determine which offices and employees hold security clearances. This information should be reported within 90 days to the Majority and Minority Leaders along with comments and recommendations on the feasibility of reducing the number of Senate staff with security clearances.

93. Recommendation.—The proposed office should develop a Senate Security Manual, the provisions of which would be binding on all Members, Officers and employees.

94. Recommendation.—All Members and employees of the Senate should be encouraged, and employees with security clearances required, to report contacts with Communist country officials or other suspected foreign intelligence officers. The central security

Page 522 of 3957

office should establish a procedure for such reporting, either through it or directly to the FBI.

95. Recommendation.—Further recommended items for consideration by the Senate security office include: establishment of a Senate corps of cleared employees for transcribing and reporting classified hearings; and improvement in the communications security of telephone conversations, classified computer data, and face-to-face discussions of a sensitive nature.

Page 522 of 3957

APPENDIXES

APPENDIX A

UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, PLAINTIFF,

v.

JERRY ALFRED WHITWORTH, DEFENDANT.

Criminal No.: 85-0552 JPV

Affidavit of Rear Adm. William O. Studeman, Director of Naval Intelligence

1. I am William O. Studeman, a naval officer presently holding the rank of Rear Admiral. I was commissioned an Ensign in the Navy in 1963, and have served virtually continuously on active duty as a naval intelligence officer since that time. My present position is that of Director of Naval Intelligence, which I have held since September 1985. As Director of Naval Intelligence, I am responsible for the collection, analysis and distribution of intelligence information within the Naval Service. I am the Navy's sponsor for counterintelligence programs executed by the Naval Security and Investigative Command, under the policy auspices of the Office of the Secretary of Defense. I offer this affidavit to the Court for use as it deems appropriate in constructing an appropriate sentence for the defendant in this case.

2. The defendant in this case, formerly Senior Chief Petty Officer Jerry Alfred Whitworth, served the United States Navy for 24½ years, 18 of which were in the rate of Radioman, rising to the rank of Senior Chief prior to his retirement. The primary function of a Radioman is to provide and maintain the ability of Department of Defense and naval forces to communicate with each other as well as senior and subordinate commands. Unlike the navies of old, virtually all the information required to plan, operate, command, maintain, modernize, repair, replenish, warn, inform and control the military forces of all the services and our allies is exchanged electrically via communication systems, most of which are considered secure by virtue of their cryptographic cover. Electrical distribution of naval messages is an essential backbone activity designed to reach all levels of command in the Navy. This naval communications system is operated by some of our brightest people who are given the tools, training and sacred trust to protect the vital high technology systems and access to sensitive secrets which are placed

Page 523 of 3957

in their hands. It is important, therefore, to understand the vulnerabilities inherent in naval communications, to understand the concept of crytographic support to communications security (COMSEC) and to understand how Radioman Senior Chief Jerry Whitworth's violation of his trust as a member of the elite fraternity of naval communication professionals has resulted in unprecedented damage to the Navy and the nation.

3. Cryptographic systems are designed to encipher information so that only the holders of the system will be able to decipher that same information. Contemporary crypto-equipments accomplish enciphering and deciphering on the basis of complex mathematical formulas called "logic", which are designed as an integral part of the system with changeable additives called "key". To decipher an intercepted message, an adversary must know both the logic and the key of the cryptosystem used to encipher it. Since it is effectively impossible to ensure that the logic of a cryptosystem will not be compromised during the years it remains in effect, the security of our machine cryptosystems depends on ensuring the integrity of the associated key and the personnel who care for the system. "Key" literally will unlock the secrets contained in encrypted communications.

The ultimate vulnerability of cryptosystems and all procedures designed to protect sensitive information lies at the human level. For this reason, personnel chosen for communications-related duties are carefully screened and indoctrinated in the especially sensitive nature of the positions they hold and the fiduciary-like nature of the trust placed in them. No system ever designed can be invulnerable to the corrupt, cleared individual who has access to sensitive information. Thus, we depend on an individual's integrity and deterrence of the law to ensure that this trust is fulfilled.

4. The importance of key was amply demonstrated by the evidence in this trial. The Soviets were clearly willing to pay a high price for key—more than $300,000 for the defendant alone. But the price paid by the Soviets pales in comparison to its worth. Naval intelligence analysis has led us to conclude that the Walker-Whitworth espionage activity was of the highest value to the intelligence services of the Soviet Union, with the potential, had conflict erupted between the two superpowers, to have powerful war-winning implications for the Soviet side.

5. The importance of the individual spy cannot be overestimated in this type of intelligence acquisition. When an adversary covertly obtains the protective key supplemented by large volumes of actual messages, he can potentially read any or all intercepted messages which that key protects. In the case of Navy operational command circuits, this can be literally hundreds of messages per key setting, many of which are vital to the national security of the United States. Normally, the information contained in those encrypted messages could be expected to include, at a minimum, further plans, ship locations and transit routes, military operations, intelligence activities and information, weapons and sensor data, naval tactics, terrorist threats, surface, subsurface and airborne doctrine and tactics, and similar information which could prove of incalculable value to hostile powers. Undetected theft of cryptographic key by persons intent on penetrating COMSEC safeguards can have ex-

Page 525 of 3957

tremely dire consequence to the defense posture of the nation. History is replete with examples of the benefits and risks associated with COMSEC made vulnerable by espionage or otherwise penetrated for the benefit of one side or another. Such vulnerabilities sustained over time have altered the course of history and can do so again in the future.

6. With respect to this specific case, the sheer volume of encrypted data compromised to the Soviet Union makes it impossible to describe all of that data with specificity. The Court has already heard a few of the specifics during trial; therefore, in paragraphs 7-9, I will simply describe generically the types of information which have likely been traded to the Soviet Union through the years of this espionage enterprise. I will briefly mention some of the more significant aspects of the defendant's activities. I will also provide to the Court certain conclusions I have drawn concerning these compromises. My conclusions are based on my twenty-four years experience as a naval officer, as both a user and producer of intelligence information, and on my current responsibilities as Director of Naval Intelligence and the Senior Intelligence Officer for the Department of the Navy.

7. *Ship location and transit information.*—This is perhaps the most common type of information transmitted over naval communications circuits. On any given day the transit passages and locations of numerous naval vessels, both U.S. and allied, will be transmitted in encrypted radio traffic. Normally, this type of data is held confidential until the information is no longer valid. The reasons that ship locater information is temporarily classified are three-fold. First, simple prudence dictates that the location of ships of the line be held confidential while that sort of information can enhance their vulnerability. This is especially true during periods of hostility. For example, during the Vietnam era, compromises of this type of information could have been responsible for ineffective air strikes, downed aircraft, abandoned targets and infantry losses. It is also particularly true today when U.S. and allied vessels pose a lucrative target for terrorist attack. Secondly, the location and transit routes of naval vessels can be valuable information leading to disclosure, either directly or by informed analysis, of naval doctrine and tactics. This, in itself, could prove to be decisive to the outcome of an engagement at sea. Finally, the rationale that persuades the United States to maintain the confidentiality of ship movements is universally shared by allied nations. Disclosures of transit movements of our allied navies would be as potentially harmful to them as to our own ships; therefore, inappropriate disclosures of such information resulting from breaches of U.S. security could reasonably be expected to have some adverse impact on both foreign relations and on international military cooperation.

8. *U.S. Naval operations information.*—The volume of communications traffic concerning naval plans and operations is large. As with the previous section, analysis of naval plans and operations information can lead, either directly or by informed analysis, to disclosure of naval excerises, contingency activities, and future combat operations which can be exploited to the advantage of a hostile power. In addition, communications will invariably reveal classified technical information, intelligence data, intelligence sur-

Page 525 of 3957

veillance activities or information critical and potentially harmful to the foreign policy of the United States. It would directly reveal substantive information used by the United States in making decisions concerning the security of the nation and its foreign policy. If a hostile power were to obtain that information, it would be possible to turn this newly acquired information to the disadvantage of the United States, either by adopting measures to counter the advantage otherwise available to the United States, or by inserting misleading data into the collection process. An indirect benefit of obtaining this information would be the ability to analyze it for intelligence value, and to inferentially extrapolate the location and concentration of resources dedicated by the United States to obtaining similar information worldwide. Thus, disclosures of specific data can lead to harmful results, both for the specific collection activity involved, and also for similar activities conducted worldwide by U.S. forces and other agencies of the government.

9. *Special category (SPECAT) information.*—Frequently it is necessary to transmit information which is of such a degree of sensitivity that its disclosure must be limited to only those individuals with an absolute need to acquire the data. One method of restricting access to especially sensitive information is to permit its dissemination only within special, restricted channels of communication called Special Category (SPECAT) channels. The defendant was on several occasions in a position to have access to SPECAT communications and had the ability to transfer the information to the Soviet Union.

Some examples of operations that are planned and executed through SPECAT channels are:

a. Covert Military Operations: Disclosure of communications concerning covert operations jeopardizes the United States' ability to conduct missions vital to the national defense and world peace. The risks involve not only extreme embarrassment to our government, but also danger to the lives of the personnel involved.

b. Counterintelligence Operations: Only through the aggressive pursuit of counterintelligence initiatives such as double-agent operations, surveillance, and eavesdropping can the United States protect itself from the threat of espionage conducted against our defense establishment. Disclosure of SPECAT communications concerning such operations allows hostile intelligence services to develop countermeasures and techniques to render these operations ineffective.

c. Human Intelligence (HUMINT) Operations: HUMINT is unquestionably the most fragile of intelligence sources, due to the difficulties in recruiting human agents, the ease with which they are lost, the personal danger often involved and because the quality of information is entirely dependent on the abilities of the individual recruited. Disclosure of any information relating to HUMINT operations, even the intelligence report derived from HUMINT can lead to loss of the source, personal harm to the agent and the insertion of false and misleading information through the agent once the target organization becomes aware.

Page 527 of 3957

10. Based upon an analysis of Whitworth's access to classified information during his participation in the espionage scheme, on the trial testimony, and on debriefings conducted by the Office of Naval Intelligence, we wish to point out certain areas of concern:

a. Mr. Whitworth met with John Walker two to four times per year between 1976 and 1985, and supplied Walker with between twenty-five and fifty rolls of Minox film at each meeting. Since the rolls were undeveloped, Walker cannot assure us of their content, but he believes that it was largely photographed key material. The amount of money paid by the Soviets corroborates that belief. Whitworth was originally paid $2,000 per month for the material he supplied, however, this was subsequently increased to $4,000 and then $6,000 per month later in the conspiracy.

b. We also know that Whitworth compromised detailed plans for primary, secondary and emergency communications circuits which are used by the National Command Authority to maintain contact with operational units. With this knowledge, an adversary can gain significant advantage during crisis events or hostilities.

c. Whitworth also compromised operational military plans, operations orders, and operational message traffic over a significant period of time. For example, he provided the Soviets with a full year of operational message traffic from the USS Enterprise, including TOP SECRET information. He also compromised the operations order for Fleet Exercise 83–1, a unique exercise conducted near the Soviet coast by three carrier battle groups. We believe that he also compromised the communications plan for all U.S. naval forces in the Indian Ocean and all littoral nations.

11. Most importantly, the activities of Jerry Whitworth, continuing as the principal agent of collection for John Walker, permitted the Soviets to gauge the true capabilities and vulnerabilities of the U.S. Navy. The U.S. Navy is a technology-intensive service, conducting sophisticated and often sensitive operations using highly advanced warfare capabilities. Soviet access to those operations and capabilities provided them with the motivation to dramatically improve the Soviet military posture, and identified the specific steps which could achieve the largest gains relative to the U.S. It allowed them the focussed insights required to reduce their own vulnerabilities while simultaneously increasing the vulnerability of the U.S. We have seen clear signals of dramatic Soviet gains in all naval warfare areas, which must now be interpreted in light of the Walker-Whitworth espionage conspiracy conducted over approximately two decades. Mr. Whitworth's role was all the more important because of the new directions taken by the U.S. Navy during his years of collection for the Soviets. For example, through Whitworth the Soviets were able to monitor the U.S. Navy transition to use of satellite systems as its principal communication network.

12. In conclusion, the U.S. Navy and the nation have been seriously wounded by Jerry Whitworth's breach of faith and honor wherein he agreed to sell the secrets with which he was entrusted to a foreign power for personal gain. His misuse of a position of trust in naval communications has jeoparized the backbone of this

Page 527 of 3957

country's national defense. Recovery from the Walker-Whitworth espionage will take years and millions of taxpayer dollars. Even given these expenditures, we will likely never know the true extent to which our capabilities have been impaired by the traitorous and infamous acts of Jerry Whitworth.

WILLIAM O. STUDEMAN,
Rear Admiral, United States Navy.

Subscribed and sworn to before me this 25th day of August 1986.

PATRICK A. GENZLER,
Lieutenant Commander,
Judge Advocate General's Corps, United States Navy.

Notary service provided in accordance with 10 U.S.C. sec. 936.

UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, PLAINTIFF,

v.

JERRY ALFRED WHITWORTH, DEFENDANT

CR. No. 85-0552 JP

I, John L. Martin, declare under penalty of perjury that the following is true and correct:

1. I am Chief of the Internal Security Section of the Criminal Division of the United States Department of Justice in Washington, D.C. As such, I am responsible for the supervision of all investigations and prosecutions of violations of the espionage law. In the performance of my official duties, I am routinely briefed on foreign counterintelligence matters by the agencies of the United States intelligence community including the Federal Bureau of Investigation, Central Intelligence Agency and National Security Agency.

2. By virtue of my position in the Department of Justice, I am aware of the facts surrounding the defection to the United States in July, 1985, of Admiral Vitaly Yurchenko, then a high official of the primary Soviet intelligence agency, the K.G.B. (Committee for State Security). The information set forth in this declaration was provided to me by United States government officials who were responsible for debriefing Admiral Yurchenko.

3. Vitaly Yurchenko defected to the United States by voluntarily walking into the United States Embassy in Rome, Italy, in July, 1985. Yurchenko was at that time a 25-year veteran of the K.G.B., having attained a military rank in the Soviet Navy of Admiral and serving since March of 1985 until his defection as Deputy Chief of the First Department of the First Chief Directorate. The First Chief Directorate of the K.G.B. is responsible for the clandestine acquisition of intelligence outside the Soviet Union, and the First Department of that Directorate is responsible for such activities in the United States and Canada. Previously, Yurchenko served as Chief of the Fifth Department of Directorate K of the K.G.B., where he supervised internal security matters, including cases involving suspected espionage by K.G.B. officers. Yurchenko had various responsibilities for internal security matters for a ten year

Page 529 of 3957

period, including a five-year assignment from 1975 through 1980 as principal security officer at the Soviet Embassy in Washington, D.C. In that position, he was in charge of liaison between the embassy and United States law enforcement officials concerning the security of the embassy, and had responsibility for assuring the loyalty and security of K.G.B. officers asigned to the Embassy. During his career, Yurchenko was the recipient of many awards and decorations. In July, 1985, shortly before his defection, Yurchenko received the K.G.B.'s highest honor, the title of "Distinguished Officer of the Organs of State Security."

4. One of Yurchenko's responsibilities as a Deputy Chief of the First Department of the First Chief Directorate was to review and supervise the handling of important cases in the United States and Canada. Moreover, because of his previous experience and expertise in matters of security in the K.G.B., Yurchenko was frequently consulted when K.G.B. officers came under suspicion of having been compromised.

5. As the evidence in the trial of this case showed, John Anthony Walker, Jr. was observed making a "drop" of classified information to a Soviet intelligence officer on May 19, 1985. He was promptly arrested and charged. Publicity concerning his arrest was widespread. It was also widely publicized that Walker's former wife, Barbara Walker, had tipped the FBI to Walker's espionage months before his arrest.

6. Soon after Walker's arrest and the attendant publicity, Yurchenko was briefed and consulted about the Walker case. The K.G.B. did not believe that the FBI had been tipped by Barbara Walker and suspected that one of the K.G.B. officers directly involved with Walker had been compromised by Western intelligence agencies. Because of his expertise in internal security matters, Yurchenko's advice was sought with regard to the appropriate course of action for dealing with the suspected compromise. In his position in the First Department, it was also appropriate to brief him concerning the Walker/Whitworth case. Because of the high degree of compartmentalized protection given to a case like Walker-Whitworth, Yurchenko, despite his previous assignments involving internal security and at the Soviet's United States Embassy, had not previously been aware of the Walker/Whitworth operation.

7. From his briefings, Yurchenko learned that the K.G.B. regarded the Walker/Whitworth operation to be the most important operation in the K.G.B.'s history.

8. Yurchenko stated that the information delivered by Walker enabled the K.G.B. to decipher over one million messages. Early on, operation was transferred to Department Sixteen of the K.G.B, which handles only the most sensitive and important clandestine K.G.B. operations around the world.

9. The K.G.B. officers who handled the operation received important promotions and decorations for their successes. One of these officers secretly received the "Hero of the Soviet Union" award after the Soviet Navy expressed its delight over the success of the operation. Two other K.G.B. officers involved with the Walker/Whitworth operation were awarded the coveted "Order of the Red Banner." Certain K.G.B. officers from Department Sixteen were, at various times, assigned to the Soviet Embassy in Washington solely

Page 529 of 3957

Page 530 of 3957

to handle "drops" made in connection with Walker/Whitworth espionage. The most recent of these, Aleksey Tkachenko, was returned to the Soviet Union when Walker was arrested.

10. Yurchenko was informed by a high K.G.B. official that the information learned from the Walker/Whitworth operation would have been "devastating" to the United States in time of war.

Dated: August 26, 1986.

JOHN L. MARTIN,
Chief, Internal Security Section, Criminal Division.

Page 530 of 3957

APPENDIX B

[From the Defense Security Institute Security Awareness Bulletin, August 1984]

PARTNERS IN ESPIONAGE

THE CASE OF JAMES HARPER AND RUBY LOUISE SCHULER

An American named "Jimmo" sporting an Irish Brotherhood medallion meets a Polish intelligence agent called "Jacques" at the Museum of Anthropology in Mexico City—such is the international, and distinctly bizarre, flavor of the latest espionage case to hit the Defense Industrial Security Program.

This is the case of James Durward Harper who was sentenced to life in prison, with a recommendation that he never be paroled, on May 14, 1984. He had pleaded guilty in April to selling classified documents to the Polish Intelligence Service. The material, classified up to Secret, pertained to survivability of the Minuteman missile system and to U.S. defenses against attack by ballistic missiles.

Harper was a self-employed electronics engineer in Mountain View, California. He first became involved with the Poles in 1975 when a business associate, William Bell Hugle, introduced him to Polish agents seeking U.S. electronics technology.

Harper was at that time running a small firm, which made and marketed the world's first digital stopwatches. He sold technologi-

cal information to the Poles for several thousand dollars. During this period, Harper did not hold a security clearance and had no direct access to classified information.

But in May 1979 Harper began what appears to have been a sort of "business-romance" with a woman named Ruby Louise Schuler. She held a Secret clearance as executive secretary to the president of Systems Control Inc., (SCI) in Palo Alto, California, a Defense contractor doing research for the U.S. Army Ballistic Missile Defense Advance Technology Center, Huntsville, Alabama. Schuler agreed to provide documents to be copied and sold. Harper contacted Hugle who, in return for a share of the proceeds, arranged a meeting with Polish Intelligence in Warsaw.

Harper conducted a total of a dozen meetings with Polish agents in Warsaw, Vienna and various locations in Mexico betwen July 1979 and November 1981. He received approximately $250,000 for documents whose loss has been rated by Army experts as "beyond calculation."

Harper and Schuler were married in October 1980. She died in June 1983 from complications of cirrhosis of the liver.

James Harper was ultimately arrested in October 1983, partly on the basis of information from a source within the Polish Intelligence Service. But his apprehension was also partly due to his own futile efforts to negotiate immunity and and a double-agent role for himself through anonymous contacts with the CIA and the FBI. Shortly after his arrest numerous classified documents were recovered from a safe deposit box in his name in a bank in Tijuana, Mexico.

The case against Harper has now been completed with his sentencing and incarceration. But certain aspects of this investigation remain active. Some details have not yet been released, and of course some never will be.

This account is based primarily upon court papers pertaining to the prosecution of Harper, especially affidavits and testimony by the FBI investigators. We have also drawn upon a follow-on inspection of the cleared facility by the Defense Investigative Service.

The most detailed account of Harper's activities was provided by prosecution testimony at a pre-sentencing hearing on April 16, 1984. This hearing did not receive extensive coverage in the press, although more limited information available at the time of Harper's arrest last October was widely reported.

As additional information becomes available on the case, we will provide follow-up articles in future *Bulletin* issues.

HIGH STAKES HAGGLING

Accompanied by his friend Mr. Hugle, James Harper sat down on July 17, 1979 in Warsaw across the table from Zdzislaw Przychodzien, known publicly as an official of Polish Ministry of Machine Industry but in fact a lieutenant colonel in the Polish Intelligence Service and head of an intelligence section or "Wydzial" using the Ministry as cover for collection operations against the West. Przychodzien was fluent in English, having been assigned to the U.S. in the 1970's with the Polish Commercial Office in New York.

Page 533 of 3957

Harper described the materials now accessible to him through Louise Schuler at Systems Control, including classified documents pertaining to U.S. strategic forces and ballistic missile defenses. And he provided reproduced excerpts of ten documents. (Enroute to Warsaw he had placed copies of the full documents in a safe deposit box at the Citibank in Paris.)

Przychodzien was very interested in the material. He promised generous payment, although he demurred at the American's initial asking price of one million dollars. Also discussed at this July meeting were other materials available to Harper including computer database tapes obtainable through his contacts in Silicon Valley.

Harper and Hugle agreed to meet with Przychodzien again in Vienna the following October. On that occasion Harper delivered full copies of the ten documents which Przychodzien had previewed earlier. He also provided excerpts of additional documents.

But a disagreement arose, or rather erupted, over the matter of payment. Harper and Hugle had come down a good deal from their original demands, but they understood that $15,000 would be paid for one of the ten documents. When Przychodzien declined to pay that much Hugle started a shouting match which quickly broke up the get-together, which was taking place in a public lounge at the Hotel International.

Harper had travelled to Vienna with Louise Schuler. They left the city immediately following this incident and returned to California. Harper was naturally unsure of his position with Przychodzien.

It appeared that the Poles were not as interested in the classified Defense documents from SCI as he had originally thought, so he buried them, in an out-of-the-way location in the San Joaquin River delta near Stockton, California—just for safe-keeping in case a buyer could later be found.

SOGGY SECRETS AND GREETINGS FROM YURI

At this point Harper wanted nothing further to do with the excitable Mr. Hugle, but he was able to reestablish contact with Przychodzien through a friend in Switzerland, and he returned to Warsaw in May 1980 with the Silicon Valley database tapes and without any classified documents.

But it was the classified ballistic missile material that Przychodzien really wanted. The intelligence officer paid $10,000 for the ten documents delivered at the stormy meeting in Vienna, apologized for the misunderstanding and urged Harper to come back with all of the Defense documents he could get his hands on.

So Harper went back to the delta, dug up his "stash" and transported the additional documents to Warsaw (via Vienna and Geneva) the following month (June 1980). Harper later estimated that this second delivery of reports, some of which were classified, weighed about 100 pounds. The documents were somewhat the worse for their seven month interment on the banks of the San Joaquin River. But Przychodzien's people worked through the night of June 5 to separate the matted pages and restore the materials to decipherable condition.

Page 533 of 3957

On June 6 the documents were brought to the Soviet Embassy where a team of 20 KGB experts, flown in specially from Moscow, declared them to be genuine and extremely valuable. Harper was paid $100,000 on this occasion. A month later Przychodzien and his unit received a commendation for their efforts, directly from KGB Chairman Yuri Andropov.

JIMMO MEETS JACQUES

Harper next returned to Warsaw in September 1980, this time bringing along a document registered for the safe in his wife's office, i.e., an inventory of all documents in the SCI president's security container. The Poles selected several items for purchase and Harper delivered them during visits to Warsaw in October and November 1980, receiving $20,000 in payment.

During the November meeting with Przychodzien Harper was instructed to meet next time in Mexico City with a Polish agent whom he knew only as "Jacques." Harper himself was given the code name "Jimmo." He occasionally wore an "Irish Brotherhood" medallion, and this was to be used as a recognition device. In addition, Harper wrote a limerick on the back of the laundry slip. This was then torn in half, and Jimmo and Jacques were to confirm identities by matching the halves of the paper.

The first meeting with Jacques took place as agreed at the cashier cage of the Museum of Anthropology on December 14, 1980. Harper brought no documents, treating the occasion as a dry run to establish contact and "get the feel of the city." Jacques paid him $10,000 anyway, and at the next encounter in the same city two months later Harper brought nine Secret documents and received $60,000.

Following one more transaction with Jacques (eight classified documents and excerpts of 30 more, in return for $50,000), Harper told the agent in September 1981 that he was dissatisfied with the payments he was receiving. He brought no documents to the September meeting, in Guadalajara, and received no payment, although Jacques had brought along $30,000 for the 30 documents previewed last time in extract. It was agreed that Harper would go back to Warsaw to work out his complaints with Przychodzien directly.

This was in fact the end of Harper's active dealings with the Poles. He made a trip to Warsaw in November 1981 and spoke with Przychodzien, but he remained dissatisfied with the payments offered and no further contacts ensued.

Before going to Warsaw Harper had driven with Louise to Tijuana and placed his remaining collection of classified documents in a safe deposit box, where they remained until retrieved by the FBI, with Harper's cooperation, following his arrest.

These were actully the last documents available to Harper, since Louise lost her clearance in August 1981—not due to any suspicion of her activities but rather due to acquisition of her company by a foreign firm.

Under an arrangement approved by the Department of Defense, SCI's Defense contracts have been retained by a "spin-off" company insulated from the parent by a stock proxy agreement. The fa-

cility clearance for this subsidiary was later upgraded from Secret to Top Secret. But Ruby Schuler remained an employee for the original SCI organization, now under British ownership, and her Secret clearance was administratively terminated as a result.

She had major surgery in August 1982 and died the following June of cirrhosis of the liver. Her death certificate lists "alcoholism" as a "secondary cause" of death.

PLAYING BOTH ENDS

In September 1981, at the time he was becoming increasingly unhappy about his exchanges with the Poles, Harper contacted attorney William Dougherty requesting that Dougherty act as go-between in negotiations with the CIA and FBI. Harper wanted to arrange immunity from prosecution in exchange for information on his activities and services as a double agent. While concealing his identity from the lawyer, he provided detailed written and tape-recorded accounts of his espionage activities through Dougherty to the government. This continued for two years until Harper's ultimate arrest, although the government showed no willingness to agree to his terms.

Investigators succeeded in positively identifying him in March 1983. He was immediately placed under physical surveillance at his home in Mountain View, California, where he was at that time living with Louise. Wiretaps were also authorized and installed on their telephone.

Investigators were able to learn the location of a storage locker where Harper kept records of his activities. They also learned that he was planning overseas travel and was again in contact with the Swiss friend who had arranged earlier meetings with Przychodzien.

He was arrested on October 15, 1983, forestalling any chance that he would turn over his remaining documents.

THE KGB CONNECTION

One lesson of this case is unmistakable confirmation of the intimate ties between Warsaw Pact intelligence services and the Soviet KGB. It is clear not only that the Polish Intelligence Service works closely with the KGB, but that they in fact work for the KGB.

When Harper brought his main installment of documents to Warsaw in June 1980 the Poles spent the night putting the pages in order, but once collated the materials were immediately turned over to the Soviets for evaluation and analysis.

Harper has stated to the FBI that the tasking presented him by the Polish agents was derived from a "master shopping list" provided by the Soviets. And this has been confirmed by the Polish intelligence officer who served as a source in breaking the Harper case. U.S. investigators have not revealed the source's identity but they have testified that he was an officer of the Polish Intelligence Service at the time Harper was active, that he was a close colleague of Zdzislaw Przychodzien and that he served as liaison officer with the KGB for Przychodzien's intelligence unit. The source has confirmed that Polish agents respond directly to detailed tasking from the KGB, with military collection as a top priority.

Page 536 of 3957

The Polish source was aware of Harper's activities, although he did not know Harper's identity. Przychodzien had told him of the initial meetings with an American, fitting Harper's description, who had access to ballistic missile information.

He even recalled seeing a phone message from Hugle written on Przychodzien's desk calendar at the time of those first meetings in October 1979. This inside information confirmed the authenticity of Harper's accounts once his anonoymous statements began coming in.

SECURITY IN THE FACILITY

Information so far available does not reveal any major security deficiencies at SCI which can be identified as contributing directly to Harper's and Schuler's activities. She apparently removed the documents from the facility to be reproduced at home on a paper copier which Harper had bought for the purpose. As in most facilities, governmental or industrial, there were no searches at the exists to prevent removal of classified material.

Schuler was noted in the facility during evenings and weekends. On at least one occasion Harper was with her. But this was not a violation since he was escorted—by Schuler! Unexplained off-hours activity has often been highlighted as a possible indication of espionage, and this is another case in point.

As a result of the case the company has centralized its classified document storage at one location under direct control of the security officer (something which would obviously not be possible for a larger facility), and they have implemented tighter personnel access controls for non-working hours.

There are some indicators that certain adverse information regarding Louise Schuler was known to co-workers and company officials and was not reported. She was, first of all, an alcoholic and ultimately died of complications from that disorder. Quotations in the press indicate that co-workers were aware that she carried vodka in her purse and drank on the job. An inquiry into that issue might have revealed some indication of her illicit activities, or possibly exerted some deterrent effect.

In addition, a former employee of the company, also a cleared individual, had a close involvement with Louise during much of the period in question, and he was aware not only of her drinking but also of her unexplained income. She does not seem to have flaunted her ill-gotten gains in a public sort of way, and most co-workers would have had no occasion to notice anything out of the ordinary.

But this other employee was with her on at least one occasion when she placed a large stack of $100 bills in a safe deposit box at a local bank, and he did not report this.

THIS CRIME DIDN'T PAY

Much of what makes the Harper case an interesting story also makes it an atypical story, therefore limiting its value as a source of "lessons-learned" for future reference and edification. But it does bring to the public view a rare glimpse of the inner workings of a foreign intelligence service. And it emphasizes the clear and present danger which espionage poses to our national security.

Page 536 of 3957

The case dramatically demonstrates that our security system is inherently and perhaps inevitably vulnerable to betrayal from within. Procedures and physical barriers can keep uncleared people from direct access to classified material. But when a cleared person goes bad, our defenses have already been breached and some damage is bound to occur.

Above all, the case highlights yet again that our system rests ultimately upon the integrity of the cleared individual. We must strive to indentify and motivate that quality, however elusive.

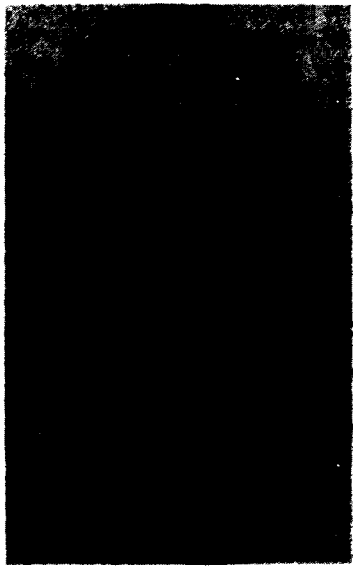
Finally, the sentence received by Harper provides a "lesson-learned" that is hard to overlook.

At the time of sentencing Judge Samuel Conti emphasized that he had "never heard the defendant say that he was sorry," and he called Harper's criminal activities "beyond comprehension or toleration." "Your actions have exposed all of our people to risk and danger," he said, "a danger that could well extend into the 21st century."

"There can be no crime more serious than that of selling our country's defense secrets to a foreign government," the Judge stated. "Your crime concerns each and every living and yet unborn citizen of this country," and it threatens "the very heart and existence of our freedom."

"It is ironic, indeed, that you pled guilty on April 15th, and that's the very day that all federal income taxes were due. It goes without saying that a great portion of the billions paid in taxes goes for national defense and yet you, for your own personal greed, would cause many of these billions to go for naught and to the advantage of a foreign power."

The judge then imposed the maximum sentence—life imprisonment, with recommendation against parole.



APPENDIX C

[From the Defense Security Institute Security Awareness Bulletin, June 1983]

CAUGHT UNAWARES: THE CASE OF WILLIAM BELL AND MARIAN ZACHARSKI

Marian Zacharski arrived in Los Angeles from Poland in late 1976. He was assigned as West Coast Branch Manager for the Polish American Machinery Company (POLAMCO), a U.S.-incorporated firm serving as marketing arm for the Polish trade agency, Metal Export.

But machinery was not Zacharski's only business. He was also covertly assigned by the Polish Intelligence Service to spot and recruit agents within California aerospace industry. And he was for a time highly successful in both his occupations. By early 1981 (at the age of 29) he had been appointed president of POLAMCO, and he had recruited at least one agent with access to important classified weapons information and technology.

Thereafter, Zacharski's fortunes took a turn for the worse, and by the end of 1981 he was serving a life sentence for espionage against the United States—but not before doing both a lot of good for Polish exports and a lot of harm to U.S. national security.

William Bell was Zacharski's agent. He was born in Seattle, Washington on May 14, 1920. He was employed an an engineer with Hughes Aircraft Company and met the Polish businessman in 1977 at the Cross Creek Apartments in Playa del Rey where both were residents. The two shared an interest in tennis as well as a common concern with the aerospace industry, where Zacharski sold much of his industrial equipment.

After almost a year of purely social and recreational contacts, Zacharski began to ask Bell for unclassified literature from work. Then he asked for "interesting" material and received first Confidential, then Secret documents to look over. He paid Bell lavishly for his minimal "consulting" work. And when Zacharski proposed that Bell, for additional thousands of dollars, photograph classified documents and carry them to Europe to meet other Polish representatives, Bell was ready to go along. Soon he felt "over his head" and too committed to back out. William Bell is now in prison, serving an eight-year sentence.

Zacharski's recruitment approach was a standard one. It should be as familiar and hence as ineffective as attempts to sell shares in the Brooklyn Bridge. But Bell's susceptibility was not the result of tender years, or slim experience or lack of education, training or intelligence. He was 57 years old when he meet Zacharski, with 25 years in Defense work, a B.S. in applied physics from UCLA and two overseas tours with his company.

Page 538 of 3957

Bell had been briefed on the threat of hostile intelligence services, but he did not recognize the classic approach when he encountered it in real life. He did not believe that it could actually be happening to him, that this amiable Polish tennis buff (who reminded him of his estranged older son) could possibly be anything other than what he appeared to be.

Bell was experienced, educated and informed—but not *aware*. We are using his story, as he has recommended that it be used, to enhance the awareness of others who may face a similar approach—and in the hope that they will respond by promptly reporting such contacts to security officials, for their own protection and for the protection of U.S. national security.

I. THE FACTS

Marian Zacharski was arrested for espionage in June 1981 and went to trial in October. He was convicted largely on the basis of William Bell's testimony against him, and Bell's lighter sentence was based in part upon consideration of his cooperation with the government in the final stages of the investigation and the trial. This account of the Bell/Zacharski espionage case is based primarily upon the transcript of Zacharski's trial. It also draws upon Bell's testimony in May 1982 before the Senate Permanent Subcommittee on Investigations.

Troubled times

In the Fall of 1977, when he was first introduced to Marian Zacharski at the swimming pool of the Cross Creek Apartments, William Bell had recently returned to Los Angeles from an assignment in Brussels as Manager of European Operations for the Radar Systems Group, Hughes International Corporation. He was now a Project Manager in the Advanced Systems Division, Radar Systems Group at the main Hughes facility in Los Angeles.

Bell held a Secret security clearance and was responsible, as he later testified, for "development and promotion of the radar fire control product line for tank vehicles." He had been with Hughes since graduation from UCLA in 1952, employed entirely at the Los Angeles facility except for two European assignments (in the mid-1960's and from 1974 to 1976).

In his Senate testimony Bell stated that these overseas assignments had been "financial nightmares" for him, "although they are touted as glamorous and lucrative." Upon his return in 1976, he recalled, he was "pursued by four separate IRS offices for back taxes on disallowed deductions primarily arising out of my overseas assignments." The year of 1976 was in fact a low point in Bell's life for a number of reasons. He was divorced from his wife after 29 years of marriage ("in an extended proceeding") and was faced with alimony payments of $200 per week. His accumulated debts forced him to file bankruptcy in July 1976. During the previous year, Bell's family had suffered a tragic loss when his 19-year-old son died in a camping accident in Mexico.

In addition to finanical hardship, divorce and personal tragedy, Bell also later recalled feeling "like an outsider" upon his return to the Los Angeles plant. "I returned from Europe to find a younger

group at Hughes and I [was] shunted off to a quiet back room." But regardless of any disappointment with his assignment, Bell was in fact given major responsibilities for development of advanced weapons systems—a fact which Marian Zacharski was quick to learn.

New beginnings

When he met Zacharski in 1977 Bell was attempting to make a new start. He had remarried ("to a young Belgian citizen," formerly his secretary overseas) and had taken up residence with her and her six-year old son at the Cross Creek Apartments. He was making a gradual financial recovery (although alimony, taxes and debts still put a strain on his $35,000 income). And he found comfort in the companionship of a close friend:

> Zacharski and his wife moved into the apartment complex and I began to play tennis [with him] on a daily basis. He slowly became my best friend. He was about the age of my oldest son who had been close to his mother and quite distant from me since our divorce.

Marian "made friends easily," Bell recalled. The two couples socialized frequently both by themselves and with an informal "little United Nations," a social group at the complex consisting of couples one or both of whom were foreign nationals. And the two men found common professional interests as well. Zacharski was a skilled and successful salesman of industrial equipment and the California aerospace industry was one of his principal sales targets. He naturally discussed the aerospace business with his tennis partner and, in about mid-1978, he asked Bell for help in making contacts at Hughes and other companies in the field.

Bell gave Zacharski's name to a purchasing manager at Hughes and also contacted people at Lockheed and Northrop. And for this Zacharski paid him approximately $5,000. At the trial, the cross-examining attorney wondered why Bell had not been suspicious of such generosity. He had been, he claimed, though evidently only temporarily. "To recieve four or five thousand dollars for doing pratically nothing made me very suspicious."

> Q: It also made you very glad, did it not, Mr. Bell?
> A: It sure did. I needed the money.

The conscientious consultant

Bell and Zacharski discussed the possibility that Bell might be permanently retained by POLAMCO as a "consulting engineer" and sales advisor, although the terms of the arrangement were left studiously indefinite ("I was working, in a way, and talked about working as a consultant for POLAMCO . . ."). Bell began, again around mid-1978, to provide printed material from the office, to help Zacharski keep abreast of sales opportunities. "It started out [with] simple things," Bell later told the Grand Jury, "like the Hughes News," the company newspaper.

Then came documents of more technical substance. He brought Zacharski copies of the Hughes "Vector," a technically-oriented publicity sheet on company programs. Zacharski had specifically requested these openly-published materials. But then Bell began to

volunteer materials in response to Zacharski's general expressions of interest. "I could tell from our conversations that they were things that he would like to see." "We would be talking about it at the tennis court—unclassified documents in the beginning."

During the summer of 1978 he provided Marian with several documents "related to items that were machined." These were unclassified, at least for the most part, but "there was possibly one confidential. . . . I'm not certain." Bell has never been sure of exactly when he first showed Zacharski a Confidential document—or just which or how many such documents he had compromised.

He may also have been uncertain in his grasp of security requirements for the handling of Confidential material, as indicated by this courtroom exchange between Bell and prosecutor Robert Brewer:

> Q: Would that [taking documents home] be a violation of . . . security policy?
>
> A: Not a confidential document no. You can bring confidential documents home. You cannot bring secret documents home.

CAWGS, LPIR and DPWS

The Secret documents which Bell compromised can be more reliably identified since the company maintained accountability records for them (not required by the *Industrial Security Manual* for Confidential). Bell determined that his first transfer of Secret material occured in October or November of 1978 when he lent Zacharski (at the tennis court) Copy No. 8 of the "Proposal for a Covert All-Weather Gun System, Executive Summary, Volume I." Bell was the author of this material. He wanted Zacharski to understand his role at Hughes and he wanted to impress him with his work. "I was proud of it," he said of the Executive Summary, "and I gave it to him." Later Bell turned over an unclassified document on the same subject and stamped it Secret "to make it look more important."

The Covert All-Weather Gun System ("CAWGS") was the primary development project under Bell's technical management at that time. It envisioned the application to tanks of the Low Probability of Intercept Radar ("LPIR") or "quiet radar." LPIR utilizes a disguised radar signal which is difficult for enemy targets to identify as radar; they are thus prevented from taking evasive action or using the radar signal for directing return fire. The CAWGS, subsequently redesignated the Dual Purpose Weapon System or "DPWS" (to be used against both aircraft and other tanks), was Bell's main responsibility throughout his relationship with Zacharski. It was, according to trial testimony, the principal program compromised by his espionage activities.

A Friend in Need

It was announced in mid-1978 that the Cross Creek Apartments would be converted to condominiums. Bell and his wife wanted to remain, but he was worried that he could not make the down payment required to purchase this unit. His friend Zacharski said he might be able to help. And in February 1979 he provided Bell with

$12,000 in two payments handed over in envelopes at the door of Bell's apartment. They were speedy and uncomplicated transactions, as Bell later testified: "Q: Did you say anything to him? A: 'Thanks.' "

He used the money for the condominium payment and for back taxes. He assumed that the money was from POLAMCO's "marketing" fund. And he credited Marian's good will with inspiring this generosity. "I thought we were good friends and I knew he would like me to stay in the apartment complex. I wanted the condominium and I accepted the money."

Foreign liaison

Bell still thought it was in connection with "consulting" activities when Zacharski suggested, in the Summer of 1979, that he travel to Europe to meet certain unidentified Polish representatives ("whom I thought would be POLAMCO people"). He was asked to photograph documents from work and bring the film with him to the meeting in Innsbruck, Austria. Marian had earlier given Bell a Canon movie camera, which turned out to have a frame-by-frame capability ideal for photographing documents. He provided a tripod and special film and instructed Bell in using the camera in his bedroom.

William Bell departed on the first of four overseas "missions" on November 26, 1979. Marian gave him about $2,500 for expenses, although Bell's wife was an airline flight attendant and his trans-Atlantic fare was $18. On the morning of November 30 he went to a pre-designated restaurant in Innsbruck and was met by a man who introduced himself as "Paul" and asked "are you a friend of Marian's?"—the agreed-upon recognition signal. The two left the restaurant and entered a car driven by another man (name not recalled) and drove to the outskirts of Innsbruck.

Bell handed over his film and the three men discussed Bell's work, the types of information he should attempt to collect and the need for secrecy and security. At one point Bell was shown a picture of his wife and son. "He [Paul] told me that I had a lovely family. Then he said that our security depended upon each other and that if anybody got out of line that he'd take care of them." The Poles did not dwell on the point, but Bell clearly perceived an "implied threat" in Paul's words. Before leaving Innsbruck, he received $7,000 and agreed to another meeting in the same city in May 1980.

Lost innocence

When he returned to Los Angeles, Bell received an additional list of desired collection targets from Zacharski. On this and other occasions he was surprised at Zacharski's highly specific knowledge of system designations and even particular document numbers.

> Q: And did you ever ask Mr. Zacharski where he obtained those numbers:
> A: Yes.
> Q: What did he say, if anything?
> A: He didn't answer me. He just smiled.

By now, at the end of 1979, Bell could no longer maintain the illusion that he was involved in a (more or less) innocent consulting arrangement with POLAMCO. It was clear, as he testified, that he was "conducting espionage" for "agents or officers of the Polish Intelligence Service." And Zacharski himself dropped any such pretense after that time. He made no more requests for assistance in promoting machine tools.

Bell took three more trips to Europe, meeting with one or both of the Polish operatives at Innsbruck in May 1980, at Linz (Austria) in October 1980 and at Geneva in April 1981. Prior to each meeting he photographed several documents with the movie camera in his apartment (when his wife was away). At the Innsbruck meetings he provided film of unclassified and Confidential documents. At Linz and Geneva he turned over copies of Secret material related to the DPWS and LPIR system. He continued to receive substantial payments, in bills and in gold, from both Zacharski and the handlers overseas.

Deja Vu

After Geneva, Bell's next meeting with the Poles was to be in Mexico City. He was uneasy about transacting his business there, he testified, in part because "Mexico City is where a spy was caught, I don't recall his name." The name, of course, was Daulton Lee, accomplice of TRW spy Christopher Boyce. But Bell was relieved of the necessity of following Lee's footsteps to Mexico. He was called to Hughes security on June 23, 1981 to be questioned by the FBI. At the trial Special Agent James Reid recalled the crucial point of the interrogation as follows:

> [REID]: I showed Mr. Bell a translation of a Polish newspaper article which indicated an individual who had been assigned to the U.N. In New York had defected to the United States Government. I then explained to Mr. Bell that this individual had in fact defected, and that he had been providing the FBI with information concerning activities of the Polish Intelligence Service in this country.
>
> Q: What if anything did Mr. Bell say?
>
> A: Mr. Bell asked, "Did he mention me?" And then without waiting for an answer, he said, "this is very serious. I would like to talk to an attorney."
>
> [Reid told Bell that he could talk with a government attorney or make a telephone call to an attorney of his own.]
>
> Q: And after you said that, what happened?
>
> A: Well, at that point Mr. Bell physically slumped in his chair and he said, "I did it. I do not need an attorney."

Bell signed a confession and agreed to cooperate in the further investigation of Zacharski. On June 28 he was fitted with a hidden recording device when he met with Marian on the apartment grounds to discuss further payments and certain sensitive programs at Hughes which Zacharski was interested in targeting. Zacharski was arrested shortly thereafter.

II. THE LESSONS

The Bell case, like any other espionage case, has its unique and peculiar elements. But it is, by and large, a "text-book" case which confirms many of the long-standing precepts of counterintelligence, as well as patterns derived from recent espionage cases.

Motive and predisposition

Financial gain was Bell's primary motivation. This is typical of most recent cases, and his testimony was quite clear on the point. Politics or ideology did not play a part:

> Q: You are not, in other words, a secret Polish patriot?
> A: No I am not.

The motivation was primarily mercenary. "Mr. Zacharski had found a fool that needed money. I had a weak spot. He took advantage of me." Bell also cited the veiled threats from "Paul." This played some part in his thinking and discouraged him from pulling out once he was involved, but "the motive was always money." ("Q: Was it worth it? A: No, absolutely not.")

Financial difficulties and other personal problems were an important cause of Bell's susceptibility to recruitment. From his trial testimony, it appears that Bell faced the kind of difficulties which everyone encounters at some time during life, although the coincidence of several misfortunes in quick succession clearly contributed to an imbalance in judgment. Withdrawal of clearances in cases like this would generally be both cruel and unuseful. But certainly whatever positive assistance or counselling an organization might provide to employees in trouble, combined with an active program of defensive security training, will help to ensure that a person like Bell is not so choice a target for a person like Zacharski.

Job dissatisfaction or some element of grudge against the company or the U.S government have figured as predisposing elements in several recent cases (Boyce, Kampiles, Edwin Moore, etc.). Bell's remarks display some signs of disgruntlement with Hughes. The European assignments were not as "glamous and lucrative" as they were "touted" to be; he felt like an "outsider" among the younger personnel at the Los Angeles plant—and so forth. But here again Bell's difficulties were of a rather ordinary sort, providing no obvious warning of an employee who was ready to take desperate measures.

Espionage indicators

Several attempts have been made in recent years to draw up a behavioral profile of the typical spy, to identify the patterns of activity which are characteristic of espionage in progress. A listing of such "warning signals" published recently by the U.S. Air Force Office of Special Investigations (AFOSI) is provided following this article (below, p. 122). Bell's is presumably one of the cases which underlies this analysis and his activities do in fact lend credence to several of the major espionage indicators. AFOSI calls these factors an "Ounce of Prevention" since early reporting of suspicious behavior may help to halt an espionage operation before irreparable damage is done.

Page 545 of 3957

Unexplained affluence is well known as a possible tip-off to ongoing espionage and certainly Bell received a substantial increase in income from his illicit activities. His estimates of the total amount varied wildely, from $70,000 to $170,000. Payments specifically cited during the trial were totalled to between $101,000 and $103,000.

Bell spent or invested most of the money, although some of the gold remained unconverted at the time of his arrest and was confiscated by the government. His testimony indicates that he was relatively conservative in his use of the funds, and even the luxury items cited—a "red Cadillac," a $2,000 necklace for his wife and a brief vacation to Rio de Janeiro—would not necessarily appear extravagant for a family with an income of $52,000 (in 1980): Bell, $40,000, his wife, $12,000). Much has been made in press coverage regarding the "young stewardess" angle in the case, but there is no indication that Bell's second wife either contributed to his financial setbacks or drove him to seek new income in support of an inflated lifestyle. (And she was not in fact an airline flight attendant when she met and married him but entered training in Janaury 1979.)

Bell's windfall earnings were directed not to high living but primarily to hastening his recovery from bankruptcy. His was a case not so much of unexplained affluence as of unexpected solvency. Any major alteration in financial circumstances may be of significance when personnel with access to classified information are involved.

Attempts to gain unauthorized access to classified information (e.g., beyond legitimate need to know) are often characteristic of diligent spies, but Bell seems to have avoided this pitfall. He was apparently a cautious (or lazy) agent and did not seek out information beyond his assigned projects. The major compromises confirmed at the trial (LPIR, DPWS) fall within the scope of his primary duties as a project manager.

Removal of classified material from the facility is a more or less inevitable accompaniment to spying, and certainly Bell took some risk in this regard. When he carried documents home to be photographed he was vulnerable to detection since Hughes had a policy of random searches at the plant exits. Either Bell was lucky in his timing or he was somehow able to anticipate the searches. In any case he was never caught in the act.

Foreign travel, on a regular basis and without sufficient explanation, is another "tell-tale sign" displayed by Bell and one which evidently contributed to his detection. His trips to Europe were partially legitimized by company business and family visits. But testimony (Bell himself and by a Hughes security official) indicates that his overseas travel—and, on one occasion, incomplete reporting of his itinerary—was a factor which helped to place him under suspicion.

Awareness: The best prevention

So Bell confirms, to some degree, certain of the behavioral patterns associated with previous cases of this kind. Financial difficulties and job-related dissatisfaction can predispose an individual to espionage. Unexplained income, unauthorized removal of documents and unexplained foreign travel may be indicators that espio-

Page 545 of 3957

nage activity is underway. But the case also confirms the difficulty of applying this sort of preventive counterintelligence to real-world situations, without the benefit of "20/20"hindsight." The real "ounce of prevention" would have involved measures to forestall Bell's recruitment in the first place. And there is good reason to think that this could have been done—with the infusion of a little more awareness.

"Who Would Expect it . . ."

This presupposes that Bell was genuinely unaware, during the initial stages, of what Zacharski was up to. A more cynical view might suppose that he knew exactly what was happening all along and complied with Zacharski's wishes, from the beginning, with his eyes wide open. But those who investigated and prosecuted Bell are inclined to accept his account of the evolution of the case. And Bell has testified that, when he returned to the state-side facility from Brussels, he assumed that his worries were over where hostile intelligence activities were concerned. "When you are sent to Europe," he told the Senate Subcommittee, "you are told to expect attempts by foreign spies, but whoever would expect it to happen here at home?

He received the required briefings and signed the required forms upon rejoining the Los Angeles organization, but apparently treated them as a matter of insignificant routine. A "Security Briefing and Termination Statement" was introduced in evidence at the trial, and he acknowledge having seen it: "I recall signing the normal form you sign when you hire into the company. . . . There are many forms you sign and I am sure that was one of them."

"Whoever would expect it to happen here at home?" It was in this innocent frame of mind that Bell initially made the acquaintance of the Polish machinery salesman and then agreed (in fact eagerly sought) to serve as a consultant for POLAMCO, an arrangement which included providing inside information on his company. The delusion persisted right up to his first overseas visit:

> Even as I went to Innsbruck, Austria, I was rationalizing and kidding myself that the persons I would meet were representatives of POLAMCO, that this was just the kind of industrial espionage that goes on all the time.

After his return from Innsbruck, Bell knew exactly what he was doing and exactly what had been done to him. Why he did not extricate himself at that point is a complex psychological question involving a confluence of material inducements, Zacharski's personal magnetism and "Paul's" implicit menace. For whatever reason, Bell now felt genuinely trapped. He told the Senators after his conviction: "There is little left of my life now but I feel I am freer in prison than I was with Zacharski."

The classic modus operandi

Clearly there was more to this entrapment than simple monetary temptation. And we must not take too literally Bell's own statement that he was "a fool that needed money." A fool he may have been and he was certainly hungry for cash. But too much

stress on Bell's foolishness can lead us to ignore Zacharski's skill. Preoccupation with financial motives, moreover, can obscure the fact that many months of cultivation *preceded* the first mention of money between Zacharski and Bell. We must not ignore the subtle but powerful psychological influences which reinforced the material incentives once offered and laid the groundwork for Bell's receptivity, by creating a willingness to regard Zacharski's offers as well-intentioned, as motivated by friendship and a good will.

Cover

Bell's recruitment was the result (not necessarily the only result) of a carefully planned and orchestrated intelligence operation. As the focal point for this operation, Zacharski was provided with the best possible cover for his activities, a cloak of propriety calculated to inspire the least possible suspicion. To begin with, his nationality was in his favor. As a citizen of an Eastern European country he would not present the same threatening image as a Soviet national—although there can be no doubt that the information he collected was to be shared with Poland's Warsaw Pact ally. (It might be recalled in this connection that during the year Zacharski arrived, 1976, a Presidential candidate had come very close to declaring Poland a member of the free world!)

In addition he was provided with a commercial rather than a diplomatic position. He was employed, in effect, by the Polish government, but as a salesman of industrial equipment he assumed an image which was less official and hence, again, less threatening. In addition, he was exempt from travel restrictions imposed upon diplomats from communist countries and had more flexibility of movement and greater access to U.S. industrial facilities and personnel. Of course commercial status carried with it a certain disadvantage: no diplomatic immunity. Zacharski is no doubt now hoping to be exchanged for someone imprisoned in the Soviet bloc, but there have been no indications that a swap is contemplated.

Once fitted with suitable camouflage, Zacharski was introduced into a promising hunting ground, the technology-rich area of Los Angeles, California. He moved into an apartment complex where many executives and engineers of aerospace companies were residents. And he set to work.

Closing in

Having met William Bell, as he must have met many others in similar professional positions, and having decided to proceed with cultivation, Zacharski worked with extreme caution and practiced subtlety. He was a skilled salesman and master persuader and well equipped for his task.

Bell testified that they first met in Autumn 1977. He could recall no requests of any kind from Zacharski until mid-1978. So Zacharski spent the better part of an entire year simply making friends with his prospect, insinuating himself into his personal life, meeting and befriending his family, assessing his character traits (and flaws), learning his likes and dislikes (and sharing them), discerning his weaknesses and above all his needs.

Only after many months of this did he *begin* seeking active assistance from Bell and overtly feeding his desire for money. Corne-

lius G. Sullivan, a former counterintelligence agent with the FBI, testified at the trial that this is a crucial "dividing line" in the process of developing an agent, the boundary between a simple social relationship and one involving overt exchange. This "barrier" is typically overcome, he said, by first requesting unclassified and seemingly innocent items—and this of course is the approach which Zacharski adopted.

There is also a second dividing line—between providing innocent, public materials and handing over restricted, sensitive and/or classified items. Zacharski used the "consulting" process to bridge the barrier between legal and illicit activities, and this was perhaps the central gambit in his very successful strategy. It was so effective in fact that Bell apparently volunteered the first transfers of classified material on his own initiative.

The "Pitch"

Offering the prospect of a consulting arrangement, as a prelude to espionage, proved successful in this case for a number of reasons. The promise of additional income appealed to Bell's financial hunger, of course. And it must also have appealed to his entirely normal professional vanity to be asked to lend his technical expertise and the benefit of his contacts in the industry. Because the arrangement was obviously improper to a degree, it introduced a surreptitious element into the Zacharski/Bell relationship and helped to ease Bell toward a fully clandestine role as a full-fledged spy. (Bell explained his additional income to his wife as coming from work for a Swiss aircraft firm. He asked her to be discreet about the arrangement, stating that Hughes would not approve of his consulting for a competitive firm.)

Perhaps above all the consulting arrangement permitted Zacharski to deceive Bell, and Bell to deceive himself, into regarding the initial compromises of national security information as a venial sort of "industrial espionage." "Within the avionics industry," Bell told the Senate Subcommittee, "it is a common practice for all companies to obtain the secrets of their competitors by the same techniques Zacharski used with me." He thought of POLAMCO as "an American company." They had offered him a job which would be "the solution to all my problems." And providing them with inside information from Hughes would only be adhering to the common practices of the industry, as he interpreted them:

> An engineer for one company is interviewed by the management of another. Considerable benefits are dangled in front of the engineer in terms of increased earnings and better position. He is asked to produce samples of his work and this is normally done without regard to security classification. . . .

Whether or not Bell accurately describes a common practice, he certainly does reflect a common attitude—"Everybody's Doing It." Zacharski exploited this attitude and used the consulting ploy to ease Bell almost imperceptibly into his intitial ventures in the illegal exchange of information. After that Bell felt that it was too late to back out, and it was indeed too late to prevent some damage to the national security, since some damage had already been done.

Thinking about espionage

"It would have been so much easier to warn me." This statement during Bell's Senate remarks does not excuse his crime—and it was not offered as exculpatory—but it may be the central lesson-learned in the case. Either he was not sufficiently warned, or he did not heed the warnings he received. Whether the blame is laid upon the system of security education or upon the individual, the damage to national security is the same. And better awareness training—drawing upon Bell's case as a cautionary example—should help to warn others similarly situated. As Bell himself put it: "Every person employed in a security job should know what I did to myself, to my loved ones and to my country and [should] realize how easy it is to get trapped."

In an article published on the anniversary of the trial, the Los Angeles *Daily News* stated the lesson of the Bell case very aptly: "When William Holden Bell worked for Hughes Corporation, he never seriously thought about espionage. But it happened anyway." Thinking seriously about espionage, about the reality of espionage, is the first requirement of security awareness. And security awareness is the key to security compliance.

III. THE BOTTOM LINE

Based upon the lesson of Bell/Zacharski, and other similar cases, awareness briefings should stress the following:

What you should know

There is potential danger in any sustained contact with a communist-country national (and not just with Soviets). You are not required to avoid all contact; just be careful.

Recruitment is a subtle, gradual process (a "long, bit-by-bit thing," Bell called it). Cultivation may last for months or years and initial active involvement may have nothing to do with espionage in any recognizable form.

Recruitment may involve no elements of blackmail or threat, so those who regard themselves as "clean-living" may nonetheless be susceptible to this sort of activity.

Positive inducements are generally more effective than threats. And such inducements will involve psychological ploys (friendship, flattery, sharing of common opinions/interests) as well as (and usually prior to) material offerings.

"Entrapment" once it comes is as much a psychological as a material entanglement, and commitment (as in Bell's case) may only be recognized after the fact.

What you should do

As a cleared contractor employee, you *must* report to the security supervisor: 1) all acts of espionage or suspected espionage, 2) any attempt to gain unauthorized access to classified information, 3) any compromise or suspected compromise of classified information, 4) plans for travel to (or through) a communist-controlled country, 5) plans to attend any professional meeting where communist-country nationals may be in attendance, 6) plans to host a facility visit by communist country nationals.

You should (for your own protection) report any contact, particularly sustained contact, with a communist-country national, even if purely personal and seemingly casual. In this way you avoid any suspicions which might arise regarding your own conduct and permit authorities to warn you if the individual is suspected of intelligence involvement.

POSSIBLE ESPIONAGE INDICATORS: "AN OUNCE OF PREVENTION"

(Source: U.S. Air Force Office of Special Investigations (AFOSI)
(Adapted from TIG Brief 18, 1982))

From an analysis of confirmed espionage cases, AFOSI has developed a listing of characteristics shared by several of the spies in varying degrees. *While no element of this list of "warning-signs" is, in itself, proof of an individual's involvement in espionage,* observation of such characteristics in the behavior of an individual with access to classified information should be a matter of concern to security and supervisory personnel. Even where espionage is not present, several of the characteristics may be indicative of problems in suitability or security which cannot be prudently ignored.

The list as presented here has been adapted to reflect the special requirements applicable to Defense contractors under the *Industrial Security Manual for Safeguarding Classified Information (ISM,* DoD 5220.22-M), as well as requirements for DIS employees.

Behavior patterns of possible significance include the following.

Attempts to expand access to classified information, through repeated volunteering for special assignments with additional access or inquiries concerning information for which the individual has no need to know.

Unauthorized removal of classified material from the work area, by making extra carbons or copies or placing of classified materials in briefcase, purses, gym bags, etc.

Repeated or unusual overtime, especially unaccompanied, whereby the individual arranges to be alone or unobserved in an office containing classified material.

Falsifying destruction records by requesting certification or witnessing signatures for destruction of classified materials which the individual has not actually seen destroyed.

Sudden, unexplained affluence as indicated by purchase of expensive cars, real estate, jewelry, etc.; by display of large amounts of cash; or by lump-sum repayments of significant debts, large stock purchases, or opening of substantial savings accounts—in the absence of some legitimate source of increased income. Unexplained affluence is of particular concern when it follows a period of leave or travel.

A pattern of recurring travel, within the United States or (especially) abroad, perhaps 2 to 4 times per year, without apparent recreational or business purpose. Married individuals who travel for tourism or recreation unaccompanied by family members may also be of concern.

Falsification of locations visited on leave statements or trip reports. Also reluctance to describe or ignorance concerning places supposedly visited.

Page 551 of 3957

Travel to Communist countries or on communist-flag ships or aircraft not involving an organized tour and not explained by business or family connections. Any attempts to visit communist countries without complying with applicable reporting requirements is of particular concern (e.g., paras. 5u and 6b[9], *ISM*).

Repeated association with Communist-country nationals without *bona fide* business purpose or without required reporting.

Note for contractors

Under the *ISM* cleared contractor employees must report anticipated contacts with communist-country nationals at professional meetings or through facility visits (para. 5u). A forthcoming change to the *ISM* (new para. 5ah, to be published in "Industrial Security Letter" no. 83L–1 and the next edition of the *ISM*) will require contractor employees to report "all questionable or suspicious contacts with nationals or representatives of communist countries," i.e., any contact "determined to consist of an actual, probable or possible hostile intelligence collection effort." Paragraph B, Appendix VII, is referenced for assistance in recognizing reportable contacts. (Para. 6c will be revised to require relaying of such reports from Security Supervisors to DIS and the FBI.)

Note of DIS employees

DIS employees, as well as all Federal employees, are required to report improper or suspicious contacts by representatives of any foreign interest, just as contractors are required to report. These naturally include contacts by communist-country nationals. See DIS Regulation 25–5.

While none of the indicators listed is proof of espionage, any pattern of conduct on the part of a cleared employee which suggests the possibility of improper activity should be reported by supervisors or managers to the Facility Security Supervisor (under para. 5af of the *ISM*). Security Supervisors should report in turn to the Defense Investigative Service and the FBI, as called for under paras. 6a(1), 6b(1) and 6c.

Where there is doubt whether information should be reported, it should be furnished to the proper authorities for evaluation. Security Supervisors should be aware that in two 1967 cases the U.S. Court of Appeals for the 4th Circuit held that a contractor is not liable for defamation of an employee because of reports made to the U.S. Government pursuant to the *Industrial Security Manual* (*Becker vs. Philco* and *Taglia vs. Philco,* 389 US 979). The Court stated in essence that such reports are privileged, since the contractor in executing the requirements of the *Manual* dons the cloak of a federal official.

Such reports do not of course constitute incrimination in themselves, and adverse action by government activities can only be taken with probable cause and due process. But the effectiveness of U.S. security and counterintelligence efforts is directly and vitally dependent upon early reporting of any possible instances of compromise or espionage.

Page 551 of 3957

APPENDIX D

[From the Defense Security Institute Security Awareness Bulletin, December 1985]

PORTRAIT OF AN UNEASY SPY—CAVANAGH CASE HIGHLIGHTS THE VALUE OF GOOD SECURITY

Thomas Cavanagh had secrets to sell. And he made no bones about his motive. "I'm after big mony," he told the prospective buyers. "Before our relationship ends, I want to be independently wealthy."

He knew that espionage was a serious crime and knew about several people who had recently been arrested and gone to jail. But in order to clear up mounting debts, and make himself rich, the Northrop engineer was willing to take some chances.

"They're real security conscious [at Northrop] and all that crap," he remarked during one meeting at the Cockatoo Motel near Los Angeles. Cavanagh thought he knew how to get around the document controls and random searches at the plant, but he was still very worried about being caught.

What he didn't know was that he had already been caught. The "KGB agents" he was meeting with at the Cockatoo and the Lucky Lodge in Commerce, California were actually FBI undercover agents.

In December 1984, after three meetings monitored and recorded by the Bureau, Cavanagh was arrested and charged with espionage.

In May 1985 he was sent to prison for life.

The Thomas Cavanagh case has some comic sidelights, but also some serious lessons for counterintelligence and industrial security. For the most part it's a success story, both for the FBI, which caught him before he could get to the Soviets and for the security program which put some real curbs on his ability to damage the nation.

Some of the lessons are plain. Above all, the case points up the importance of document accountability and reproduction control. And it suggests that exit searches can be an effective deterrent to espionage activity.

In the first part of the article we'll set the scene and tell the story of Cavanagh's encounters with FBI undercover agents, who posed as KGB officers speaking Russian and broken English. We'll listen in on their conversations as Cavanagh discusses what he's up against at the Northrop plant and how physical security and document control are cramping his style as a spy.

Less straight-forward, as always, are the implications for personnel security: adverse information reporting and the psychological "profile" of the espionage offender. Follow-up investigation concluded that Cavanagh's supervisors had not neglected their reporting responsibilities and that the reporting program at his facility

Page 552 of 3957

Page 553 of 3957

was satisfactory—although there were some hints in his behavior that might seem obvious in hindsight.

There's no question about Cavanagh's main motivation. He wanted money, first to clear up current debts, then to make himself "independently wealthy." But his conversations with the undercover agents also hint at other contributing motivations—job dissatisfaction, disgruntlement with management, social and/or political resentments.

Investigation by the FBI and Defense Investigative Service after the arrest revealed further details about Cavanagh's background and personality—for instance, a fraudulent salary claim when he first came to work at Northrop and a pattern of impatience and indifference regarding rules and procedures.

In the second half of the article we'll look into Cavanagh's background, as revealed through these interviews with former managers, supervisors and coworkers. And perhaps glean some insights into what brought him to the Cockatoo Motel on that day in December, with a classified document stuffed inside his shirt.

SOME ASPECTS OF THE CAVANAGH CASE REMAIN CLASSIFIED

We can't discuss how he was originally detected and became involved in meetings with the undercover agents, since that would compromise important investigative methods. But it's significant to note—for the benefit of other would-be spies—that someone attempting to contact the KGB can end up in touch with the FBI instead.

And we can't discuss the information which Cavanagh was trying to sell. He didn't succeed in selling it, and obviously we don't want to give any of it away for free.

Suffice it to say that he was working on a classified project requiring Special Access, and he'd been put in for Top Secret clearance requiring a Background Investigation. He told the "KGB" that a substantial down payment on his information would insure that excessive indebtedness did not interfere with the clearance upgrade leading to even more sensitive access.

At the first meeting, on December 10, 1984, Cavanagh introduced himself to his contacts as Mr. "Peters."

Two topics dominated his conversation: his financial problems and worries about getting caught.

He said early in the first meeting: "I'm up for a Top Secret clearance rating but I won't get that clearance rating because of my bill problems.

"So somehow we have to come to an agreement, ah, on money." He needed several thousand dollars, he said, "just to get the bill collectors off my back."

"Peters" was worried about being caught partly because of the recent espionage cases which he had heard about. He mentioned Bell, Boyce and "the two people in Sunnyvale" (the Harpers).

He was worred about leaks "on your end," i.e., U.S. informants inside Soviet intelligence, no doubt thinking of the informants inside Polish intelligence who helped put Bell and Harper behind bars.

See appendix C on Bell and appendix B on Harper.

Page 553 of 3957

Page 554 of 3957

And he didn't want to talk with his contacts on the telephone—"because it's constantly being bugged; they bug it with microwaves."

But his biggest source of anxiety was the security program at Northrop.

He was extremely concerned about his accountability for documents. He wouldn't turn them over to the "KGB" agents, and he wanted to get them back to the plant as quickly as possible.

"I can't give you the documents and have them back in time. They have audits. A guy just came by today and asked me how many secret documents I have." Security might open his safe and check his documents at any time.

By sheer coincidence, Cavanagh had faced a surprise audit of his classified documents on the very day of this first meeting with what he thought was the KGB.

It was strictly a random check by a company security representative—who had no suspicion that the material he was reviewing was about to be put up for sale to the Soviets. Everything was in order, but Cavanagh had been visibly upset, according to coworkers interviewed after the arrest.

"What are you messsing around with me for? I've served my time in Vietnam," he told the security officer. Cavanagh obviously thought twice about what he was doing—although he went ahead and did it. But the system of strict accountability put some important limits on his espionage activities.

Cavanagh was also hampered by reproduction controls at Northrop. "You can't run you own copies in the plant. They got that regulated too." The agents had to bring in a camera and a portable copier and make copies in the motel room.

Northrop employees were subject to random search of anything handcarried in or out of the plant. And Cavanagh was worried about that as well. "I had to stick it in my shirt and walk out with it."

He couldn't always fit things under his shirt. But he thought he could get through the exit searches without detection. The searches, he believed, were sufficiently infrequent and predictable to be successfully avoided.

Tougher and tougher and tougher

When he arrived for a second meeting on December 12, Cavanagh was greeted warmly by his friends at the motel:

> "KGB": "So, how are you today?"
>
> CAVANAGH: "Good. But a little nervous because, ah, getting the documents out is getting tougher and tougher and tougher."
>
> "KGB": "Why tougher?"
>
> CAV.: "They're real security conscious, and all that crap. Okay?"
>
> "KGB": "So you were scared?"
>
> CAV.: "Well not scared, just very careful and apprehensive. . . . Every once in a while you get somebody that's real conscientious and wants to look at everything going in and out."

Page 554 of 3957

So the "triple threat" of document accountability, reproduction controls and random searches made Cavanagh a very nervous spy—very "careful and apprehensive," as he put it. (And an "apprehensive" spy is a certain sign of good security, although in this case it fell short of total deterrence.)

Cavanagh was unable to obtain documents without signing for them (though he tried to do so, as we will see).

Making "bootleg" copies was impossible. Northrop Advanced Systems Division controls document reproduction through a system of "fully-controlled machines." In other words, no self-service. Special operators handle all copying machines, under the oversight of security. They make sure that all requirements are met for authorization, marking and accountability.

Cavanagh was also worried about the entrance and exist searches. But he felt that they presented an acceptable risk.

He didn't get the chance to test this assumption over the long run. There's no way of knowing if he could have gotten past the guards throughout the "long-term relationship" which he hoped to establish with the KGB. But he, and perhaps others, had the *perception* that the search system could be beaten. It was a threat, but not enough of a threat.

"It's cash and carry

During the second meeting (December 12) Cavanagh pressed anxiously for quick payment. "It's cash and carry cause I'm in debt up to my ears. I'm after big money."

He wanted the several thousand dollars in two days, but the "Russians" wouldn't make any promises.

> CAVANAGH: "Is it, is it possible to see money by Friday [Dec. 14].
> "KGB": "By Friday, I don't know. By Christmas. . . ."
> CAV.: "Oh God."
> "KGB": "Oh, you have very, how you say Merry Christmas. If documents are good."
> CAV.: "To be honest with you gentlemen, I need it before the 25th for security reasons [the Background Investigation]. I need that money."
> "KGB": "Okay, we do our best."

They met again on December 18. Right away, Cavanagh asked about the money. The agents had the money. And an arrest warrant.

> "KGB": "So, ah, how do you do today? Good to see you."
> CAVANAGH: "Okay, okay. Any word on the cash?"
> "KGB": "Oh we got good surprise for you today."
> CAV.: "Okay, okay. Am I gonna get it today?"
> "KGB": "Da da, yes."

Cavanagh showed them the documents he had brought along, and they struggled to make the portable copier function properly. He spoke of his financial bind. He was bitter that he couldn't get a business loan for his AMWAY distributionship, while Vietnamese immigrants, he felt, easily got money for fishing operations.

Page 556 of 3957

The agents suggested that future meetings be held outside the United States. But Cavanagh didn't want to keep his documents out that long. Besides, unexplained foreign travel might "flag" his activities with security.

Cavanagh was a gun collector and showed the agents a .45 caliber pistol he was carrying, because he was "nervous." Earlier he had warned the "Soviets" against carrying firearms ("No guns, no guns, all right, no guns.") They discussed guns and hunting. One agent took the gun to admire it, and then quietly held on to it.

A long-term relationship

After copying the documents, the agents handed Cavanagh the payment in small bills. He counted it eagerly. He wanted to have monthly meetings, he said, with substantial payment each time.

It should be worth it to them, "because billions of dollars worth of research went into those drawings. Billions!" Of course he didn't want to be "too greedy." "You know, if we play it right, it's a long-term relationship."

Cavanagh complained that bill collectors were calling him at work. "It's demeaning, degrading, cause everybody knows your business, you know?" "Of course, must be problem," one agent sympathized.

Cavanagh added: "I'm bitter because I worked hard for the company and sometimes politics plays a big role in getting ahead."

As they finished their business Cavanagh heard a noise outside. "It must be the maid, or perhaps the pipes," one agent said. "It wouldn't be bad just to look out the door," said "Peters." The agent looked out. "It is nothing."

But then a knock. The door was opened again. "FBI! Freeze, don't move!"

Cavanagh was arrested and charged with two counts of espionage. He was sentenced, on May 23, 1985, to two concurrent life terms in prison.

Postmortem

Espionage which threatens U.S. national security is never cause for celebration. But this case is, at least relatively, a success story. The F.B.I. caught Cavanagh before he reached the Soviets. And Northrop security did its job in curbing the range of his activities, through document accountability and control—and effective enforcement of need-to-know.

Particularly notable is the taming of the "Xerox" machine. Ready access to photo reproduction is popularly thought to have made document control obsolete.

But the copiers at Northrop were effectively controlled, so Cavanagh was forced to use original documents which were under accountability. This exposed him to detection through random audits, and it limited both the number of documents he could compromise and the length of time he was willing to keep them outside the plant.

Page 556 of 3957

Page 557 of 3957

Greed and indebtedness were the major motivations for Cavanagh. But there were other, more subtle, influences at work as well.

After the arrest, Cavanagh's activities, behavior and background were naturally probed in detail by both the FBI and Defense Investigative Service. We've already looked at Cavanagh's brief and very unsuccessful career as a spy.

What follows is the story of his career as a technician and engineer, with the U.S. Navy and three of the country's biggest aerospace companies. That career wasn't as successful as Cavanagh apparently thought it should have been.

Disappointment with his advancement both professionally and financially seems to have played a major role in the psychological lead-in to espionage.

Prologue

At the time of his arrest in late 1984, Cavanagh, 40 years old, was earning about $40,000 as an Engineer Specialist with the Advanced Systems Division of Northrop Corporation, Pico Rivera, California. He had begun his technical career as an Interior Communications specialist for four years in the Navy, leaving the service in 1967 as a Petty Officer Third Class. Between 1967 and 1978 he attended Cerritos Junior College, ultimately earning an Associate Degree.

He was married and had two sons, born in 1967 and 1968.

Rockwell and Hughes

He worked for North American Rockwell for about a year (July '68 to August '69) and then went to work for Hughes Aircraft Company, El Segundo, California. While at Hughes, Cavanagh was promoted from technician to "Research Associate." But he was unable to attain full status as an engineer without a four-year degree.

Records and recollections at Hughes didn't reflect anything particularly distinguished or out of the ordinary about Cavanagh. One supervisor recalled him as high-strung and temperamental but generally manageable. Another had found him likeable and easy to get along with.

But a third former boss said Cavanagh had problems dealing with people and recalled a heated argument in which he seemed on the verge of physical violence.

Cavanagh had once been formally counselled for tardiness and had been placed on a one-year probation for parking violations. His salary had been attached on three occasions, for debts of $125 or less.

He was very "money motivated," said one coworker. And he had a high opinion of his own skills and abilities. But he was unlikely to advance very far at Hughes, even apart from the lack of an engineering degree. Most coworkers assessed his professional abilities as fair-to-middling at best. His technical skills were "reasonably good," according to one supervisor. Another, more typically, rated him as a marginal electronics technician and better suited to mechanical assembly.

Cavanagh held a Secret clearance while working at Hughes.

Page 557 of 3957

Page 558 of 3957

Northrop: He hoodwinked us

In November 1981, Cavanagh made the jump to full engineer status when he joined Northrop Electronics Division in Hawthorne, Califorinia. Northrop gave him a substantial raise and the title of "Senior Engineer," on the basis of over ten year's experience as an electronics technician—and also due to Cavanagh's ability to sell himself despite a marginal record at Hughes.

But the size of the raise which Northrop gave him was based upon an inflated claim of final base pay at Hughes. Several co-workers at his former office were aware that he had presented Northrop with a pay slip reflecting substantial unitemized overtime, claiming the total amount as base salary for the pay period. Northrop Personnel Office accepted the claim, although one of Cavanagh's managers was pretty sure that he had "hood-winked us."

Cavanagh's Secret clearance was transferred from Hughes and he was assigned to work on automatic test equipment for the F-5 aircraft. At Northrop, Cavanagh generally held supervisory positions, even though here again his technical abilities were generally rated as marginal.

He had a "dynamic"—sometimes "brash"—personality, according to one coworker. His assertiveness evidently commended him to management as a potential leader, but it also led to some interpersonal problems on the job.

On his first assignment, supervising integration of test equipment for the F-5 project, Cavanagh's managers rated his engineering skills below par. One supervisor later recalled that he seemed better suited to a technician's role. He was "in over his head technically," said one coworker, but he had a "big ego" and "radiated confidence" in his own abilities.

Colleagues remembered him as a frequent complainer with a short temper. A couple of incidents had led to threatening remarks ("I'll knock her block off," and the like). Once he slammed a door into the back of a supervisor who was leaving the room after a heated exchange.

New assignment

In mid-1982 the F-5 project closed down and Cavanagh was given a less technically demanding assignment. One manager recalled that he took the downgrade in stride (there was no cut in pay), but he showed little enthusiasm for the new project. He was more "paper oriented" than the assignment required and "didn't like to get his hands dirty."

Part of his job involved computer maintenance, but he frequently called in the manufacturer's technician without really trying to fix a problem himself. Cavanagh viewed himself as a supervisor, one manager remarked, when the job really called for a "doer."

Managers and co-workers had seen no signs of major financial difficulties while Cavanagh worked in the Electronics Division. He wore good clothes and had a gun collection and two Corvettes (mid-70's vintage)—but nothing really out of line for someone making in the neighborhood of $40,000 per year. He asked for an early paycheck on a couple of occasions. During 1982 he took about $1000 as an advance on a trip to Beaverton, Oregon for a technical training

Page 558 of 3957

Page 559 of 3957

course. He apparently had trouble repaying what was due when he returned and was contacted several times by the finance office. He sometimes complained casually about owing money to unspecified creditors. But, in all, his co-workers had no reason to suspect substantial problems.

Cavanagh was separated from his wife at about this time (1982). He had no really close friends at Northrop and co-workers were unsure about the exact timing and details of his marital difficulties. But it was generally known that he had begun an affair with another woman during the trip to Oregon. After he moved out of the family house, the Beaverton woman came down to California to live with him in an apartment.

In January of 1984 Cavanagh was transferred on loan with several other engineers to an urgent and sensitive project in Northrop's Advanced Systems Division (ASD) in Pico Rivera. Cavanagh was one of the first to be chosen to go, according to one manager. Supervisors had agreed that he was more troublesome personally than he was worth technically.

Last stop

And again at ASD he ran into personal difficulties and soon had a reputation as a "chronic complainer." He had at least one heated exchange with his first supervisor, and co-workers recalled other "loud and nasty" remarks. He frequently objected that others were receiving promotions and raises while he was getting less than his due.

A subsequent supervisor at ASD recalled that Cavanagh was careless and impatient with controls and procedures and had an inflated view of his own capabilities. But this manger thought Cavanagh might respond to additional responsibility, so he placed him once again in a supervisory position, as a lead engineer—his final assignment prior to the arrest in December 1984.

ASD management personnel interviewed after the arrest suggested that Cavanagh had some problems with administration and working with others but was improving in those areas. Again his engineering skills were called into question, but he seemed to be meeting basic expectations.

In this last assignment Cavanagh seemed to be generally well-liked by co-workers and subordinates. He regularly bowled and played softball with groups from the office.

One engineer who worked for him said that Cavanagh was the "clown" of their group. Everyone had laughed when, shortly before his arrest, he asked if he could deposit $10,000 in a bank without alerting the IRS.

Financial brinksmanship

Co-workers at ASD had a general idea that Cavanagh was financially pressed. Most attributed this to his separation and divorce. One colleague recalled being mildly surprised when Cavanagh bought another car (1984 Blazer). He was upset in November 1984 about a raise which he considered inadequate. At about that time he had asked the company to pay him a $3000 referral bonus for his own employment. (They didn't.)

Page 559 of 3957

Page 560 of 3957

One colleague remembered that Cavanagh seemed to have a lot of credit cards. And a couple of people mentioned a recent two-week Club Med vacation in Mexico.

Cavanagh complained to the undercover agents that "everybody" knew his business. But in fact no one had any idea of the extent of his indebtedness.

When investigators reviewed Cavanagh's financial records, they found about 25 outstanding credit accounts, including two American Express cards (one green, one gold), two Master Card accounts and five Visa cards. In December 1984 his balance with Club Med was almost $17,000.

Overall, he owed more than $41,000, in addition to a $98,000 mortgage. He had managed to make most of his payments so far, and none of the creditors had yet taken legal action. But there were several past due notices and he clearly had more debt than he could manage for much longer.

Looking for loopholes

Several former supervisors remarked that Cavanagh often tried to "test" the system, to see how far he could bend the rules. But he generally fell into line when counselled or confronted.

This pattern held true in his handling of classified material. At the Advanced Systems Division Cavanagh regularly obtained classified documents from two control stations. The document control people at both locations remembered having trouble with him. He would often pull documents from the cabinet himself, which many employees did during busy periods.

But Cavanagh would sometimes try to walk out without signing a receipt. When challenged he would plead absent-mindedness or simply treat the process as a joke.

The control clerks learned to keep an eye on him. And they apparently succeeded in keeping tabs on his documents. All the classified items which Cavanagh handed over to the undercover agents were duly signed for—hence his anxiety to get them back to the plant as quickly as possible.

Cavanagh's attempts to disregard and dismiss security requirements are typical of an attitude which is frequently encountered, perhaps most frequently among senior executives or "technical types" who feel they have a claim to special exemption from the rules.

Security Awareness Bulletin #2-85 (December 1984) describes several cases of this kind, in an article entitled "Above the Law." These were cases of security violations which did not—so far as we know—involve actual espionage. But they still involved compromise and potential damage to national security.

Cavanagh was not allowed to circumvent the system. But his case is a reminder of just how dangerous this kind of attitude can be.

No easy answers

The "typical" spy has yet to be discovered and the behavioral profile that will let us recognize one every time has yet to be invented. The psychology of espionage is not a source of tidy conclusions.

Page 560 of 3957

Page 561 of 3957

But Cavanagh shows some traits which we've encountered before in other spy cases. Job and career dissatisfaction is a big one, especially when it involves a sense of resentment toward the organization. Financial difficulties and/or irresponsibility are old standbys. Cavanagh, in addition, showed some tendency to violent or disruptive behavior, some instances of dishonesty and a general lack of respect for authority and procedural process.

Still, none of this rose to the level where supervisors considered reporting it for security purposes. Cavanagh was not a model citizen, but his behavior was well within normal, or at least tolerable, limits—until, quite suddenly by all indications, he went over the edge and tried to sell out the country to make himself rich.

How do we distinguish the Cavanaghs, *before* the fact, from the many other cleared people who are simply having difficulties with life's normal trials and tribulations?

Unfortunately, we don't often distinguish them, until after the fact. And we can't—until and unless we know a lot more about human psychology.

But we *can* protect the documents and the information, as Northrup did, by applying the proper measures for accountability and control, as well as physical safeguards. None of that will prevent espionage. A clearance, like any other kind of trust, always carries the potential for betrayal. But controls can make spying a lot tougher and a lot more expensive and a lot more risky.

Mr. Cavanagh took the risk and lost. He'll be in prison for a long time. Others will be that much more reluctant to take the same chances.

Page 561 of 3957

APPENDIX E

UNITED STATES DISTRICT COURT, EASTERN DISTRICT OF NEW YORK AND SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

AGAINST

1. GENNADIY FEDOROVICH ZAKHAROV, DEFENDANT,

2. PREMISES KNOWN AND DESCRIBED AS THE SECOND FLOOR APARTMENT OF A TWO-FAMILY RESIDENCE LOCATED AT 6019 TYNDALL AVENUE BRONX, NEW YORK; AND

3. ONE 1982 BLUE PLYMOUTH RELIANT BEARING NEW YORK LICENSE PLATE 2281-ASJ

Affidavit for an Arrest Warrant and Search Warrant

(T. 18, U.S.C. § 794(c))

EASTERN DISTRICT OF NEW YORK, SOUTHERN DISTRICT OF NEW YORK, *ss:*

Daniel K. Sayner, being duly sworn, deposes and says that he is a Special Agent of the Federal Bureau of Investigation, duly appointed according to law and acting as such.

In or about and between April 1983, to and including the date of this affidavit, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant Gennadiy Fedorovich Zakharov (hereinafter "Zakharov") did knowingly and willfully combine, conspire and agree together with others known and unknown, to communicate, deliver, transmit and attempt to communicate, deliver and transmit to a foreign government, to wit, the Soviet Union, directly and indirectly, documents, writings, code books, instruments and other information relating to the national defense with the intent and reason to believe that it was to be used to the injury of the United States and to the advantage of a foreign nation, in violation of Title 18, United States Code, Section 794(a).

OVERT ACTS

In furtherance of the conspiracy and to effect the objects thereof, the following overt acts, among others, were committed in the Eastern District of New York and elsewhere:

1. On or about May 10, 1986, the defendant Zakharov met with a confidential source (hereinafter "CS") in Queens, New York, and entered into an agreement with "CS" whereby "CS" would be re-

Page 562 of 3957

Page 563 of 3957

quired to obtain classified information relating to the national defense for Zakharov and the Soviet Union. The defendant Zakharov made a payment to "CS" of a sum of money at this meeting.

2. On or about August 2, 1986, the defendant Zakharov met with "CS" in Queens, New York, and assigned "CS" the task of surreptitiously copying documents kept in a locked safe at "CS's" place of employment, a manufacturer of precision components for use in the engines of military aircraft and in radars, so that Zakharov could determine the importance of the information contained in the documents.

(Title 18, United States Code, Section 794(c))

Upon information and belief, there is presently concealed within the premises known and described as: (1) The second floor apartment of a two family residence located at 6019 Tyndall Avenue, Bronx, New York (hereinafter the "Premises") and (2) One 1982 blue Plymouth Reliant bearing New York license plate 2281-ASJ property; namely, 1) espionage paraphernalia including a) devices used to conceal and transmit classified and intelligence information; b) materials utilized by espionage agents to communicate among each other and with a foreign government; to wit, coded pads; secret writing paper; greeting cards and other documents containing microdots; microfiche and instructions in the use of the materials; recording and electronic transmittal equipment; and c) chemicals used to develop coded or secret messages; 2) books, records, documents and papers which reflect a) identities of foreign espionage agents; b) financial transactions including payments made to foreign espionage agents; c) telephone records reflecting contact among foreign espionage agents; 3) fingerprints of various persons who have visited or been at the Premises; and 4) other documents and paraphernalia that refer or relate to Zakharov's activities as an espionage agent. The aforedescribed property constitutes evidence of a violation of Title 18, United States Code, Section 794(c), to wit, conspiracy to transmit, deliver and communicate documents and information relating to the national defense to a foreign government with the intent or reason to believe that it is to be used to the injury of the United States and to the advantage of a foreign nation.

The source of your deponent's information and the grounds for his belief are:

1. "CS" is an individual known to your deponent to be a confidential source working for the Federal Bureau of Investigation. "CS" has provided information to your deponent for approximately the last one and one-half years regarding the defendant Zakharov's contacts with "CS" and has provided information to other agents since in or about April of 1983 regarding the defendant Zakharov's contacts. The majority of the meetings between the defendant Zakharov and "CS" described below which occurred from March of 1985 to August 2, 1986 have been tape recorded. The recordings corroborate "CS's" accounts of his meetings with Zakharov. In addition, surveillance agents of the Federal Bureau of Investigation have observed numerous meetings between Zakharov and "CS".

Page 563 of 3957

2. "CS" has informed agents of the Federal Bureau of Investigation that in April 1983, "CS" was approached by Zakharov on the campus of Queens College, New York, where "CS" was a third-year student majoring in computer sciences. Zarharov did not identify himself as a Soviet, but did tell "CS" that he worked at the United Nations doing scientific research. Zakharov requested "CS's" help in obtaining material of robotics and computer technology. Zakharov offered to pay "CS" a sum of money for "research time" necessary to obtain unclassified microfiche from local university libraries. At this first meeting Zakharov gave "CS" a list of specific microfiche relating to robotics and computers that "CS" was to obtain for Zakharaov. A second meeting was scheduled.

3. On or about May 3, 1983, a second meeting occurred between "CS" and the defendant Zakharov. During this second meeting, Zakharov identified himself as a Soviet and paid "CS" a sum of money even though "CS" had not located any material for Zakharov.

4. During the period from May 1983 to March 1985, Zakharov met with "CS" on numerous occasions, most often in Queens, New York, but also occasionally in Brooklyn, New York. In compliance with Zakharov's instructions during this period of time, "CS" would steal unclassified microfiche from various libraries and information centers and provide the microfiche to Zakharov. Zakharov continued to pay "CS" for his services.

5. As "CS's" graduation from Queens College approached in January 1985, the defendant Zakharov regularly encouraged "CS" to apply for a job with a high tech company. Zakharov paid "CS" to have professional résumés prepared to assist "CS" in obtaining such employment. Additionally, Zakharov advised "CS", in substance, that the Soviets would be willing to pay for educational expenses if "CS" wanted to go to graduate school.

6. During the period from in or about March 1985 through in or about May 1985, the defendant Zakharov discussed with "CS", among other topics, emergency meeting procedures, development of drop sites for the transfer of documents between Zakharov and "CS", and emergency signaling procedures. Zakharov further advised "CS", in substance, that he wanted to have a longterm relationship with "CS" and that "CS" should not be in this type of activity entirely for money but also to hurt America.

7. In or about September 1985, "CS" became employed at a company located in Queens, New York (hereinafter the "Company"). The Company manufactures unclassified precision components for use in military aircraft engines and in radars that are assembled by major defense contractors such as the Bendix Corporation and General Electric Corporation.

8. After "CS" began working for the Company, Zakharov's emphasis in the gathering of information shifted from seeking unclassified microfiche on technical subjects such as robotics, computers and artificial intelligence to seeking documents from the Company relating to the Company's manufacturing activities. For instance, on or about January 18, 1986, Zakharov instructed "CS" to photocopy the first few pages of the operating manuals for the machines that the Company uses to manufacture its military aircraft components. Zakharov stated to "CS", in substance, that by knowing the

Page 565 of 3957

type of machines the company uses, his "Institute" would be able to determine specifically what the Company manufactures. Zakharov also cautioned "CS" at this time that their relationship was no longer as innocent as it had been previously and that no one should know of their relationship. Your deponent believes that the "Institute" is a term that Zakharov uses to refer to his superiors in the United States and Moscow.

9. On or about March 15, 1986, the defendant Zakharov met with "CS" in Queens, New York. At this meeting, "CS" provided Zakharov with unclassified documents pertaining generally to the maintenance and manufacture of components of military aircraft engines. At this meeting, Zakharov asked "CS" if any materials at the Company to which he might have access were classified. Zakharov further discussed with "CS", in substance, whether "CS" would like to enter into an agreement with Zakharov pertaining to their clandestine relationship. At this meeting, Zakharov made payment of a sum of money to "CS".

10. On or about April 20, 1986, Zakharov met with "CS" in Queens, New York. At this meeting, Zakharov stated, in substance, that before Zakharov could make payment to "CS" for delivery of documents and information, Zakharov would first have to send the material to Moscow for their review.

11. During a meeting on May 10, 1986, which occurred on a subway platform in Queens, New York, Zakharov dicated an agreement to "CS" whereby "CS" would continue to work for the Soviets for a period of ten years, after which the agreement could be reconsidered and renegotiated. The agreement dictated by Zakharov to "CS" specifically included a provision that "CS" would be required, as part of his assignments, to obtain classified material for the Soviets which could not be obtained by a citizen of the USSR. The agreement entered into between Zakharov and "CS" further provided that the amount of payment to "CS" for his services would be based on the quality and quantity of the information provided by "CS". As Zakharov dictated the agreement, "CS" wrote it out on a piece of paper. "CS" then signed the agreement and handed it to Zakharov who retained possession of the agreement. Zakharov made a payment to "CS" of a sum of money at this meeting.

12. On or about May 31, 1986, the defendant Zakharov again met with "CS" in Queens, New York. During this meeting, Zakharov asked "CS", in substance, if any of the documents maintained in the Company's safe were stamped confidential or were restricted in any manner. Zakharov further urged caution on the part of "CS" in entering the Company's safe. Zakharov also requested that "CS" remain unmarried.

13. Shortly after this meeting, the defendant Zakharov travelled to the Soviet Unon where he remained until on or about July 20, 1986.

14. Upon Zakharov's return to the United States, he again met with "CS" in Queens, New York on or about August 2, 1986. At this meeting, Zakharov told "CS" that the "Institute" recommended that "CS" attend Queens College initially and then transfer to Brooklyn Polytechnic Insitute at a later time. Zakharov further stated, in substance, that he would pay "CS" a sum of money for graduate school plus additional expenses at their next meeting.

Page 565 of 3957

Page 566 of 3957

15. Also during this meeting of August 2, 1986, the defendant Zakharov sought more information from "CS" about "CS's" employment and, specifically, about the safe located at the Company. "CS" informed Zakharov that he had seen documents in the safe that bore the designations "(C), (U) or (O)," but that "CS" did not know what these designations meant. Zakharov instructed "CS", in substance, to attempt to copy some of the documents in the safe so Zakharov could determine if the material was important.

16. Investigation has disclosed that the defendant Zakharov currently resides at the premises and has resided there for over three years. On two occasions in 1986 on which Zakharov met with "CS", surveillance agents first observed Zakharov depart from the premises carrying a shoulder-strap gym-style bag. On both occasions, Zakharov was observed entering a 1982 blue Plymouth Reliant bearing New York license plate 2281-ASJ and driving off. On one of these occasions surveillance agents followed Zakharov and observed Zakharov drive the Plymouth Reliant to a location, park, exit the car and walk in the direction of a subway station, all the while carrying the shoulder-strap gym-style bag. On both of the occasions on which Zakharov was observed leaving the premises, Zakharov subsequently arrived at the designated meeting place carrying what appeared to be the same shoulder bag and met with "CS". Also on various occasions, Zakharov has mentioned to "CS" that he (Zakharov) has parked his car in Manhattan prior to meeting with "CS". Zakharov uses the shoulder bag to conceal documents provided to him by "CS" at their meetings. In your deponent's experience, automobiles used by espionage agents often contain counter-surveillance devices, such as scanners.

17. Investigation by agents of the FBI has determined that the defendant Zakharov is employed in the United States as a Scientific Affairs Officer assigned to the Center for Science and Technology for Development at the United Nations Secretariat in New York. He has been in the United States since in or about December 1982.

18. Your deponent has been assigned to the Foreign Counterintelligence Squad in New York City for the past two years. During this period of time, I have worked on more than a dozen cases involving Soviet and East European intelligence service operations and have therefore become thoroughly familiar with tactics, methods and operational techniques of the intelligence services of these countries. In your deponent's experience, and based on information provided to your deponent by other officials in the Foreign Counterintelligence area, Soviet and East European Intelligence agents utilize espionage paraphernalia including devices designed to conceal and transmit classified and intelligence information, materials used by espionage agents to communicate among each other and with a foreign government to wit, coded pads, secret writing paper, greeting cards and other documents containing microdots, microfiche together with instructions in the use of these materials, recording and electronic transmittal equipment, chemicals used to develop coded or secret messages; and books, records, documents and papers which reflect: a) the identities of foreign espionage agents; b) financial transactions including payments made to foreign espionage agents; and c) telephone records reflecting contact

Page 566 of 3957

Page 567 of 3957

among foreign espionage agents. It is also your deponent's experience that these materials are kept in safe houses and residences used by intelligence agents. Based upon the facts set forth above, it is your deponent's belief that the defendant Zakharov is a Soviet intelligence agent conducting espionage activities in the United States. Moreover, the investigation has established, as described above, that the premises known and described as the second floor apartment of a two-family residence located at 6019 Tyndall Avenue, Bronx, New York and one blue 1982 Plymouth Reliant bearing New York license plate 2281-ASJ are being used by an agent of Soviet Intelligence in the conduct of his espionage activities.

19. Agents of the Federal Bureau of Investigation presently plan to arrest the defendant Zakharov on Saturday, August 23, 1986, after he has received the latest batch of documents from "CS". It is anticipated that the arrest will occur on or after 4:00 p.m. on Saturday. Your deponent fears that confederates of the defendant Zakharov will be warned of the arrest when Zakharov fails to return promptly from the meeting and may attempt to destroy evidence of the conspiracy at the location to be searched. Therefore, your deponent requests that authority be given for agents to execute the warrant at any time of the day or night.

Wherefore, your deponent respectfully requests (1) that a warrant issue for the arrest of the defendant Gennadiy Fedorovich Zakharov, so that he may be dealt with according to law; (2) that a warrant issue allowing your deponent or any Special Agent of the FBI with proper assistance to enter at any time of the day or night the premises known and described as the second floor apartment of a two-family residence located at 6019 Tyndall Avenue, Bronx, New York and therein to search for property; namely, 1) espionage paraphernalia including a) devices used to conceal and transmit classified and intelligence information; b) materials utilized by espionage agents to communicate among each other and with a foreign government to wit, coded pads; secret writing paper; greeting cards and other documents containing microdots; microfiche and instructions in the use of these materials; recording and electronic transmittal equipment; c) and chemicals used to develop coded or secret messages; 2) books, records, documents and papers which reflect a) identities of foreign espionage agents; b) financial transactions including payments made to foreign espionage agents; c) telephone records reflecting contact among foreign espionage agents; 3) fingerprints of various persons who have visited or been at the apartment; and 4) other documents and paraphernalia that refer or relate to Zakharov's activities as an espionage agent.

DANIEL K. SAYNER,
Special Agent, Federal Bureau of Investigation.

Sworn to before me this 22nd day of August, 1986.
United States Magistrate, Eastern District of New York.

Page 567 of 3957

APPENDIX F

United States Information Agency
Washington D.C. 20547

USIA

April 29, 1986

Senator David Durenberger
375 RSOB
Washington, D.C. 20510

FORGERY

Dear Senator Durenberger:

Now that there is conclusive evidence that [illegible] explosion of a Chernobyl nuclear power plant reactor produced a considerable quantity of radioactive fallout, we have a chance to utilize this fact for propaganda purposes. Furthermore, it is good for us that Moscow has made no official statement on the event.

Therefore we suggest that following steps should be taken:

- Reports should be spread by our associates in European information media giving the public the details of Chernobyl disaster:

  - number of victims should be alleged to be somewhere between 2,000 and 5,000;

  - mass evacuation of population from the 100-mile zone;

  - transport problems, shortage of various goods, chaos, and panic should also be given publicity;

  - appropriate illustrations and textual material should be provided;

  - campaign should be organized by USIA officials who should also supply the material needed.

- In view of the forthcoming Tokyo summit data should be provided for the statement on the Chernobyl disaster to be issued by the seven leaders.

- Considering the facts about the increased air pollution, our allies should be recommended to stop imports of food and other commodities from Eastern bloc.

- Our allies should be influenced so as to make a request for compensation for contamination of their territory.

We will keep you informed of any future measures.

Best regards,

Herbert Romerstein

Herbert Romerstein
Senior Policy Officer
on Soviet Active Measures

(142)

United States
Information
Agency

Washington D C 20547

USIA

August 16, 1985

Dear General Schweitzer:

Enclosed is a copy of the forgery attributed to you.

We are able to draw some conclusions at this time.

1. The copy of the forgery in our possession was placed on the desk of an Italian journalist by an unknown person. It was in a plain white envelope. This method of surfacing a forgery is a well-known Soviet technique.

2. Based on information supplied by General Schweitzer, USIS Rome was able to convince the journalist that the letter was a forgery. As a result the perpetrators were compelled to use a Guatemalan "news service" known to be associated with the Cuban-Nicaraguan-backed insurgents to provide credibility to the Italian news agency that surfaced the forgery. This revealed the Cuban-Nicaraguan hand in the forgery.

3. General Schweitzer's evidence, provided to the Italian press service, was widely distributed both by them and USIA. Thus, the facts about the forgery are now well-known. Such exposes raise the cost to the forgers.

The following are preliminary findings of an unofficial but expert forensic examination of the forgery:

1. Paper: Not common in America.

2. Text: Possibly, the letterhead and the text were all printed on one machine, although it is difficult to determine from a copy. The letterhead does not appear to be "spliced" on.

3. Signature: Because the letter is a photocopy and the note provided was signed with a felt-tip pen it is difficult to say anything about the signature. However, it appears to be well executed. Lab would need several samples of the General's signature to determine such things as where he signs his name in relation to the signature bloc.

4. Comments: Based upon a cursory examination, it appears the document is an excellent forgery.

A linguistic examination of the forgery is now being done.

Lt. General Robert L. Schweitzer
Inter-American Defense Board
2600 16th St., N.W.
Washington, D.C. 20441

I am sorry that I did not get back to you earlier on this matter. We will continue to pursue this forgery and will keep you advised as we gain additional information.

Best regards,

Herbert Romerstein
Senior Policy Officer
on Soviet Active Measures

Enclosure: Letter

Page 571 of 3957

INTER-AMERICAN DEFENSE BOARD
2600 - 16th Street, N.W.
Washington, D.C. 20441

25 de febrero de 1985

Su Excelencia
Augusto Pinochet Ugarte
Presidente de la República de Chile
Cap. Gral. del Ejército
Palacio de la Moneda
Santiago

FORGERY

Estimado Sr. Presidente:

Me complace informar a Su Excelencia que la entrega a Chile del nuevo armamento solicitado será decidida en el más corto plazo. Me ha causado agrado al saber, a través del Sr.Motley, que usted ha mostrado vivo interés por ampliar nuestra cooperación en el terreno militar. Estimamos su profunda comprensión de las particularidades de la nueva situación internacional y de las iniciativas del presidente Reagan, encauzadas a fortalecer nuestra capacidad defensiva común.

Quisiera asegurar a Su Excelencia que seguirá usted contando con nuestro decidido apoyo en sus esfuerzos por fortalecer la libertad y la democracia en Chile.

Con respecto a nuestras acciones conjuntas en América Central, quisiera sugerirle la conveniencia de que las primeras unidades chilenas sean trasladadas a El Salvador y Honduras ya en marzo. Nuestros representantes en dichos países recibirán instrucciones dentro de dos semanas. Junto con su representante trataremos los demás problemas de nuestra cooperación en una de las próximas reuniones de la JID.

Con los mejores testimonios de mi más alta consideración y estima personal hacia Su Excelencia, saludo a usted

Muy atentamente,

Robert L. Schweitzer
ROBERT L. SCHWEITZER
Lieutenant General, U.S. Army
Presidente

JID SECRETO

Page 571 of 3957

APPENDIX G

DRAFT SENATE SECURITY MANUAL

FOREWORD

The United States Senate is obligated to safeguard the classified information we obtain and produce as a result of our legislative activities. To ensure that the Senate lives up to its obligations, this manual is published to establish uniform security practices within the Senate.

TABLE OF CONTENTS

	Page
SECTION I. GENERAL	146
1. Scope	146
2. Designation of Senate Office of Security	147
3. Reports	147
SECTION II. HANDLING OF CLASSIFIED INFORMATION	147
1. Policy	147
2. Classification	147
3. Marking Classified Material	148
4. Record of Classified Material	148
5. Inventory/Accounting of Classified Material	149
6. Special Requirements for Secret and Top Secret	149
7. Storage and Certification	149
8. Safeguards During Use	150
9. Transmission	150
10. Reproduction	150
11. Exemptions	151
SECTION III. PERSONNEL SECURITY	151
1. General	151
2. Clearance Standards for Senate Staff	151
3. Investigative Requirements	151
4. Consultants or Contract Personnel	152
5. Denials and Terminations of Security Clearances	152
6. Reinvestigation and Revalidation Program	152
7. Secrecy Agreements	152
8. Security Violations	153
9. Penalties for Breaches of Security	153
10. Security Education and Awareness	153
11. Termination of Security Clearances, Employment, or Extended Leave	154
12. Security Responsibilities in Personal and Committee Offices	154
13. Foreign Travel	154
14. Contact Reports	155
GLOSSARY	155

SECTION I. GENERAL

1. *Scope.* This manual establishes the requirements for safeguarding classified information to which employees of the United States Senate have access or possession. The manual is written in terms of the most common situations where the employee has access to, or possession of, classified information in the performance of assigned duties. It is the responsibility of every employee of

Page 573 of 3957

the Senate to be familiar with security requirements and to comply with them. If you have any questions regarding the proper safeguarding of classified information, or any problems relating to security matters in general, contact your office security manager for guidance and direction before you act.

2. *Designation of Senate Office of Security.* In order to insure that all Senate offices handle classifed information in a uniform and acceptable way, an Office of Senate Security has been created under the auspices of the Senate Majority Leader. The duties of the Director of the Senate Office of Security shall include the following:

a. Function as a central point within the Senate for the receipt, control, transmission, storage, and destruction of classified material.

b. Process clearance requests for personnel of the Senate.

c. Provide centralized recording and certification of clearances held by Senate personnel.

d. Administer a security awareness program, including security briefings and debriefings for the benefit of all Senate personnel.

e. Consult on security issues with Senate offices and conduct security surveys, inspections, and audits.

f. Conduct security liaison, both internal and external, on behalf of the Senate.

g. Such other duties related to personnel and document security which the Majority Leader may direct.

3. *Reports.* The Director of Security shall immediately submit in writing to the Majority Leader a report of any loss or compromise of classified material or information, or any other serious breach in Senate security procedures which merits the attention of the Majority Leader.

a. An annual report shall be provided to the Majority Leader on the number of security violations which resulted in disciplinary action being taken against Senate employees.

b. An annual report shall be provided to the Majority Leader on the number and types of clearances held by Senate employees.

SECTION II. HANDLING OF CLASSIFIED INFORMATION

1. *Policy.* Executive Order 12356 provides a uniform system for classifying, declassifying, and safeguarding national security information. This order assigns original classification authority to certain members of the Executive branch. Classified material originated by the Executive branch and under the custodial control of the Senate will be handled and safeguarded in accordance with the provisions of E.O. 12356 and this manual.

2. *Classification.* The assignment of classification involves a determination of the degree of protection certain information requires in the interest of national security. There are three categories of classified information: Top Secret, Secret, and Confidential. Classification of material may be supplemented by special designations and access requirements. Definitions of classification designations and other supplemental access designations may be found in the glossary of this manual.

Page 573 of 3957

3. *Marking Classified Material.* The originator of material which contains classified material is responsible for properly marking the security classification of the material. Classification designation by conspicuously marking serves to warn the holder what degree of protection is required for that information or material. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all classified material be marked in such a manner that it is clear to the holder what level of classification is assigned to the material. Although not required by this manual, those who originate material which contains classified information are urged to classify individual paragraphs within a document if deemed necessary.

a. The markings shown in paragraphs (1) through (4) below are required for all classified information. Some material, such as documents, letters, and reports can be marked easily with the appropriate markings. Marking other materials, such as ADP media and slides, will be more difficult due to size or other physical characteristics. Since the purpose of the markings is to warn the holder that the information requires special protection, it is necessary that all classified material be marked with the appropriate markings to the fullest extent possible to ensure it is afforded the necessary safeguards.

(1) *Identification Markings.* All classified material shall be marked to show the office responsible for its preparation, and the date of preparation. These markings are required on the face of all classified documents.

(2) *Overall Markings.* The overall classification of a document, or any copy or reproduction thereof, shall be stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), and on the outside of the back cover (if any).

(3) *Page Markings.* Interior pages of classified documents shall be stamped at the top and bottom with the highest classification of the information appearing thereon, or with the overall classification of the document.

(4) *Additional Markings.* In addition to the markings specified above, classified material shall be marked, if applicable, with one or more notations which indicate the material is further restricted to special access categories (e.g., Restricted Data notation and Dissemination and Reproduction notices).

4. *Record of Classified Material.* a. *Accountability Records.* The security manager of each Senate office shall maintain an accountability record of all Top Secret and Secret material, and special access materials regardless of classification. The record shall include all such classified material received or produced by, or in the custody of, the office and shall reflect as a minimum:

(1) The date of receipt.
(2) The classification of the material.
(3) The office which originated the material.
(4) The Senate Office of Security or Committee control number.
(5) A brief unclassified description of the material.
(6) The disposition of the material and date thereof (e.g., file location, or return to the Senate Office of Security).

5. *Inventory/Accounting of Classified Material.* When directed by the Director of Security (approximately on a semi-annual basis), each Senate office shall make an inventory and accounting of all Top Secret and Secret material, and special access materials, and shall submit a report to the Director of Security. The inventory and accounting shall consist of the actual sighting of each item listed in the accountability records. The report of each office's holdings will then be checked against the records of the Office of Security to insure proper disposition has been made for all accountable classified holdings.

a. *Receipt of Classified Material.* As a matter of practice, all classified material destined for Members' offices should be received by the Senate Office of Security. In the event classified material is received by a Member's office directly, it should be taken to the Office of Security within one working day to be properly receipted for and brought under Senate control procedures.

b. *Production of Classified Material.* When an office produces Top Secret or Secret material, and special access materials, such documents must be registered with the Office of Security within one working day.

c. *Semi-Annual Review of Classified Material.* For the purpose of reducing to a minimum the quantity of classified material on hand at any given time, each Senate office shall establish a program for the semi-annual review of classified material. All Senate offices wishing to dispose of classified information or place it in long-term storage may forward it to the Office of Security (using proper receipting procedures) who will assume responsibility for the proper storage or destruction of same.

6. *Special Requirements for Secret and Top Secret.* It is essential that an up-to-date record be maintained of all persons who are afforded access to Secret and Top Secret information. A record shall be maintained with each item of Secret and Top Secret material that shows the names of all individuals given access to the item and the date (or inclusive dates) on which access by each individual occurred. Such record shall be retained in the Office of Security for a period of three years from the date the material was destroyed, dispatched outside the Senate, declassified, or downgraded to less than Secret.

7. *Storage and Certification.* Classified material must never be left unattended. It must be secured in an approved storage container or under direct surveillance of an authorized person at all times. Senate offices will not be eligible to receive or store classified material until they have been certified by the Director of Security as having adequate storage capability. Classified material, when not in actual use, shall be stored as follows:

a. *Top Secret and Special Access—Cabinets and Vaults.* Top Secret and Special Access material shall be stored in a General Services Administration (GSA) approved security filing cabinet bearing a GSA Test Certification label or in a Class A vault constructed in accordance with the requirements of the Department of Defense Industrial Security Manual.

(1) Entry to the room in which the container or vault is located shall be controlled by a properly cleared employee so as

to control admittance to the room during normal working hours.

(2) During non-duty hours the room in which the container or vault is located shall be patrolled and each container or vault inspected by a Capitol Police Officer at least once during each four-hour period. The inspection procedure will be supervised by a system which provides a written record of the coverage.

b. *Secret and Confidential Cabinets.* Secret and Confidential material may be stored in a Top Secret cabinet or vault, or in a steel file cabinet secured by a steel bar and the three-position changeable combination padlock.

c. *Supervision of Storage Containers.* Only a minimum number of authorized persons shall possess the combinations to the storage containers or vaults, or have access to the information stored therein. To facilitate investigation of a container found open and unattended, a record shall be maintained by the Office of Security of the names, home phone numbers, and addresses of persons having knowledge of the combination. In addition, the combinations of storage containers in Members' offices shall be maintained, in a sealed envelope, by the Office of Security. Such envelope may be opened only at the direction of the Member or the office security manager. Cabinets and vaults in which classified information is stored shall be kept locked when not under the direct supervision of an authorized person entrusted with the combination or the contents.

d. *Alternate Storage Location.* The Office of Security shall maintain a list of all approved classified storage cabinets and vaults within the Senate. Each cabinet or vault listed shall be identified by location. In the event a cabinet or vault become damaged or inoperable in a Senate office, the Office of Security will provide temporary secure storage until such time the cabinet or vault is restored to good repair.

8. *Safeguards During Use.* Classified information is provided to a properly cleared person on the basis of a need-to-know. Determination of a need-to-know is an individual responsibility. Before divulging any classified information, Senate employees shall make certain of the recipient's identity, level of clearance, and need-to-know. The Office of Security will maintain a list of Senate employees whose level of clearance has been properly established. Classified materials, when not safeguarded as provided for in paragraphs 7a and 7b, and when in actual use by cleared personnel, shall be protected as follows:

a. Kept under the constant surveillance of an authorized person, who is in a physical position to exercise direct security controls over the material.

b. Covered, turned face down, placed in storage containers, or otherwise protected, when unauthorized persons are present.

c. Returned to storage containers as soon as practical after use.

9. *Transmission.* Transmission of classified material from Senate offices to any other Senate office, government agency, or other authorized recipients shall be registered with the Office of Security.

10. *Reproduction.* All reproductions of classified material shall be marked or stamped with the same classification as the original. Re-

production of classified material shall be made only on equipment specifically designated by the Director of Security for the reproduction of classified material. The Senate office which reproduces classified material is responsible for immediately bringing all copies under proper accountability controls and notifying the Office of Security of the particulars as provided for a paragraph 4, "Record of Classified Material."

11. *Exemptions.* Those Senate Committees which have custodial control over large amounts of classified material may be exempted from the provisions of Section II of this manual after the Director of Security has certified their policies and procedures for handling classified information fully meet the standards of this manual.

SECTION III. PERSONNEL SECURITY

1. *General.* A security clearance represents formalization of a determination that an individual is authorized access, on a "need-to-know" basis, to a specific level of classified information. Requests for clearance originate with and are validated by Members themselves (in the case of personal staffs), or, in the case of Senate Committee staffs, a determination by Committee or Subcommittee Chairmen and/or Ranking Minority Members, as specified in the Rules of each Committee.

2. *Clearance Standards for Senate Staff.* The criteria for security clearances require that nominees be individuals:

a. of excellent character, discretion, trustworthiness, and loyalty to the United States;

b. who are citizens of the United States.

3. *Investigative Requirements.* To ensure that personnel meet the criteria cited in paragraph 2 above, the following investigative coverage will be accomplished prior to granting a security clearance:

a. *Confidential and Secret.* A clearance for access to Confidential and Secret information shall require:

(1) A National Agency Check. This consists primarily of a check of the records of the Federal Bureau of Investigation, Office of Personnel Management, Immigration and Naturalization Service, and the Defense Central Index of Investigations.

(2) A personal interview either before or as part of the investigative process.

(3) A credit check.

(4) Written inquiries to present and past employers.

(5) Consent for access to financial records.

(6) Consent for further inquiries as may be necessary as a result of any unresolved issues surfaced in the investigation.

b. *Top Secret.* A clearance for access to Top Secret information requires, in addition to the requirements for a Secret clearance, a comprehensive field investigation of the nominee's background.

c. *Special Access Approvals.* Certain types of classified information require special clearances and access approval. These clearances and approvals are granted on a rigidly controlled need-to-konw basis. Requests from Committees or Subcommittees for staff clearances to special access programs will be processed on a case-by-case basis.

4. *Consultants or Contract Personnel.* Consultants or contract personnel must meet security approval criteria consistent with the sensitivity of assigned duties. Depending upon the proposed use of the individuals, specific investigative requirements will be established by the Director of Security at the time the request for security approval is submitted. In all instances, access to classified information will be limited to that needed in the performance of duty, as specified in the security approval. Any proposed change in the utilization of the individual requires submission of a request that a new security approval be granted.

5. *Denials and Terminations of Security Clearances.*

a. *Denial of Security Clearance.* If, after receipt of an investigative report, the Director of Security judges that a clearance should not be granted, the case will be discussed with the Member who requested the clearance. If the Member concurs, a denial is issued. If the Member does not agree with the assessment of the Director of Security, the matter will be reported to the Senate Majority or Minority Leader, depending on the requesting Member's party affiliation.

b. *Termination of Security Clearance.* The Director of Security will terminate staff security clearances of an individual if:

(1) the sponsoring Member requests such termination;

(2) the employee terminates employment with the Senate;

(3) the employee has committed security violation(s) of such severity as to warrant termination of clearances. If the sponsoring Member does not agree with the termination of a staff member's clearance, the matter will be reported to the Senate Majority or Minority Leader, depending on the Member's party affiliation.

6. *Reinvestigation and Revalidation Program.*

a. *Revalidation.* In order to maintain the number of Senate staff having access to classified information at a minimum, the Director of Security will revalidate the need for staff clearances on an annual basis with the sponsoring Member.

b. *Reinvestigation.* For those Senate employees holding security clearances and approvals, a reinvestigation will be conducted at least every five years. The Director of Security shall maintain a control system to insure such reinvestigations on staff members are accomplished.

c. *Requested Reinvestigation.* The Director of Security will also initiate a reinvestigation of a Senate employee at the request of the sponsoring Member.

7. *Secrecy Agreements.* A secrecy agreement must be executed by all Senate employees who are granted security clearances. The agreement will contain provisions that prohibit the signer from divulging or releasing classified information to unauthorized individuals. Where appropriate, the employee will be required to submit to the Executive branch, through the Director of Security, for prepublication review all writings, scripts, or outlines of oral presentations intended for non-Senate publication, which may contain material or information which the employee is pledged not to disclose by the terms of the secrecy agreement.

Page 579 of 3957

8. *Security Violations.* All security violations or alleged violations within the Senate will be investigated by the Director of Security. The formal investigation report will include:

a. A finding on whether a probable disclosure for classified information occurred.

b. A written report of those interviewed.

c. A finding as to the person(s) responsible.

d. A statement as to the degree of compromise involved.

e. The security violation history of each person found responsible.

f. Recommendations for remedial action to preclude recurrence of such violation(s).

9. *Penalties for Breaches of Security.* Senate employees who fail to observe security policies and procedures or who are found to be responsible for security violations are subject to the following administrative actions. These penalties are for inadvertent security violations that concern failure to properly secure classified information and do not involve either intent or gross negligence.

a. *First Violation.* Written notice by the Director of Security or the sponsoring Member and warning of possible consequences of further violations.

b. *Second Violation.* Written reprimand by the Director of Security or the sponsoring Member and warning of the possible consequences of subsequent violations.

c. *Third Violation.* Suspension without pay for a period of five days and a written warning from the Director of Security or the sponsoring Member as to the consequences of a fourth violation.

d. *Fourth Violation.* Suspension without pay for ten days and a complete review of the individual's security file by the Director of Security who will provide the sponsoring Member with the recommendation for a more severe penalty, if warranted. Such recommendation may involve a longer period of suspension without pay and/or result in termination of clearances or Senate employment. Where the recommended penalty is termination of clearances or employment, and the sponsoring Member does not agree, the matter will be reported to the Senate Majority or Minority Leader, depending on the Member's party affiliation.

e. *Two-Year Provision.* In the case of a Senate employee who has served two continuous years without a security violation of the nature set forth above, any violations that he or she committed prior to the commencement of the two-year period will be disregarded for purposes of determining whether a violation is the first, second, third, or fourth.

10. *Security Education and Awareness.* The Director of Security has overall responsibility for the security education program. The Director of Security will ensure that before the granting of a security clearance, Senate employees are briefed on the provisions of this manual as well as other pertinent security instructions. The security briefing and indoctrination will, at a minimum, include the following:

a. The employee shall read the espionage laws concerning disclosure of information relating to the national defense. The briefer will ascertain that the individual understands the espi-

Page 579 of 3957

Page 580 of 3957

onage laws and will clarify and emphasize responsibilities and consequences under the law if the statutes are violated.

b. The employee must attend a security education class prior to initial access and periodically thereafter. A mandatory requirement for the initial security education class will be the requirement for Senate employees to immediately report such contacts as explained in paragraph 14 of section III of this Security Manual.

c. The employee is required, as a condition of holding a security clearance, to sign a Secrecy Agreement with the understanding that termination of employment or such clearance does not relieve the individual of any obligations in the agreement concerning unauthorized disclosures of classified information.

11. *Termination of Security Clearances, Employment, or Extended Leave.* Those Senate employees whose security clearances have been revoked, whose employment has been terminated, or who are taking extended leave for a period of 60 days or more will:

a. Surrender before departure all classified documents or materials over which the Senate has custodial control.

b. Again read and be rebriefed on the espionage laws.

c. Be reminded that the Secrecy Agreement executed upon being granted a security clearance continues to be valid and that termination of employment or clearances does not release the individual from the conditions of the Secrecy Agreement. As a reminder of their continuing obligations, employees will be given a copy of their Secrecy Agreement upon separation.

12. *Security Responsibilities in Personal and Committee Offices.* A high level of security consciousness and good security practice is a basic responsibility of every person holding a security clearance. To achieve and maintain a strong security posture, a Security Manager will be designated for each Member's personal office and in all other Senate offices which receive or store classified information. Under the administrative guidance of the Director of Security, each office security manager will be responsible for the following duties:

a. Providing security advice and guidance to office personnel.

b. Serving as focal points within their offices for security matters.

c. Promoting general security awareness within their offices.

d. Monitoring office procedures for proper control and storage of classified material.

e. When directed by the Director of the Senate Office of Security, conduct an inventory of all Secret and Top Secret, and special access materials held within their office.

f. Retain a record of personnel within their offices who hold security clearances and who travel abroad. This report shall be maintained in a manner to be furnished by the Director of Security.

13. *Foreign Travel.* During foreign travel, Senate personnel are more accessible to foreign intelligence services. To minimize the threat to the individual or to classsified information, the Director of Security will establish procedures to provide for defensive briefings for persons planning private or official travel to designated

Page 580 of 3957

Page 581 of 3957

foreign countries. All Senate employees who hold clearances will, as a matter of routine, contact the Office of Security to arrange for a defensive briefing. Such will be provided if deemed necessary by the Director of Security. Since any traveler might become involved in an act of terrorism, hijacking, or piracy, guidance on what to expect and how to behave in such situations will also be made available to Members and Senate employees contemplating travel.

14. *Contact Reports.* All Senate personnel shall immediately report any contact with a foreign national of any nationality, either within or outside the scope of the employee's official activities, in which:

a. Illegal or unauthorized access is sought to classified information; or

b. The employee is concerned that he or she may be the target of an attempted exploitation by a foreign entity.

In addition, all cleared Senate personnel shall immediately report any contact, either within or outside the scope of the employee's official activities, with an official or representative of a governmental or commercial entity of the following communist countries: Albania, Bulgaria, Cuba, Czechoslovakia, German Democratic Republic, Hungary, Kampuchea, Laos, Mongolian People's Republic, Nicaragua, North Korea, People's Republic of China, Poland, Romania, Socialist Republic of Vietnam, Soviet Union.

Uncleared Senate personnel are also encouraged to report such contracts. Reports shall be made to the Director of Security who shall advise the FBI of the fact of the contact, unless the sponsoring Member or office security manager determines that the FBI should be informed directly.

Glossary

ACCESS—The ability and opportunity to obtain knowledge of classified information. An individual may be able to obtain classified information by being in a place where such information is kept, provided the security measures in effect do not prevent him from doing so.

AUTHORIZED PERSON—An individual who has established: (1) a need for access to, knowledge of, or possession of classified information, and (2) holds proper clearance to receive classified information. It is the responsibility of the person having control of the classified information to determine that the requester of the information has: (1) a need-to-know the material, and (2) clearance to receive it. (See also "Need-to-Know.")

CLASSIFICATION—The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

CLASSIFIED INFORMATION—Official information, including foreign classified information, that has been determined, pursuant to statute or executive order, to require protection in the interests of national security.

CLASSIFY—To assign information to one of the three classified categories (Confidential, Secret, or Top Secret) after determination that the information requires protection in the interests of national security.

COMPROMISE—The known or suspected exposure of classified information to an unauthorized person.

CONFIDENTIAL—The designation applied to information or material the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

COURIER—Any cleared individual who has been authorized in writing to hand-carry classified material. Couriers are of two types: (1) those who carry material in connection with a specific trip and task to be accomplished, and (2) those who carry material as a regular part of their work assignment.

Page 581 of 3957

DERIVATIVE CLASSIFICATION—Classification based on or derivied from previous, officially classified material or prescribed in a security classification guide.

DOCUMENT—Any recorded information regardless of its physicial form or characteristics, including, without limitation, written or printed material, data processing disks, cards, and tapes; maps; charts; paintings; drawings; engravings; sketches; working notes and papers; reproductions of such things by any means of process; and sound, voice, or electronic recordings in any form.

FORMERLY RESTRICTED DATA—Data that have been removed from the Restricted Data category upon determination, jointly by the Department of Defense and the Department of Energy, that such data relate primarily to the military use of atomic weapons and that can be adequately safeguarded as classified defense information.

INDUSTRIAL SECURITY—That portion of national security concerned with the protection of classified information in the possession of industrial contractors to the Department of Defense or other user agencies.

MATERIAL—Any document, product, or substance on or in which information may be recorded or embodied.

NEED-TO-KNOW—A determination that a prospective recipient of classified information, in the interests of national security, has a clearance and a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract approved by a user agency.

OFFICIAL INFORMATION—Information that is owned by, produced by, or is subject to the control of the United States Government.

ORIGINAL CLASSIFICATION—An initial determination that information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure. Such classification is not based on or derived from any previously classified material.

PUBLIC DISCLOSURE—The passing of information and/or material to any member of the public in any manner.

REPRODUCTION—The term reproduction, as used in this manual, means copying, duplicating, photographing, or otherwise making a facsimile, replica, or counterpart of an original article, regardless of the means used to copy or reproduce.

RESTRICTED DATA—All data (information) covering: (1) the design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but not to include data declassified or removed from Restricted Data category pursuant to the provisions of the Atomic Energy Act of 1954.

SECRET—The designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

SENSITIVE COMPARTMENTED INFORMATION—All information and materials requiring special controls indicating restricted handling within present and future intelligence collection programs and their end products. These special controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs.

SPECIAL ACCESS PROGRAM—Any program imposing need-to-know or access controls beyond those normally prescribed for access to Confidential, Secret, or Top Secret information.

TOP SECRET—The designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

WASTE, CLASSIFIED—Preliminary drafts, carbon sheets, carbon ribbons, stencils, handwritten notes, backing sheets, stenographic notes, worksheets, and similar items containing classified information. Pending destruction, classified waste must be marked and safeguarded according to its classification.

O

Page 582 of 3957

Return to
Michael Deutsch
343 S. Dearborn #1607

COUNTER-INTELLIGENCE:

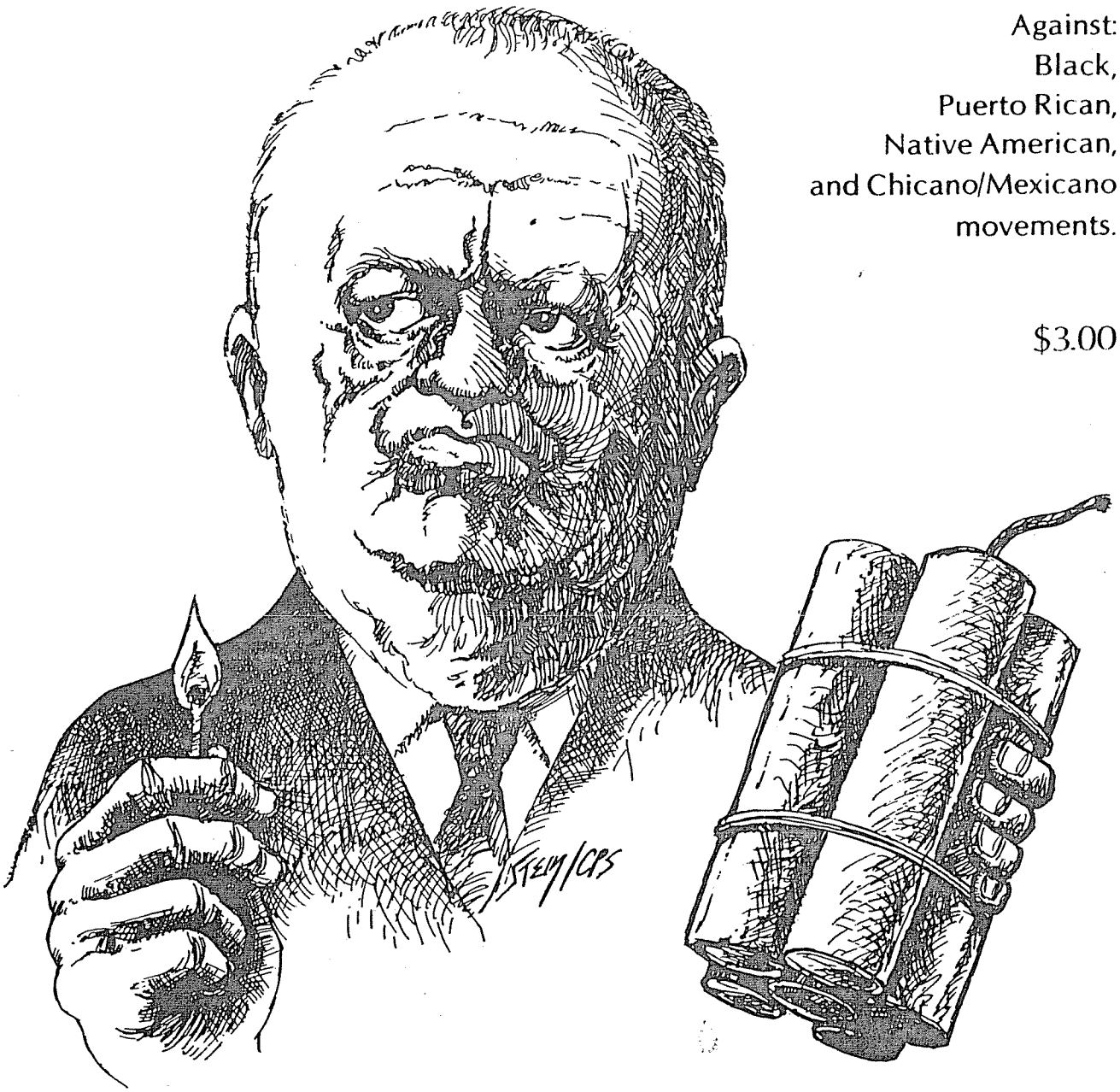
A Documentary Look at America's Secret Police

NLG

Volume One
revised and expanded

The FBI's Counterintelligence Operations Against: Black, Puerto Rican, Native American, and Chicano/Mexicano movements.

$3.00



Introduction

This collection of FBI documents and newspaper stories is designed as a resource and educational tool for lawyers and lay persons alike. Having spent the last few years studying and litigating against the FBI and its counterintelligence programs, we publish this collection in order to share our knowledge with those engaged in similar political and legal work.

We feel this publication is an important part of the task we set out for ourselves when we started the Task Force on Counterintelligence and the Secret Police at the National Lawyers Guild meeting in February 1978. At that time we decided to exchange information with and aid the litigation of those engaged in similar work; and to bring a political understanding and analysis to both the information collected and the work done which is consistent with the realities as we see them - an analysis which emphasizes that the repressive counterintelligence programs of the FBI and other secret police agencies were and are designed to systematically disrupt and destroy domestic Third World liberation movements and their leadership by any means necessary.

We wish to encourage others to bring this understanding to their work, and to move beyond omnibus spy suits and their attendant voluminous dossiers, and to focus on discovering and attacking past and present counterintelligence policies and tactics, with an eye toward aiding those victims of repression who are criminally charged or remain in prison as a result of these tactics. While this is a book composed primarily of documents, we do not see it as scholarly research with no other purpose than to satisfy historical curiosity; we hope it will be used as a tool by past victims of counterintelligence, and by the people who are the current targets of FBI harrassment.

We welcome your support and ideas, your criticisms, and especially your direct participation. Let's join together to hoist the secret police on their own petard!

Flint Taylor, and
Margaret Van Houten
Co-Chairs, NLG Task Force
on Counterintelligence
and the Secret Police
1/26/80

National Lawyers Guild Government Repression and Police Misconduct Committee - Counterintelligence Documentation Center - Suite 918 - 343 South Dearborn Street, Chicago, Illinois 60604

Editor's Note

This is the third edition of Counterintelligence: A Documentary Look at America's Secret Police. Since the last edition, we have collected and included in this book newly-released documents on the Republic of New Africa, American Indian Movement, former Black Panther Party leader Geronimo Pratt, and the continuing cover-up in the civil case concerning the murder of Fred Hampton and Mark Clark. While we feel the book is improved, we are by no means satisfied that we have gathered and published a definitive collection of documents. We therefore ask that those people reading this book contact us and send documents, newspaper clippings, and other materials that you feel would make our next edition more complete. We are especially interested in materials concerning the Chicano/Mexicano, Puerto Rican, and Native American movements.

To assist in the collection and dissemination of documentary materials regarding this area, the Government Repression and Police Misconduct Committee of the National Lawyers Guild has established a Counterintelligence Documentation Center in Chicago, Illinois. The Center makes available to interested persons over 20,000 pages of FBI files dealing with the New Left, Black Activists, Special Operations, and Media Program. The Center also coordinates the publication of the Police Misconduct Litigation Report newsletter, and the Public Eye Magazine, which recently merged with the Committee.

We would also like to inform our readers of two other groups who are doing significant work in the area of counterintelligence research and litigation - The National Task Force on Cointelpro Litigation and Research at P.O. Box 65, Bronx, New York 10473; and FOIA, Inc. at 36 West 44th Street, New York City 10036.

Please send any documents, synopses of files, or other materials to NLG Counterintelligence Documentation Center, Suite 918, 343 South Dearborn Street, Chicago, Illinois 60604. If you wish to be on our mailing list, please write us. For further information contact Chip Berlet, coordinator NLG/CDC at the above address or leave a message at the Chicago National Lawyers Guild (312) 939-2492.

Copyright 1980 - NLG Task Force on Counterintelligence and the Secret Police

(Ed. Note: In most cases the FBI memos are photocopies of original documents. Where reproduction was of a poor and illegible quality, we have retyped specific paragraphs, using similar type and margins. Not one word in those paragraphs has been deleted or altered. On some pages, different documents have been placed together, and are seperated by a wavy line to indicate the difference. Dashed lines indicate paragraphs have been removed for reasons of space and relevance.)

Table of Contents

PART ONE: **The Political Mission of the FBI** 1
Chicago Tribune 8/78 (FBI-KKK link in Birmingham) 4
FBI memos 1961 (FBI - local police - KKK cooperation) 4-5
FBI memo 11/15/60 (campaign against Puerto Rican groups) 6
FBI memo 8/4/60 (disrupt Puerto Rican Independence Movement) 7
FBI memo 6/12/61 (disrupt Puerto Rican Independence Movement) 8
FBI memo 1/22/69 (exacerbate Malcolm X/Nation of Islam dispute) 9
FBI memo 8/22/69 (exacerbate Malcolm X/Nation of Islam dispute) 10
Washington Star 11/19/75 (program to destroy Dr. King) 11
FBI memo 8/25/67 (neutralize and disrupt black movement) 12-14
Daily Defender 12/4/75 (destroy leadership of Dr. King 14
FBI memo 6/1/67 (have friendly columnist "expose" King-Spock) 15
Chicago Tribune 7/30/79 (manipulation of NAACP delegate election) 16
FBI memo 1959 (commendations for manipulating NAACP election) 16
FBI memo 3/4/68 (prevent rise of a "messiah," SAC directive) 17-21
FBI memo 5/15/68 (Dick Gregory: anonymous letter to Cosa Nostra) 22
FBI memo 11/25/68 (cripple B.P.P. and create dissension) 23
FBI memo 5/27/69 (attack B.P.P. breakfast program - scold SAC/S.F.) 24-27
FBI memo 12/2/70 (sabotage RNA purchase of land) 28
Chicago Daily News 12/3/75 (smear Rev. Charles Koen) 29
St. Louis Post-Dispatch 11/30/75 (smear Rev. Charles Koen) 29
FBI memo 10/23/68 (Chicago Eight trial as disruption technique) 30
FBI memo 1975 (informants as disruption technique for A.I.M.) 31
FBI memo 1/2/70 (disrupt United Farm Workers and S.D.S.) 32
Black Panther 2/4/78 (COINTELPRO in Mexico) 33
FBI memo 3/25/71 (extend COINTELPRO - effective in disruption) 34

PART TWO: **Violent Methods and Tactics** 35
New York Times 7/14/78 (FBI provocateur involved in Klan) 36
*Case Study: Black Panther Party 37-47
*FBI memo 11/29/68 (phony letter to cause vendetta between BPP/PFP) 37
*FBI memos (taking credit for causing widespread violence in BPP) 38
*FBI cartoons circulated to provoke violence between BPP and US) 39
*FBI memo 1/13/69 (Jeff Fort anonymous "hit" letter) 40-41
*Chicago Sun-Times 2/12/76 ("No Hits, No Guns, No Terror" column) 42
*FBI files - Floor plan of apartment where Fred Hampton murdered) 43
*FBI memo 12/11/69 (FBI takes credit for Hampton raid, asks bonus) 44
*Chicago Sun-Times articles on Hampton raid - 1976 45
*Articles on FBI provocateur William O'Neal 46-47
Chicago Tribune 6/27/75 (attempted assassination funded by FBI) 48
New York Times 1/11/76 (funding of right-wing terrorist group) 48

PART THREE: **Other Methods and Tactics** 49
FBI memo 5/14/70 (evaluation of Counterintelligence Program) 50-51
FBI memo 8/30/67 (phony arrests and prosecutions against RAM) 52-54
New York Times 3/13/75 (AIM informant Doug Durham) 55
FBI memo 3/16/73 (informants report excerpt - Wounded Knee) 55
FBI memo 9/16/70 (FBI lying encouraged - facts "immaterial") 56-57
FBI memos (snitch jacket implying Stokely Carmichael is agent) 58
FBI memo 12/2/68 (snitch jacket on BPP member - murder possible) 60
FBI memo 10/8/63 (FBI leaflets against Puerto Rican group) 61-62
FBI memo 10/10/68 (FBI racism and media manipulation) 63
FBI memo 5/21/69 (FBI article given to cooperative media) 64
FBI memo 3/16/73 (use of unwitting journalist as informant - AIM) 65

(Part Three: Other Methods and Tactics - continued)
*Case Study: American Indian Movement 66-72
*Article 6/26/76 (smear AIM with fabricated report) 66
*FBI memos (showing contradictory views on AIM purposes & FBI plans) 67
*FBI memo 4/24/75 (Wounded Knee assessment - call for less control) 68-69
*FBI memo 1975 (excerpt detailing information sharing) 69
*FBI memo 3/29/79 (re-assign AIM to Domestic Security section) 70
*FBI memo 1975 (assessment of AIM leader John Trudell as "eloquent") 70-71
*Public Eye article on arson deaths of family of John Trudell 71
*Chicago Tribune 3/14/75 (Senate probe asked into informant) 72
*FBI memo 6/27/75 (Senate probe dropped after FBI violence) 72
*Case Study: Republic of New Africa 73-77
*FBI memo 5/8/69 (phony meeting notices to cause disruption) 73
*FBI memo 3/11/71 (RNA rejuvenation prompts counterintelligence) 74
*FBI memo 8/17/70 (RNA conference disrupted through media plant) 75
*FBI memo 7/12/73 (Jackson SAC urges Obedele conspiracy prosecution) 76-77
*FBI memo 1976 (FBI says RNA actions not pre-planned or conspiracy) 77
*Case Study: Geronimo Pratt 78-82
*Letter from Rep. McCloskey proving FBI cover-up 78-81
*FBI memo 1/28/70 (counterintelligence against Pratt called for) 81
*FBI memo 1970 (phony leaflet mentioning Pratt) 82

PART FOUR: **Deception and Cover-Up** 83
FBI memo 1/9/70 and others (hiding role of FBI in disruptions) 85
FBI memo 8/9/68 (careful to disguise FBI-authored letter) 86
Washington Post 4/25/75 (Black Bag Jobs - Do Not File file) 87
FBI memo 7/19/66 (Sullivan memo on Black Bag Job procedures) 88-89
Chicago Sun-Times articles on evidence destruction by FBI 90
Articles on witholding of files and cover-up) 91
*Case Study: Panther Case cover-up 92-99
*Articles on files withheld by FBI and attorneys 92
*Articles on judge's actions in Panther case 93
*Article revealing secret communications between judge and Justice 94
*Excerpts from Judge's letters to Attorney General and investigator 95-96
*Article revealing Appeals Court Judge formerly with FBI 97-98
*Excerpts from material calling for defense of FBI 98-99
Use of judges in cover-up and counterintelligence 100-101
Chicago Tribune 4/28/78 (suppression of FBI burglary probe) 102
Seven Days 5/7/78 (shooting of William Sullivan) 103
FBI memo 7/15/64 (Counterintelligence as basic FBI policy) 104

Part One: The Political Mission of the FBI

The history of FBI counterintelligence and repression against the Black liberation movement began with the establishment of the Bureau itself, in 1919. In October of that year, J. Edgar Hoover, fresh from his exploits as Attorney General Palmer's "legal advisor" for the notorious Palmer raids, initiated a campaign against Marcus Garvey which resulted in his frameup on false fraud charges, and ultimately in his deportation as an "undesirable alien". Counter-intelligence tactics were employed against other Black leaders and spokespersons, such as Paul Robeson and Richard Wright, and may have been involved in Wright's mysterious death in Paris. As Blacks became active in the Communist Party, the FBI moved to destroy racial unity and play on racism within the Party. The Bureau further developed this technique in an extensive campaign to discredit the black Party leader Claude Lightfoot in the 1950's.

In the late 1950's and early 1960's the FBI moved to quash the growing civil rights movement in the South. Over one-fourth of all Klan members in the South were FBI agents and informants, and much violence against the civil rights movement can be directly attributed to these agents. One FBI provocateur, Gary Thomas Rowe, was an active participant in widespread Klan violence, including the murder of civil rights worker Viola Liuzzo, the bombing of a Birmingham church which killed four Black children, and the killing of a Black man during a racial disturbance in Birmingham in 1963. Much of the FBI's attention, as has now become well known, was focused on Dr. Martin Luther King, Jr. and the Southern Christian Leadership Conference(SCLC).

As early as 1960, the FBI started a comprehensive program, originating in Chicago, designed to disrupt and neutralize the Nation of Islam. Although the bulk of the files are still secret, released documents reveal that one of the primary purposes of this program was to exacerbate the tensions between Malcolm X and Elijah Muhammed, and these activities either directly or indirectly led to the assassination of Malcolm X in 1965. Also in 1960, the FBI ordered their field offices to begin counterintelligence activities to "thoroughly disrupt" the Puerto Rican Independence movement, especially the Puerto Rican Nationalist Party and what is now the Puerto Rican Socialist Party.

As the civil rights movement moved to the north, and urban ghetto uprisings punctuated Black people's demand for liberation, the FBI greatly expanded their counterintelligence programs against the Black movement and its leadership. In August of 1967 Hoover directed all field offices to establish a "black nationalist" counterintelligence program, designed to "expose, disrupt, misdirect, discredit and otherwise neutralize" Black nationalist organizations and their leaders. The Student Non-Violent Coordinating Committee (SNCC), SCLC, the Revolutionary Action Movement (RAM), the Nation of Islam, and the Deacons of Defense were specifically targeted, as were Stokely Carmichael, H. Rap Brown, the Honorable Elijah Muhammed, and Maxwell Stanford, among others.

On March 4, 1968, Hoover exhorted 41 field offices to redouble their counterintelligence efforts against the Black liberation struggle, instructing them to "prevent coalitions between militant Black nationalist groups", to "prevent the rise of a 'messiah' who could unify, and electrify, the militant black nationalist movement", and to "prevent the long-range growth of militant black nationalist organizations." One month later, Dr. King, the target of countless counterintelligence maneuvers which included wiretaps and bugs, blackmail, a suicide note, and an attempt to replace him with an FBI plant, was felled by an assassin's bullet, an assassination which still leaves many unanswered questions concerning the FBI's role, and reveals yet another FBI coverup.

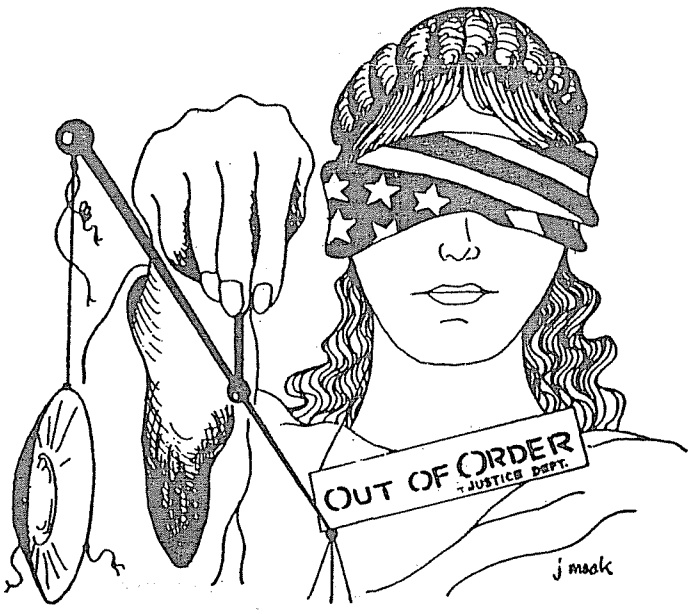
The Bureau set out to implement this expanded program with a vengeance. They moved to neutralize public figures such as Dick Gregory and Muhammed Ali, sought to disrupt militant Third World community organizations, and focused on revolutionary nationalist organizations and the Republic of New Africa (RNA), which had gained wide influence in the Black liberation struggle in early 1968 after declaring that all Black Americans (New Africans) were citizens of the Black nation, whose rightful land was 5 states of the deep South. Much energy was expended on discrediting Stokley Carmichael, who was branded by the FBI as a CIA agent.

It did not take long, however, for the FBI to make its main target the Black Panther Party. In late 1968, the Bureau sent out a communique to all field offices exhorting them to "cripple the BPP." For the next four years, in what the Senate Select Committee on Intelligence described as a "covert program to destroy the Black Panther Party," the FBI maintained a massive counterintelligence program, steeped in violence and illegality, against the Panthers. Determined to silence the strongest and most militant black revolutionary organization, the Bureau used everything from wiretap to murder. They coordinated police raids against Panther homes and offices throughout 1969, and set up the police murder of Fred Hampton, one of the youngest and most inspiring of all Black leaders, on December 4, 1969. They put special emphasis on disrupting the BPP's most successful programs, such as the Breakfast Program and the Black Panther Newspaper, and instructed all field offices to "destroy what they stand for." Although they focused on the Panthers, they also continued to disrupt the Young Lords, the Republic of New Africa, and the Nation of Islam; and worked hard to discredit Rev. Charles Koen, who was leading a heroic battle against Klan terror in Cairo, Illinois. The Bureau took credit for the demise of several Panther chapters, and for the 1971 split between Huey Newton and Eldridge Cleaver.

During 1971, the FBI office in Media, Pennsylvania was secretly entered by nameless American patriots, who managed to liberate a number of counterintelligence documents. The FBI then claimed that it was disbanding its counterintelligence programs, but, in fact, it has only charged the names. FBI counterintelligence against the American Indian Movement and Native American people across the country has intensified over the past several years, as the events at Wounded Knee and FBI terror on the Pine Ridge reservation show.

The FBI until recently orchestrated and coordinated violent attacks on the Iranian Student Association by agents of the Shah of Iran's Secret Police (SAVAK) in the United States, in order to crush the ISA in this country. The FBI and the Justice Department have resumed the inquisitional use of Grand Juries to jail Puerto Rican and Chicano activists, and have employed widespread intimidation and harrassment in Puerto Rican and Chicano communities to disrupt activities there. The FBI continues to assist in and condone violence against Native Americans. While Assata Shakur and Imari Obedele are no longer in prison, many other victims of FBI counterintelligence remain incarcerated, victims of set-ups and frame-ups: Geronimo Pratt and citizens of the Republic of New Africa, to name but a few. COINTELPRO continues. A tragic repitition of history occured when five members of the Communist Workers Party were slain by members of the Ku Klux Klan and American Nazi Party in Greensboro, North Carolina on November 3, 1979. The local police and FBI, who were aware of the intentions of the Klansmen and Nazis to disrupt the CWP demonstration -- and that they were armed -- did nothing to prevent the assault, and indeed, were many blocks away when the murders took place. The resemblance to the incident in Birmingham, Alabama almost twenty years ago that is recorded in FBI memos on pages four and five of this book, is chilling; and is also a reminder of the words of "The Director" J. Edgar Hoover, who said in a 1964 FBI memo:

> "Over the years, our approach to investigative problems in the intelligence field has given rise to a number of new programs, some of which have been most revolutionary, and it can be presumed that with a continued aggressive approach to these problems, new and productive ideas will be forthcoming. These ideas will not be increased in number or improved upon from the standpoint of accomplishments merely through the institution of a program such as COINTELPRO which is given another name, and which, in fact, only encompasses everything that has been done in the past or will be done in the future."



4

Documents detail FBI-Klan links in early rights strife

DETROIT [UPI]—Documents obtained by the American Civil Liberties Union show that in 1961 the FBI passed along information about two Freedom Rider buses to a Birmingham, Ala., police sergeant who was a known Ku Klux Klan agent.

Howard Simon, Michigan ACLU executive director, said the 3,000 pages of FBI letters, memos, and teletype messages were released to ACLU attorneys in a lawsuit filed against the FBI for allegedly failing to prevent Klan attacks on Freedom Riders.

"What we found in the documents was rather startling," Simon said Sunday. "The ACLU is charging that the FBI provoked the Klan to carry out terrorist acts against civil rights workers."

HE SAID DOCUMENTS show that the FBI knew Sgt. Thomas Cook of the police department's intelligence branch was giving the Klan the information that the FBI was providing about civil rights workers.

According to the documents, the chief of the Birmingham FBI office called Cook to inform him of the progress the buses were making through the racially tense South and when they were due to arrive at Alabama bus stations.

According to Simon, an FBI informant who had infiltrated the Klan said Cook and Birmingham's public safety director, Eugene "Bull" Connor, conspired with Klan leaders to allow physical attacks on Freedom Riders when the buses arrived at terminals in Birmingham.

THE DOCUMENTS, he said, show that Birmingham police agreed to arrive at the terminals 15 or 20 minutes after the buses arrived to give Klansmen time to attack the civil rights workers. Klansmen arrested after then were promised light sentences.

When buses arrived, no police were present. Klansmen attacked civil rights workers, reporters, and press photographers with chains, pipes, and baseball bats.

Earlier the same day, Klansmen intercepted a Freedom bus at Anniston, Ala., 50 miles to the east, and set it on fire.

"We found," Simon said, "that the FBI knew that the Birmingham Police Department was infiltrated by the Klan, that many members of the police department were Klan members, that they knew a person in intelligence was passing information directly to leaders of the Klan, and they also knew that their undercover agent had worked out an agreement with the police department to stay away from the terminals.

"THEY KNEW ALL that, and yet they continued their relationship with the police department."

The documents were released to attorneys for Walter Bergman, 80, a former Wayne State University professor and Detroit school board official who has filed a $1 million lawsuit against the FBI.

Chicago Tribune 8/78

BH 248-PCI (RAC), who has furnished reliable information in the past, orally furnished the following information:

On April 21, 1961, BH 248-PCI (RAC) telephonically contacted this Agent and advised that he had in his possession certain communications which he had received from one T. H. COOK, Sergeant of the Birmingham Police Department, which communications he had shown to ROBERT THOMAS, HUBERT PAGE, GENE REEVES and BILL HOLT, after the regular closed meeting of Eastview Klavern #13, of THE ALABAMA KNIGHT, KNIGHTS OF THE KU KLUX KLAN, INCORPORATED, on April 20, 1961.

He said he had received the inter-office communications from COOK, on the morning of April 20, 1961, and was given instructions to turn these over to ROBERT THOMAS and HUBERT PAGE, with the thought in mind that the KLAN could possibly reproduce the information contained in the communications on the KLAN press for distribution to the members of THE ALABAMA KNIGHTS.

COOK opened several file drawers in his filing cabinets and told informant that any information contained in his files was readily available to informant, for the use of the KLAN, in general.

Reference is made to matter entitled, "INFILTRATION OF LAW ENFORCEMENT AGENCIES BY KLAN-TYPE ORGANIZATIONS, RACIAL MATTERS" (Bufile [redacted]). The Bureau is aware that III Sergeant TOM COOK of the Birmingham Police Department has been furnishing information concerning potential violence given him by the Birmingham FBI Office to THE ALABAMA KNIGHTS, KNIGHTS OF THE KU KLUX KLAN, INCORPORATED.

On May 12, 1961, Birmingham Confidential Informant T-1, who has furnished reliable information in the past, advised that at a regular closed meeting of Eastview Klavern #13 of THE ALABAMA KNIGHTS, KNIGHTS OF THE KU KLUX KLAN, INCORPORATED, the arrival of the CORE group and KLAN intervention, on May 14, 1961, was discussed. All Klansmen were told to stay away from the Greyhound Bus Terminal, unless specifically instructed to participate in KLAN intervention.

After the closed meeting, according to T-1, HUBERT PAGE, Grand Titan of THE ALABAMA KNIGHTS, advised several persons that ROBERT SHELTON, Imperial Wizard, THE ALABAMA KNIGHTS, had spoken to Detective TOM COOK, Birmingham Police Department, date and time unknown, concerning CORE. PAGE further related that the CORE group was to arrive at approximately 11:00 A.M., May 14, 1961, at the bus depot, and that sixty Klansmen were to participate in the beatings.

PAGE further stated that EUGENE "BULL" CONNOR, Police Commissioner, Birmingham, Alabama, had stated, "By God, if you are going to do this thing, do it right", referring to the proposed incident on Sunday, May 14, 1961.

FROM SAC, BIRMINGHAM /149-NEW/ 6P

DIRECTOR OF NEWS, WAPI, HAS ADVISED ME THAT UPON HIS ARRIVAL AT THE TRAILWAYS BUS STATION THIS AFTERNOON

HE SAW A SHORT, HEAVY SET, WHITE MAN WEARING A YELLOW SHIRT, KNOCK A NEGRO MALE TO THE GROUND AND JUMP ON HIM, AND THAT IMMEDIATELY THEREAFTER SEVERAL MEN STARTED THROWING PEOPLE AROUND. HE STATED THAT HE SAW NO POLICE IN SIGHT, BUT DID SEE TWO NEWS PHOTOGRPAHERS TAKING PHOTOGRAPHS. HE STATED THAT THE NEGRO RAN OUT OF THE BUS STATION, HIS FACE WAS BLOØDY AND ONE OF HIS PANTS- LEGS RIPPED OFF.

6

UNITED STATES GOVERNMENT

Memorandum

TO : DIRECTOR, FBI (105-66754) DATE: 11/15/60

FROM : SAC, NEW YORK (105-32872)

SUBJECT: GROUPS SEEKING INDEPENDENCE FOR PUERTO RICO (COUNTERINTELLIGENCE PROGRAM) SUBVERSIVE CONTROL
(OO: San Juan)

Re Bureau letter dated 9/13/60.

A review of the files of the NYO has been made concerning the activities of Puerto Rican pro-independence groups which seek independence by other than peaceful means, as well as the files on the counterintelligence program as it relates to the Communist Party. It is believed that upon instituting a counterintelligence program in this field, efforts should be directed with the following aims in mind:

I. Disruption and discord.

II. Creating doubts as to the wisdom of remaining in the independence movement.

III. Causing defections from the indpendence movement.

The suggested means of obtaining these desired ends are as follows:

1) Exploiting factionalism within an organization.

Factionalism is a common fault within pro-independence groups and it is believed that this existing element can be developed, enlarged and exploited. As an example, after the demise of the Accion Patriotica

- P -

2 - Bureau (105-66754) (RM)
2 - San Juan (105-3353) (RM)
1 - New York (105-32872) (#413)

JJT:vcb
(5)

105-93124-5

15 NOV 17 1960

EX-REC

Page 594 of 3957

SAC, San Juan (105-3353) August 4, 1960

Director, FBI (105-66754) PERSONAL ATTENTION

GROUPS SEEKING INDEPENDENCE
FOR PUERTO RICO
(SUBVERSIVE CONTROL)

The Bureau is considering the feasibility of instituting a program of disruption to be directed against organizations which seek independence for Puerto Rico through other than lawful, peaceful means.

Because of the increasing boldness apparent in the activities of such organizations, their utter disregard of the will of the majority, the inevitable communist and/or Soviet effort to embarrass the United States, and the courage given to their cause by Castro's Cuba, we must make a more positive effort, not only to curtail, but to disrupt their activities.

San Juan and New York should give this matter studied consideration and thereafter furnish the Bureau observations, suggestions and recommendations relative to the institution of such a program to reach the Bureau no later than 8/25/60.

In considering this matter, you should bear in mind the Bureau desires to disrupt the activities of these organizations and is not interested in mere harassment. No action should be taken in this program without Bureau authority, at any time.

A copy of this communication is designated for the Chicago Office and a copy for the Washington Field Office for information.

2 - New York (105-32872)
1 - Chicago (105-5581)
1 - Washington Field
1 - 62-7721 (NPPR)

TC/baw
(9)

EX 109 105-93124-1
REC 89
AUG 1960

64 AUG 10 1960

MAIL ROOM ☐ TELETYPE UNIT ☐

UNRECORDED COPY FILED IN

8

1

SAC, San Juan (105-3353 Sub 1) June 12, 1961

Director, FBI (105-93124)

CONFIDENTIAL

GROUPS SEEKING INDEPENDENCE FOR PUERTO RICO
(COUNTERINTELLIGENCE PROGRAM)
SUBVERSIVE CONTROL SECTION

In order to appraise the caliber of leadership in the Puerto Rican independence movement, particularly as it pertains to our efforts to disrupt their activities and compromise their effectiveness, we should have an intimate detailed knowledge of the more influential leaders as individuals.

The names of each of the leaders listed below are maintained in the Security Index.

SAN JUAN

[redacted]

NEW YORK

[redacted]na

Your files will contain descriptive information appropriate to our investigative reporting. We should, however, for the purposes of this program, delve deeply into that part of their lives which do not show on the surface; for example, we must determine their capabilities of influencing others, capabilities of real leadership, why the intense desire for Puerto Rico's independence, what they expect to gain from independence, and the support they have from other leaders and rank-and-file members. We must have information concerning their weaknesses, morals, criminal records, spouses, children, family life, educational qualifications and personal activities other than independence activities.

2 - New York (105-32872)

DECLASSIFIED BY 6080 ltr 1977

EX-114

105-93124-95

SEE NOTE ON YELLOW, PAREC-23

TC:djw

10 JUN 13 1961

CIS

TELETYPE UNIT

OPTIONAL FORM NO. 10 MAY 1962 EDITION GSA FPMR (41 CFR) 101-11.6

UNITED STATES GOVERNMENT

Memorandum

Parsons
Violation X

9

TO DIRECTOR, FBI (100-448006) DATE: 1/22/69

FROM SAC, CHICAGO (157-2209) (P)

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
(NATION OF ISLAM)

Reurlet, 1/7/69; Chicago letters 12/24/68 and 1/14/69.

ReBulet has been thoroughly studied and discussed by the SAC, the Supervisor, and Agents familiar with facets of the NOI which might indicate trends and possible future direction of the organization. The Bureau's concern is most understandable and suggestions appreciated.

Over the years considerable thought has been given, and action taken with Bureau approval, relating to methods through which the NOI could be discredited in the eyes of the general black populace or through which factionalism among the leadership could be created. Serious consideration has also been given towards developing ways and means of changing NOI philosophy to one whereby the members could be developed into useful citizens and the organization developed into one emphasizing religion - the brotherhood of mankind - and self improvement. Factional disputes have been developed - the most noteable being MALCOLM X LITTLE. Prominent black personages have publicly and nationally spoken out against the group - U.S. District Court Judge JAMES BENTON PARSONS being one example. The media of the press has played down the NOI. This appears to be a most effective tool as individuals such as MUHAMMAD assuredly seek any and all publicity be it good or bad; however, if the press is utilized it would appear it should not concentrate on such aspects as the alleged strength of the NOI, immoral activities of the leadership, misuse of funds by these officials, etc. It is the opinion of this office that such exposure is ineffective, possibly creates interest and maybe envy among the lesser educated black man causing them out of curiosity to attend meetings and maybe join, and encourage the opportunist to seek personal gain - physical or monetary - through alignment with the group. At any rate it is felt such publicity in the case of the NOI is not overly effective.

2 - Bureau (RM)
1 - Chicago
JRS:bab
(3)

Buy U.S. Savings Bonds Regularly on the Payroll Savings Plan

10

FBI

Date: 8/29/69

Transmit the following in _____ (Type in plaintext or code)

AIRTEL _____ (Priority)

TO : DIRECTOR, FBI (100-448006)

FROM : SAC, CHICAGO (157-2209)

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
(NATION OF ISLAM)

Re Miami airtels to the Director (copy to Chicago) 8/22/69, and 8/25/69.

At the present time, Chicago does not desire to rehash some of the exposes that occurred around the time of the defection of MALCOLM X LITTLE as top level sources could be endangered and future activities thereof curtailed.

Referenced Miami airtel dated 8/25/69, reflected [redacted] is attempting to locate statements of prominent government and police officials regarding dangers created by the NOI. Again, Chicago agrees that the constant hate teachings against the white race is most undesirable. This is especially true as it relates to the children of the membership who are indoctrinated from birth on to hate the white man.

In an effort to keep [redacted] proposed documentary current, the following observations are set forth:

Report of [redacted] dated 6/20/69, pages 49 - 53, copy available to Miami, sets forth full details regarding ELIJAH MUHAMMAD's statements concerning his version of law and order; sets forth data regarding a meeting of the minds between the NOI and the Chicago Police Department; and relates details concerning plans by the National Society of Afro-American Policemen, New York City, to honor MUHAMMAD and the NOI in June, 1969. While this is in no way meant to infer the NOI is a useful, integral

Page 598 of 3957

Washington Star

11

WASHINGTON, D.C., WEDNESDAY, NOVEMBER 19, 1975 Phone (202) 484-5000

By Norman Kempster
Washington Star Staff Writer

Looking gray and wan after a 2½-month bout with cancer, Sen. Philip Hart spent one of his first days back on Capitol Hill listening to a catalog of apparently illegal FBI activities that ranged from fomenting violence to suggesting suicide.

"Over the years, we have been warned about the dangers of subversive organizations . . . organizations that would incite and perpetrate violence, pit one American group against another. I think the story you told us today shows there is an organization that does fit those descriptions. It is the organization (the FBI) that has been most active in its warnings to be on guard against such organizations.

Hart's statement was the emotional peak of a hearing yesterday in which the committee's top two staff members, chief counsel Fritz Schwarz and minority counsel Curtis Smothers, took the lawmakers on a guided tour of 20 years of FBI files recording efforts to disrupt and destroy organizations ranging from the Ku Klux Klan to the Black Panthers.

According to Schwarz and Smothers, the most determined of all of the bureau's domestic counterintelligence activities was aimed at discrediting the Rev. Dr. Martin Luther King Jr., head of the Southern Christian Leadership Conference, and dissipating his influence in the black community.

SMOTHERS SAID the files show that Hoover was suspicious of King from the moment King first began to achieve national prominence with the Montgomery, Ala., bus boycott in 1956. One reason for the animosity, Smothers suggested, was King's criticism of Hoover.

By December 1963, shortly after the assassination of former President John F. Kennedy, the effort to discredit King began in earnest. An FBI memo summarizing a meeting devoted to ways of dealing with King contains 21 suggestions of methods of obtaining derogatory information.

Many of the ideas are phrased as questions. They include, "Can colored agents be of any assistance?" "What are the possibilities of using Mrs. King?" "Are there any disgruntled employes of SCLC?" and "What are the possibilities of providing a good-looking female plant in King's office?"

Also suggested were telephone taps and hidden microphones. The first of these was installed the next month.

In all, 16 microphones were planted in hotel rooms used by King during the next few years. There also were several telephone taps.

SHORTLY BEFORE King was to leave for Stockholm in 1965 to receive the Nobel Peace Prize, the FBI sent King an anonymous letter which seemed to be a suggestion that he kill himself. The letter was accompanied by a tape recording of some of the hotel room bugs.

"King, there is only one thing left for you to do," the letter said. "You know what it is. You have just 34 days (the number of days before the Nobel ceremony) in which to do it. . . . You are done. There is but one way out for you."

King did not kill himself. But another FBI dirty trick may have indirectly contributed to his assassination in April of 1968.

The FBI files show that the bureau leaked to a friendly reporter that King was staying in the white-owned Holiday Inn during his participation in a sanitation workers strike that included a boycott of white-owned businesses. A bureau memo said King should be called a hypocrite because he was not staying in the Lorraine, a black-owned and black-patrionized motel.

King did check into the Lorraine where he was shot to death April 4 while standing on a balcony. The FBI contends that he had checked into the black-owned motel before the reports of his stay at the Holiday Inn had surfaced.

IN 1963, former Asst. FBI Director William Sullivan suggested to Hoover that the bureau pick and develop a "national Negro leader" to take King's place. Hoover approved the plan, but apparently nothing ever came of it.

Smothers said the FBI had in mind a black who was prominent in a field other than civil rights. Smothers said the individual, whom he would not name, apparently never knew of the plan.

An obsession with communism runs through the documents that were either released or read.

An April 24, 1964, memo from Hoover to the special agent in charge of the New York office called for renewed investigation of a civil rights leader, whose name was removed before the document was made public: "The bureau does not agree with the expressed belief of the New York office that (deleted) is not sympathetic to the party cause. While there may not be any evidence that (deleted) is a Communist, neither is there any substantial evidence that he is anti-Communist."

AN EXCHANGE of memos between Hoover and Sullivan in mid-1963 illustrates Hoover's determination to find Communist influence even where it might not exist and spotlights the problems of working for the often irascible director.

Sullivan at first said an investigation had turned up no evidence of substantial Communist penetration of the civil rights movement. Hoover penned at the bottom of the memo a sarcastic note that Sullivan once doubted Communist influence on Fidel Castro.

Sullivan took the hint. He shortly wrote a memo noting that "the director is correct."

"When it came to blacks, the most violent types of methods seemed to be acceptable," Smothers said. "If they were going to have gang fights and if they were going to be killing each other, it seemed to be an opportunity to promote it."

12

SAC, Albany

August 25, 1967

Director, FBI

PERSONAL ATTENTION TO ALL OFFICES

1 - Mr. C. D. Brennan
1 -
1 -
1 -
1 -

COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
INTERNAL SECURITY

Offices receiving copies of this letter are instructed to immediately establish a control file, captioned as above, and to assign responsibility for following and coordinating this new counterintelligence program to an experienced and imaginative Special Agent well versed in investigations relating to black nationalist, hate-type organizations. The field office control file used under this program may be maintained in a pending inactive status until such time as a specific operation or technique is placed under consideration for implementation.

The purpose of this new counterintelligence endeavor is to expose, disrupt, misdirect, discredit, or otherwise neutralize the activities of black nationalist, hate-type organizations and groupings, their leadership, spokesmen, membership, and supporters, and to counter their propensity for violence and civil disorder. The activities of all such groups of intelligence interest to this Bureau must be followed on a continuous basis so we will be in a position to promptly take advantage of all opportunities for counterintelligence and to inspire action in instances where circumstances warrant. The pernicious background of such groups, their duplicity, and devious maneuvers must be exposed to public scrutiny where such publicity will have a neutralizing effect. Efforts of the various groups

MCT-34
REC 32 100-448006
X 106

2 - Atlanta
2 - Baltimore
2 - Boston
2 - Buffalo
2 - Charlotte
2 - Chicago
2 - Cincinnati
2 - Cleveland
2 - Detroit
2 - Jackson
2 - Los Angeles
2 - Memphis
2 - Newark
2 - New Orleans
2 - New York
2 - Philadelphia
2 - Phoenix
2 - Pittsburgh
2 - Richmond
2 - St. Louis
2 - San Francisco
2 - Washington Field Office

19 AUG 29 1967

MAILED 3
AUG 25 1967
COMM-FBI

Tolson
DeLoach
Mohr
Bishop
Casper
Callahan
Conrad
Felt
Gale
Rosen
Sullivan
Tavel
Trotter
Walters
Soyars

56 SEP 6 1967 (53)

MAIL ROOM ☐ TELETYPE UNIT ☐

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE.

to consolidate their forces or to recruit new or youthful adherents must be frustrated. No opportunity should be missed to exploit through counterintelligence techniques the organizational and personal conflicts of the leaderships of the groups and where possible an effort should be made to capitalize upon existing conflicts between competing black nationalist organizations. When an opportunity is apparent to disrupt or neutralize black nationalist, hate-type organizations through the cooperation of established local news media contacts or through such contact with sources available to the Seat of Government, in every instance careful attention must be given to the proposal to insure the targeted group is disrupted, ridiculed, or discredited through the publicity and not merely publicized. Consideration should be given to techniques to preclude violence-prone or rabble-rouser leaders of hate groups from spreading their philosophy publicly or through various mass communication media.

Many individuals currently active in black nationalist organizations have backgrounds of immorality, subversive activity, and criminal records. Through your investigation of key agitators, you should endeavor to establish their unsavory backgrounds. Be alert to determine evidence of misappropriation of funds or other types of personal misconduct on the part of militant nationalist leaders so any practical or warranted counter-intelligence may be instituted.

Intensified attention under this program should be afforded to the activities of such groups as the Student Nonviolent Coordinating Committee, the Southern Christian Leadership Conference, Revolutionary Action Movement, the Deacons for Defense and Justice, Congress of Racial Equality, and the Nation of Islam. Particular emphasis should be given to extremists who direct the activities and policies of revolutionary or militant groups such as Stokely Carmichael, H. "Rap" Brown, Elijah Muhammad, and Maxwell Stanford.

At this time the Bureau is setting up no requirement for status letters to be periodically submitted under this program. It will be incumbent upon you to insure the program is being afforded necessary and continuing attention and that no opportunities will be overlooked for counterintelligence action.

This program should not be confused with the program entitled "Communist Party, USA, Counterintelligence Program, Internal Security - C," (Bufile 100-3-104), which is directed

Letter to SAC, Albany
RE: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS

against the Communist Party and related organizations, or the program entitled "Counterintelligence Program, Internal Security, Disruption of Hate Groups," (Bufile 157-9), which is directed against Klan and hate-type groups primarily consisting of white memberships.

All Special Agent personnel responsible for the investigation of black nationalist, hate-type organizations and their memberships should be alerted to our counterintelligence interest and each investigative Agent has a responsibility to call to the attention of the counterintelligence coordinator suggestions and possibilities for implementing the program. You are also cautioned that the nature of this new endeavor is such that under no circumstances should the existence of the program be made known outside the Bureau and appropriate within-office security should be afforded to sensitive operations and techniques considered under the program.

No counterintelligence action under this program may be initiated by the field without specific prior Bureau authorization.

You are urged to take an enthusiastic and imaginative approach to this new counterintelligence endeavor and the Bureau will be pleased to entertain any suggestions or techniques you may recommend.

-3-

DAILY DEFENDER 12/4/75

Bare new data in FBI-King

BY DANIEL F. GILMORE

WASHINGTON (UPI)—Former Attorney Gen. Nicholas Katzenbach testified Wednesday that J. Edgar Hoover risked the reputation of the FBI—"his life's work—in a vendetta against Dr. Martin Luther King, Jr.

Katzenbach told the Senate Intelligence committee that when he was Attorney General during 1965-66, he knew of telephone wiretaps against King by the FBI and once ordered a tap on King's home phone ended.

But he said he learned later the FBI put electronic "bugs" in King's hotel room without authorization and used other "unlawful and grossly improper" tactics against King.

When questioned about three memos to him written by Hoover in 1965, giving what Katzenbach called "after-the-fact" notification of bugs in King's hotel room, he said the memos contained initials "that appear to be mine".

Also testifying was Ramsey Clark who gave no specifics about what he may have known when he was Attorney General in 1967-69, but said the FBI was trying "to destroy the desperately needed moral leadership of Martin Luther King."

"His vendetta against Dr. King, if successful, could have led to a civil strife of frightening magnitude."

DIRECTOR, FBI (100-3-104-34) 6/1/67

SAC, CHICAGO (100-32864)

COMMUNIST PARTY, USA
COUNTERINTELLIGENCE PROGRAM
INTERNAL SECURITY - C
(MARTIN LUTHER KING)

ReBulet 5/18/67 and NYlet to Bureau 5/25/67.

It is agreed that the CommunistParty's (CP) interest in a peace ticket headed by MARTIN LUTHER KING and BENJAMIN SPOCK offers the appearance of a counterintelligence opportunity. The reference to this matter in Bureau letter dated 5/18/67 obviously relates to the Presidential elections of November, 1968.

A reporter or columnist of national stature, properly briefed, could write an excellent account of the KING-SPOCK ticket. It is the sort of article or series expected of a first rate reporter with first rate sources.

It is suggested that the Bureau consider our comments as reflected above. Consider also a top columnist or reporter who might be interested in the KING-SPOCK story. It is emphasized that this person should be respected for his balance and fair-mindedness. An article or series by an established conservative would not adequately serve our purposes. In this area the Bureau might desire to consider a [redacted] A former confidant of [redacted] he has excellent sources throughout the government and is not too close to the current administration to be branded as a propagandist. [redacted] also would [illegible] the charge that he is attempting to discredit these men. Left standing would be the realization that [redacted] had good sources and came up with [redacted] in the midst of the Presidential campaign. And [redacted] would not be about to divulge the identity of his sources. Thus the Bureau would stand harmless.

It is not known whether the Bureau has information which would make [redacted] selection undesirable. If his selection is not feasible, there are others in the [redacted] field who could serve as well. But it is clear that this man [redacted] and should not be a protagonist for either those of the "hawk" or "dove" persuasion.

Since the contact with [redacted] would be made in [redacted] no specific recommendation is being made at this time.

16

FBI tried to manipulate vote of NAACP, files indicate

By Sean Toolan CT 7/30/79

COPIES OF FBI documents released Sunday indicate that the Chicago FBI office planned to manipulate a National Association for the Advancement of Colored People [NAACP] election in Chicago in 1959.

The documents, presented at a press conference at the Bismarck Hotel by Richard Gutman, a lawyer representing the Alliance to End Repression in a suit against the Chicago Police Department, also indicate that the Federal Bureau of Investigation office in Chicago suggested methods for sabotaging a planned 1968 Martin Luther King-Benjamin Spock campaign for President.

Gutman obtained the documents under the Freedom of Information Act, which gives the public access to previously secret government documents. The group has obtained previous FBI documents for use in the suit, which seeks to halt government spying on such groups.

The documents describe how the Chicago FBI office, through an infiltrator, learned that the NAACP's so-called "left caucus" planned to run a slate of candidates for delegates to the NAACP national convention.

THE FBI SENT an anonymous letter and made an anonymous phone call to Theodore A. Jones, then president of Chicago NAACP, telling him that "two Communists" were on the slate, according to the documents.

The FBI went on to report that Jones kept the location of the delegate elections secret, and that Jones "packed the meeting with members of the United Steel Workers Union whom Jones had enfranchised for the meeting."

THE FBI HERE concluded in its report that "Chicago feels it has played a definite part in the defeat of a 'left caucus,' an attempt by the CP [Communist Party] to infiltrate a 'right led' organization."

J. Edgar Hoover, then the director of the FBI, later recommended a commendation for the agent who "suggested the anonymous letter," according to the documents.

Timuel D. Black, a professor of social science at Loop College, said Sunday he was a member of the so-called "left caucus" at the time and a candidate for the board of directors of the Chicago NAACP chapter.

"I was very shocked and a bit enraged to learn that the taxpayer-supported FBI had been interfering with the democratic process they were supposed to protect."

HE SAID HE knew something unusual was happening in the local NAACP when its members weren't even able to find out when and where meetings were being held.

"And when we found out about the meetings and went to them," Black said, "they were held in a high-handed, dictatorial manner. The decisions were arbitrary. We were cut off and cut out."

Black said members of the "left caucus" thought it was Chicago's Democratic machine that was interfering with their organization.

In 1967, according to the documents, the FBI here suggested a campaign to sabotage the King-Spock presidential campaign by recommending the name of a newspaper columnist to write an article attacking the campaign as "Communist-backed." Spock ran for president and King for vice president on the ticket.

THE DOCUMENTS released Sunday also indicate that the FBI here planned to "discredit Students for a Democratic Society [a radical group] in the eyes of the Negro community. And by appropriate sources organize an anti-SDS demonstration by a group of Negroes accusing the SDS of being white-oriented."

Other documents indicate the FBI tried to remove Herbert Mohammad as a possible successor to his father as head of the Nation of Islam, by going through his tax returns for possible irregularities.

Gutman charged that the files are "proof of the Chicago FBI's massive organized campaign of disrupting the exercise of First Amendment rights, of promoting enmity between groups, of disseminating derogatory information, and of manipulating the mass media."

THE ALLIANCE to End Repression and 32 other groups have presented the FBI files as evidence for a suit filed in November, 1974, which seeks a court declaration that the government spying be halted permanently.

Asked if he thought FBI spying was still going on, Gutman said: "It was supposed to have ended in 1970, but many cases we have show it continued after then."

To: SAC, Chicago (100-32864)

From: Director, FBI (100-3-104)

The Bureau was pleased to note that the "left caucus" was badly defeated in its efforts to elect nine candidates as delegates to the 1959 convention of the National Association for the Advancement of Colored People (NAACP) at the Chicago branch meeting of the NAACP in Chicago on 5-22-59.

It is suggested that if you have not already done so, you may desire to submit your recommendations for commendation of the Agent who suggested the technique of the anonymous letter to Theodore A. Jones, president of the Chicago branch of the NAACP, which apparently played a major role in alerting Jones to the danger the Communist Party posed to his organization.

3/4/68

AIRTEL

1 - Mr. C. D. DeLoach
1 - Mr. W. C. Sullivan
1 - Mr. G. C. Moore
1 - [redacted]
1 - [redacted]

To: SAC, Albany

PERSONAL ATTENTION

REC 18

From: Director, FBI (100-448006) — 17

COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST-HATE GROUPS
RACIAL INTELLIGENCE

MAR 5 1968 COMM-FBI

Title is changed to substitute Racial Intelligence for Internal Security for Bureau routing purposes.

PERSONAL ATTENTION FOR ALL THE FOLLOWING SACs

2 - Atlanta
2 - Baltimore
2 - Birmingham
2 - Boston
2 - Buffalo
2 - Charlotte
2 - Chicago
2 - Cincinnati
2 - Cleveland
2 - Denver
2 - Detroit
2 - Houston
2 - Indianapolis
2 - Jackson
2 - Jacksonville
2 - Kansas City
2 - Los Angeles
2 - Memphis
2 - Miami
2 - Milwaukee
2 - Minneapolis
2 - Mobile
2 - Newark
2 - New Haven
2 - New Orleans
2 - New York
2 - Omaha
2 - Philadelphia
2 - Phoenix
2 - Pittsburgh
2 - Portland
2 - Richmond
2 - Sacramento
2 - San Diego
2 - San Francisco
2 - Seattle
2 - Springfield
2 - St. Louis
2 - Tampa
2 - WFO

TJD:rmm (88)

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE.

SEE NOTE PAGE SIX

5 4 MAR 18 1968

MAIL ROOM ☐ TELETYPE UNIT ☐

Airtel to SAC, Albany
RE: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST-HATE GROUPS

BACKGROUND

By letter dated 8/25/67 the following offices were advised of the beginning of a Counterintelligence Program against militant Black Nationalist-Hate Groups:

Albany	Memphis
Atlanta	Newark
Baltimore	New Orleans
Boston	New York
Buffalo	Philadelphia
Charlotte	Phoenix
Chicago	Pittsburgh
Cincinnati	Richmond
Cleveland	St. Louis
Detroit	San Francisco
Jackson	Washington Field
Los Angeles	

Each of the above offices was to designate a Special Agent to coordinate this program. Replies to this letter indicated an interest in counterintelligence against militant black nationalist groups that foment violence and several offices outlined procedures which had been effective in the past. For example, Washington Field Office had furnished information about a new Nation of Islam (NOI) grade school to appropriate authorities in the District of Columbia who investigated to determine if the school conformed to District regulations for private schools. In the process WFO obtained background information on the parents of each pupil.

The Revolutionary Action Movement (RAM), a pro-Chinese communist group, was active in Philadelphia, Pa., in the summer of 1967. The Philadelphia Office alerted local police, who then put RAM leaders under close scrutiny. They were arrested on every possible charge until they could no longer make bail. As a result, RAM leaders spent most of the summer in jail and no violence traceable to RAM took place.

The Counterintelligence Program is now being expanded to include 41 offices. Each of the offices added to this program should designate an Agent familiar with black

Airtel to SAC, Albany
RE: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST-HATE GROUPS

nationalist activity, and interested in counterintelligence, to coordinate this program. This Agent will be responsible for the periodic progress letters being requested, but each Agent working this type of case should participate in the formulation of counterintelligence operations.

GOALS

For maximum effectiveness of the Counterintelligence Program, and to prevent wasted effort, long-range goals are being set.

1. Prevent the coalition of militant black nationalist groups. In unity there is strength; a truism that is no less valid for all its triteness. An effective coalition of black nationalist groups might be the first step toward a real "Mau Mau" in America, the beginning of a true black revolution.

2. Prevent the rise of a "messiah" who could unify, and electrify, the militant black nationalist movement. Malcolm X might have been such a "messiah;" he is the martyr of the movement today. Martin Luther King, Stokely Carmichael and Elijah Muhammed all aspire to this position. Elijah Muhammed is less of a threat because of his age. King could be a very real contender for this position should he abandon his supposed "obedience" to "white, liberal doctrines" (nonviolence) and embrace black nationalism. Carmichael has the necessary charisma to be a real threat in this way.

3. Prevent violence on the part of black nationalist groups. This is of primary importance, and is, of course, a goal of our investigative activity; it should also be a goal of the Counterintelligence Program. Through counterintelligence it should be possible to pinpoint potential troublemakers and neutralize them before they exercise their potential for violence.

4. Prevent militant black nationalist groups and leaders from gaining respectability, by discrediting them to three separate segments of the community. The goal of discrediting black nationalistsmust be handled tactically in three ways. You must discredit these groups and individuals to, first, the responsible Negro community. Second, they must be discredited to the white community,

Airtel to SAC, Albany
RE: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST-HATE GROUPS

both the responsible community and to "liberals" who have vestiges of sympathy for militant black nationalist simply because they are Negroes. Third, these groups must be discredited in the eyes of Negro radicals, the followers of the movement. This last area requires entirely different tactics from the first two. Publicity about violent tendencies and radical statements merely enhances black nationalists to the last group; it adds "respectability" in a different way.

5. A final goal should be to prevent the long-range growth of militant black nationalist organizations, especially among youth. Specific tactics to prevent these groups from converting young people must be developed.

Besides these five goals counterintelligence is a valuable part of our regular investigative program as it often produces positive information.

TARGETS

Primary targets of the Counterintelligence Program, Black Nationalist-Hate Groups, should be the most violent and radical groups and their leaders. We should emphasize those leaders and organizations that are nationwide in scope and are most capable of disrupting this country. These targets should include the radical and violence-prone leaders, members, and followers of the:

Student Nonviolent Coordinating Committee (SNCC),
Southern Christian Leadership Conference (SCLC),
Revolutionary Action Movement (RAM),
Nation of Islam (NOI)

Offices handling these cases and those of Stokely Carmichael of SNCC, H. Rap Brown of SNCC, Martin Luther King of SCLC, Maxwell Stanford of RAM, and Elijah Muhammed of NOI, should be alert for counterintelligence suggestions.

INSTRUCTIONS

Within 30 days of the date of this letter each office should:

1. Advise the Bureau of the identity of the Special Agent assigned to coordinate this program.

Airtel to SAC, Albany
RE: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST-HATE GROUPS

The effectiveness of counterintelligence depends on the quality and quantity of positive information available regarding the target and on the imagination and initiative of Agents working the program. The response of the field to the Counterintelligence Program against the Communist Party, USA, indicates that a superb job can be done by the field on counterintelligence.

Counterintelligence operations must be approved by the Bureau. Because of the nature of this program each operation must be designed to protect the Bureau's interest so that there is no possibility of embarrassment to the Bureau. Beyond this the Bureau will give every possible consideration to your proposals.

NOTE:

See memorandum G. C. Moore to Mr. W. C. Sullivan captioned as above dated 2/29/68, prepared by TJD:rmm.

22

ROUTE IN ENVELOPE

1 - [redacted], Justice
May 15, 1968
1 - [redacted]
PERSONAL ATTENTION

SAC, Chicago

Director, FBI (100-448006)

COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
(RICHARD CLAXTON GREGORY)

ReBulet 4/23/68.

Chicago airtel and LHM dated 5/2/68 and captioned "Richard Claxton Gregory" concern a speech by Gregory on 4/28/68 where he noted that "Syndicate hoods (are living all over. They are the filthiest snakes that exist on this earth." Referenced Bulet instructed you to develop counter-intelligence action concerning militant black nationalist Dick Gregory.

Consider the use of this statement in developing a counterintelligence operation to alert La Cosa Nostra (LCN) to Gregory's attack on LCN. It is noted that other speeches by Gregory also contain attacks on the LCN. No counterintelligence action should be taken without Bureau authority.

TJD:pag/mrm
(5)

NOTE:
Teletype from New Orleans to Director, [illegible]/30/68, captioned "Richard Claxton Gregory" reported speech by Gregory referring to the Director and FBI Agents in derogatory terms. The Director noted, on the informative note of the teletype which said we would recommend counterintelligence action against Gregory when indicated, "Right."

REC-7 100-[illegible]

[illegible]-68

Tolson
DeLoach
Mohr
Bishop
Casper
Callahan
Conrad
Felt
Gale
Rosen
Sullivan
Tavel

95 MAY 23 1968

6 MAY 24 1968

TELETYPE UNIT

11 MAY 15 1968

PLAINTIFF'S EXHIBIT 6 23

Memorandum

TO : SAC, Baltimore

DATE: 11/25/68

FROM : Director, FBI

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE (BLACK PANTHER PARTY)

DO NOT DESTROY
ATTORNEY'S COPY

For the information of recipient offices a serious struggle is taking place between the Black Panther Party (BPP) and the US organization. The struggle has reached such proportio that it is taking on the aura of gang warfare with attendant threats of murder and reprisals.

In order to fully capitalize upon BPP and US differences as well as to exploit all avenues of creating further dissension in the ranks of the BPP, recipient offices are instructed to submit imaginative and hard-hitting counterintelligence measures aimed at crippling the BPP.

Commencing December 2, 1968, and every two-week period thereafter, each office is instructed to submit a letter under this caption containing counterintelligence measures aimed against the BPP. The bi-weekly letter should also contain accomplishments obtained during the previous two-week period under captioned program.

All counterintelligence actions must be approved at the Bureau prior to taking steps to implement them.

- Chicago

Page 611 of 3957

24

ROUTE IN ENVELOPE

May 27, 1969

Airtel

1 [redacted]
1
1
1

To: SAC, San Francisco (157-601)

From: Director, FBI (100-448006)

COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
BLACK PANTHER PARTY (BPP)
BUDED: 6/9/69

PERSONAL ATTENTION

ReSFairtel 5/14/69.

A review has been made of referenced airtel which contains your thoughts on the Counterintelligence Program (CIP). Your reasoning is not in line with Bureau objectives as to our responsibilities under the CIP.

You state that while the Department of Justice considers the BPP as a violence-prone organization seeking to

1 - Atlanta
1 - Baltimore
1 - Boston
1 - Chicago
1 - Denver
1 - Detroit
1 - Los Angeles
1 - Newark
1 - New Haven
1 - New York
1 - Seattle
1 - WFO

ST 1-116

MAILED 8
MAY 26 1969
COMM-FBI

REC-32

100-448006-964

MAY 28 1969

JAM:klw/ekw
(19)

98 JUN 4 1969

TELETYPE UNIT

overthrow the Government by revolutionary means, "There seems to be little likelihood of this." All information developed to date leads to the obvious conclusion that this group is dedicated to the principle of violent overthrow and will go to any length to further this aim.

You point out that the activities of the BPP have reached the black and white communities as evidenced by their weekly newspaper which has reached a circulation of 45,000. You have previously been instructed to review your files concerning this newspaper to determine whether we could disrupt the mailings of the publication. Your answer stated that you were not in a position to do this. You must immediately take positive steps to insure that we will be in a position to accomplish CIP objectives including the disruption of the mailing of their publications. You must develop adequate informant coverage to insure that we are in a position to accomplish all of our objectives, which include steps to counteract the impact this group has made.

You state that local and national newspapers continue to publicize information concerning the BPP. This fact automatically lends itself toward mass media disseminations to capitalize on this eagerness and to isolate the organization from the majority of Americans, both black and white. The dissemination of mass media information to selected and trusted newspapermen, pointing out the violent and dangerous nature of a group, has contributed measurably to the decline of the Ku Klux Klan in the United States Newspapers will print derogatory information much easier than they will print commendatory information, especially if the organization is by its nature violence-prone. For your information the San Diego Office has waged an effective CIP against the BPP which has measurably resulted in declining activities and considerable disruption.

26

Airtel to SAC, San Francisco
RE: COUNTERINTELLIGENCE PROGRAM,
BLACK PANTHER PARTY
100-448006

It is noted that BPP leader Bobby Seale speaks in schools and universities and receives fees of up to $1,000. This raises counterintelligence opportunities, among which are anonymous disseminations of derogatory information to universities and misuse of funds received.

As it concerns the BPP, you point out that results achieved by utilizing counterintelligence ideas such as publicizing the evils of violence, the lack of morals, the widespread use of narcotics and anonymous mailings, have not been outstanding. This is because a typical black supporter of the BPP is not disturbed by allegations which would upset a white community. You must recognize that one of our primary aims in counterintelligence as it concerns the BPP is to keep this group isolated from the moderate black and white community which may support it. This is most emphatically pointed out in their Breakfast for Children Program, where they are actively soliciting and receiving support from uninformed whites and moderate blacks. In addition, we have received information from San Francisco and other offices indicating that BPP officials are extremely suspicious of each other as to monies received. This also is a fertile ground for CIP and should be explored.

ReSFairtel states that nation-wide mailings to BPP chapter offices would automatically indicate that the FBI was the source. Mailings originating from Oakland, California, would logically be attributed to someone either at national headquarters of the BPP or a dissident who has recently resigned and had access to the records.

You state that the Bureau under the CIP should not attack programs of community interest such as the BPP "Breakfast for Children." You state that this is because many prominent "humanitarians," both white and black, are interested in the program as well as churches which are actively supporting it.

Page 614 of 3957

You have obviously missed the point. The BPP is not engaged in the "Breakfast for Children" program for humanitarian reasons. This program was formed by the BPP for obvious reasons, including their efforts to create an image of civility assume community control of Negroes, and to fill adolescent children with their insidious poison. An example of this is set forth in the May 11, 1969, issue of "The Black Panther." Page seven contains an article captioned "Black Panther Revolutionary Wedding." The article points out that two members of the Panthers were married at a church in Oakland, California, which is participating in the Breakfast Program. The crowd consisted mostly of Panther members and children from the Breakfast Program. Instead of a Bible, Bobby Seale used the "Red Book Quotations from Chairman Mao Tse-tung" to perform the marriage. After the ceremony, the children sang "We Want a Pork Chop Off the Pig."

The CIP in the San Francisco Office must be re-evaluated. During the reevaluation, give thorough consideration to the adequacy of the personnel assigned. Insure that you are utilizing the best personnel available in this program. Advise the Bureau of the results of your reevaluation by June 9, 1969.

Referenced airtel mentions several specific CIP proposals now pending. Instructions will be furnished pertinent offices by separate communication.

NOTE: San Francisco has furnished an evaluation of the CIP in that office as it affects the BPP. That office is not in line with Bureau objectives in the use of counterintelligence. We are calling attention to their derelictions and point out various situations where they should have proposed counterintelligence. We are calling for a reevaluation of the whole thinking behind counterintelligence in the San Francisco Office.

To: DIRECTOR FBI (100-448006) From: SAC, Jackson (100-980) (P) 12/2/70
II. OPERATIONS BEING EFFECTED III. TANGIBLE RESULTS

Since March, 1968, the Republic of New Africa (RNA) has been attempting to start a separate black nation in five southern states, starting with Mississippi. In this regard, the RNA has been trying to buy and lease land in Mississippi in the Jackson Division on several past occasions. (Counter-intelligence measures has been able to abort all RNA efforts to obtain land in Mississippi.)

In late July, 1970, RICHARD HENRY, aka Brother Imari, leader of the RNA, came to Jackson, Mississippi, accompanied by many out-of-state supporters to hold a national RNA meeting "on the land of the nation in Mississippi". This conference was disruptive and ineffective due to Jackson Division, Bureau-approved counterintelligence measures.

In mid-September, 1970, Brother IMARI and a few close associates of his came to look at land which was for sale in rural Hinds County, Mississippi, near Jackson; this land was owned by a Negro male who was retiring and owned over 560 acres. Jackson informants advised Bureau Agents of developments regarding this land and the fact that the owner of the land, [redacted], N/M, had advised Brother IMARI he will lease or sell him ten to twenty acres. RNA leaders, including Brother IMARI, were delighted over this land purchase or leasing prospect. Jackson informants were directed by contacting Agents to approach [redacted] privately and indicate to him that his selling land to Brother IMARI would not be a wise endeavor. Additionally, on 10/9/70, [redacted] was interviewed by Bureau Agents and advised of the true nature and violence potential of the RNA and its leaders. The interview lasted 1½ hours; following the interview, [redacted] indicated he would reconsider whether he would sell or lease any land to the RNA; on 10/21/70, Bureau Agents interviewed [redacted] who was assisting the RNA in their dealings with [redacted] regarding the land. The true nature and violence potential of the RNA and its leaders was explained to [redacted]

As a result of the above counterintelligence efforts, the land which the RNA had almost finalized plans regarding purchasing or leasing in rural Hinds County, Miss., has not been sold or leased to them. Jackson has maintained contact with [redacted] and he has advised he has no plans to lease or sell any land to the RNA in the immediate future. There have been no recent visits by top officials of the RNA to Mississippi regarding the land, it being noted they made several visits in September, 1970, when their prospects for the land purchase or leasing was good.

As a result of the above, intensive efforts of the RNA to obtain land in Mississippi over the past

Chicago Daily News
12/3/75

Bare Hoover's smear tactic

WASHINGTON (AP) — The late FBI Director J. Edgar Hoover approved a plan to discredit a Midwest black militant leader with anonymous letters accusing him of adultery and of being a bureau informant, according to FBI documents.

The documents, made available by the Senate intelligence committee, show that the bureau's campaign against the Rev. Charles E. Koen lasted from 1968 to 1971 and was approved at each step of the way by Hoover. However, it was unclear whether the letters were ever actually sent to Mr. Koen, who a committee spokeswoman said is a minister in Cairo, Ill.

According to the FBI documents, the campaign against Mr. Koen began in November, 1968, with a proposal by St. Louis FBI officials to send him an anonymous letter criticizing him for referring to the possible use of violence in his public speeches.

THE LETTER would purport to be from members of Students for a Democratic Society in St. Louis and "would have an adverse effect on the consolidatory efforts of the SDS and the Black Liberators," according to the proposal approved by Hoover.

Two months later, Hoover authorized the FBI's Baltimore office to send an anonymous letter to the No. 2 man in the Black Liberator movement informing him that Mr. Koen was working for either the CIA or FBI. The letter, signed "A Soul Brother," said Mr. Koen "was in Baltimore last week and spent most of his time in the Justice Building. Don't know whether that cat was talking to CIA or FBI."

The FBI documents also include a 1969 memo from the head of the FBI's St. Louis office who claims the campaign forced Mr. Koen's resignation as head of the Black Liberators, a black militant group.

IN FEBRUARY, 1969, after Mr. Koen had resigned as head of the Black Liberators, the FBI chief in St. Louis proposed mailing an anonymous letter designed "to alienate (Koen) from his wife and cause suspicion among the Black Liberators that they have a dangerous troublemaker in their midst," an FBI document said.

The anonymous letter would be sent to Mrs. Koen telling her that her husband has "been making it here with Sister Marva Bass and Sister Tony and then he gives us this jive 'bout their (sic) better in bed then (sic) you."

It was to be followed by sending a copy of the anonymous letter to Mr. Koen with the note "I understand she recently received this letter . . . I suggest you look into this matter."

IN A MEMO authorizing the operation, Hoover directed the agents to "use commercially purchased stationery and take the other precautions set out to insure this cannot be traced to this bureau."

The next and final step in the FBI campaign against Mr. Koen came in February, 1971, when Hoover approved a proposal for circulating a cartoon sketch of Mr. Koen that "would emphasize the cost of Mr. Koen's attire and inquire as to the source of his funds."

At that time, Mr. Koen was head of the United Front in Cairo, which, according to the FBI memo, was a "predominately black organization which has been boycotting white merchants in Cairo for the past 20 months."

The plan to send the cartoon was proposed because "it is felt that any diminution of Mr. Koen's support in Cairo would be beneficial since he appears to be the single most important cause of confrontations occurring in Cairo."

St. Louis Post-Dispatch
11/30/75

Cairo Pastor Says FBI Lied To Bishop

By MARTHA SHIRK
Of the Post-Dispatch Staff

The Federal Bureau of Investigation sent an anonymous letter to the ranking bishop of the Episcopal Church of the United States in 1971 in an attempt to discredit the United Front of Cairo, Ill., and to dry up its major source of funds, says the Rev. Charles Koen, the United Front's leader.

He said documents scheduled to be made public this week by the United States Senate Select Committee on Intelligence would disclose a pattern of harassment, including attempts to cause disagreements among the leaders of the Cairo group, provoke marital squabbles and cut off its outside financial support.

He said a committee staff member had traveled to Cairo in recent days and had shown him the letter in question. The staff member, reached by telephone Friday night, refused to comment and would say only that the facts would be disclosed this week.

The Rev. Mr. Koen said the staff member had told him that the FBI had sent an anonymous letter in 1971 to the Right Rev. John E. Hines, then the presiding bishop of the Episcoal Church.

The letter, which was written from the viewpoint of a concerned parishioner, called the United Front a violent organization and said its leaders had used donations from the church to buy weapons, the Rev. Mr. Koen said.

In 1970, the national Episcopal Church donated more than $75,000 to the United Front, a community-based self-help group with branches in East St. Louis and St. Louis. But the Rev. Mr. Koen said in an interview Friday that the church had denied the group a contribution for the next three years.

"And now we know why," he commented.

In 1969, the United Front, headed by the Rev. Mr. Koen, conducted boycotts and demonstrations against white-owned businesses in Cairo in an attempt to force the hiring of more black employes. Racial strife, and often exchanges of gunfire between the white and black communities, continued into the 1970s. The Rev. Mr. Koen, 29 years old, is assistant pastor of Cairo's First Missionary Baptist Church.

30

OCTOBER 23, 1968

CODE

TELETYPE

URGENT

SENT BY CODED TELETYPE

1 - Mr. Sullivan
(Route through
for review)

TO: SACs, CHICAGO
CINCINNATI
CLEVELAND
DENVER
MIAMI
NEW YORK
SAN FRANCISCO

VIA TELETYPE
559 MXS
OCT 23 1968
5:23 PM PAD
ENCIPHERED

1 - Mr. Deily

FROM: DIRECTOR, FBI

DISTURBANCES ARISING OUT OF DEMOCRATIC NATIONAL CONVENTION

ARL

FOR YOUR CONFIDENTIAL INFORMATION, DEPARTMENT PLANS TO SEEK INDICTMENTS IN IMMEDIATE FUTURE CHARGING APPROXIMATELY TWENTY PRINCIPAL LEADERS AND ACTIVISTS OF VARIOUS NEW LEFT ORGANIZATIONS WITH CONSPIRACY TO VIOLATE AND SLASH OR SUBSTANTIVE VIOLATIONS OF ANTIRIOT LAWS PARENTHESIS TITLE EIGHTEEN, SECTIONS TWO FOUR FIVE, TWO ONE ZERO ONE, TWO ONE ZERO TWO OR TWO THREE ONE CLOSE PARENTHESIS IN INSTANT MATTER. A SUCCESSFUL PROSECUTION OF THIS TYPE WOULD BE A UNIQUE ACHIEVEMENT FOR THE BUREAU AND SHOULD SERIOUSLY DISRUPT AND CURTAIL THE ACTIVITIES OF THE NEW LEFT. IT IS THEREFORE IMPERATIVE THAT THE FBI DO EVERYTHING POSSIBLE TO PROVIDE THE ADMISSIBLE EVIDENCE REQUIRED BY THE DEPARTMENT TO PROCEED.

RVD/lrk
(4)

SEE NOTE PAGE SEVEN

100-176410-147

REC-1

19 OCT 24 1968

61 OCT 28 1968

TELETYPE UNIT

The government's right to continue full investigation of AIM and certain affiliated organizations may create relevant danger to a few citizen's privacy and free expression, but this danger must be weighed against society's right to protect itself against current domestic threats.

The Supreme Court has observed that "unless the government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disorderly that all rights and liberties would be endangered." United States v. United States District Court, 407 U. S. 297, 312 (1972).

2. Scope of Investigation

Investigative Techniques

The key to the successful investigation of AIM is substantial, live, quality informant coverage of its leaders and activities. In the past, this technique proved to be highly effective, [redacted] As a result of certain disclosures regarding informants, AIM leaders have dispersed, have become extremely security conscious and literally suspect everyone. This paranoia works both for and against the movement and recent events support this observation. [redacted]

When necessary, coverage is supplemented by certain techniques which would be sanctioned in preliminary and limited investigations.

Physical surveillance is another useful technique and should be utilized when deemed appropriate.

No mail covers or electronic surveillance have been used to investigate AIM and none is anticipated at this time. [redacted]

32

FBI

Date: 1/2/70

Transmit the following in _____ (Type in plaintext or code)

Via AIRTEL AIR MAIL (Priority)

TO: DIRECTOR, FBI (100-449698)

FROM: SAC, HOUSTON (105-2275)

SUBJECT: COUNTERINTELLIGENCE PROGRAM
INTERNAL SECURITY - DISRUPTION
OF THE NEW LEFT

RE: HOairtel, 9/30/69.

I. Potential Counterintelligence Action

Houston Office has during recent months obtained letterhead stationery from the United Farm Workers Organizing Committee, Delano, California, which stationery was being considered for use in a counterintelligence-type letter to the organization in connection with the interest previously shown on behalf of the grape pickers strike by the Houston SDS people. During the recent several months, the SDS group have not expressed any interest in the grape pickers strike as they have previously, and any counterintelligence move utilizing the contemplated letter, would at this time, be inopportune. In the event interest again is generated by the SDS on behalf of the grape pickers strike, a specific proposal will be made.

EX-109 REC-33 100-449698-19

Informants have advised that SDS people in Houston who are currently residing at 5003 Austin are currently selling and using marijuana at this address. Informants stated also that there is a good possibility that the supply of marijuana is kept by one of the individuals living at this address. This information has been related to appropriate narcotics people at the Houston PD and also the Federal Narcotics Bureau in Houston. In the event additional specifics are obtained in this regard, appropriate authorities will be advised in an effort to disrupt the New

1 - Bureau (RM)
1 - Houston
DCS:sm

JAN 5 1970

Approved: _____ Sent _____ M Per _____
Special Agent in Charge

Black Panther 2/4/78

F.B.I.'S MEXICAN COINTELPRO PLAN REVEALED

(Mexico City, Mexico) - The Federal Bureau of Investigation (FBI) conducted an intense campaign of violence, harassment and disruption against activists in Mexico, recently released FBI files have shown.

The Bureau's Mexican activities were similar to the notorious COINTELPRO operations in the U.S., directed against militant Black groups, the antiwar movement and other so-called "subversive" activities. In Mexico, the FBI organized and fomented bombings, shootings, and murder attempts. Bureau agents also worked closely with the U.S. border cops, against both Mexican and Chicano activists.

The campaign was carried out with the collaboration and tacit support of the Mexican government.

The FBI's disruption campaign was the subject of a recent four-part series in the Mexico City daily paper *Excelsior*. The articles were based on FBI files disclosed through the Freedom of Information Act. Virtually none of the files' contents on Mexico has been reported in U.S media, the *Militant* reports.

Excelsior reported that the FBI's activities were stepped up between 1967 and 1970, a period marked by the rise of mass struggles in Mexico.

Many of the documents described by *Excelsior* were confidential memos from then FBI director J. Edgar Hoover to the "legal attache" of the American embassy in Mexico City. The "legal attache" in most American embassies, according to former CIA agent turned Marxist Philip Agee, is in reality the head of the local FBI operation.

Hoover continually stressed that the Bureau's Mexican activities were to be kept top secret — obviously to cover the fact that the FBI, supposedly "restricted" to domestic surveillance, actually carries out illegal operations abroad.

In 1967, *Excelsior* reported, Hoover sent instructions to the FBI in Mexico City to prepare a plan for disrupting "subversive" student groups.

Later in 1967, the FBI head in Mexico's capital received congratulations from Hoover. The chief was "pleased by the wave of nighttime machine gunnings to divide subversive leaders."

These shootings bear remarkable similarity to plans carried out by the FBI in the U.S. to provoke disputes between Black groups that could lead to violence. The Black Panther Party was a prime target of such tactics.

Hoover also congratulated the "legal attache" in Mexico City for the "effective and strategic detonation of bombs" that the FBI had arranged or provoked.

In 1968, according to *Excelsior*, "the terrorist activity of the FBI was intensified as part of a broadening of counterintelligence operations."

Meanwhile, in Mexico, a powerful movement of students and working people demanding release of political prisoners had arisen. The movement frightened the Mexican government —and the FBI. A 1968 memo from Hoover reveals the FBI's infiltration of the movement: "With only 10 men in the demonstration that the radicals (students) are going to hold, it is not sufficient to consummate the plans that have been made," *Excelsior* quotes.

The Mexican government moved quickly to crush the growing movement. On October 2, 1968, a peaceful demonstration of thousands of people at the Tlatelolco Plaza in Mexico City was fired on by police and troops. Hundreds of protesters were killed.

The government minister responsible for the massacre, Luis Echeverria, became the president of Mexico in 1970. Echeverria had been a close contact of the CIA, Philip Agee reported in *Inside the Company*. The FBI continued its close collaboration with the Mexican government under the Echeverria administration, the files show.

A 1971 memo from Hoover tells the FBI's agents in Mexico to "make sure that the disruptions will be carried out by our undercover agents in meetings with subversive students without endangering the life of [name deleted]," *Excelsior* reported, explaining that this was an "indirect reference" to Echeverria.

FBI agents posed as agents of the Immigration and Naturalization Service (INS) to question people who "could be of interest in relation to national security," *Excelsior* quotes one memo.

Stories were planted by agents in border city newspapers urging citizens to inform on sons and daughters of neighbors who might be "subversives."

When mere harassment was insufficient, the FBI resorted to out-and-out frame-ups. One memo admits that U.S. police planted illegal drugs — heroin, cocaine, and marijuana — in the cars of Chicano leaders.

Mexican government agencies routinely collaborated with and turned over information to the FBI □

34

UNITED STATES GOVERNMENT

Memorandum

1 - Mr. Sullivan
1 - Mr. J.J. Casper
1 - Mr. W.M. Felt
1 - Mr. C.D. Brennan
1 - Mr. G.C. Moore
1 -
1 -
1 -
1 -

TO : Mr. C. D. Brennan 1 - Mr. Mohr

DATE: 3/25/71

FROM : G. C. Moore

SUBJECT: COINTELPRO - BLACK EXTREMISTS
RACIAL MATTERS

To recommend 90-day progress letters submitted by 43 offices participating in this program be discontinued.

COINTELPRO is code word for counterintelligence program. By memorandum 2/29/68 the Director authorized submission of 90-day progress letters concerning captioned program for purpose of stimulating thinking in offices where black extremist activities are concentrated. Forty-three offices are currently participating in this project.

This program has as its objectives the neutralization of black extremist groups, the prevention of violence by these groups and the prevention of coalition of black extremist organizations. Since these offices have participated significantly in this program, it is felt we can now relax our administrative procedures by eliminating the 90-day letter. We will not suffer from this discontinuance as continued participation in this program by field is followed by individual Supervisors in Racial Intelligence Section, Domestic Intelligence Division. In addition, the Inspection Division analyzes each office's participation in this program during field office inspections. In view of the above and to streamline our operations, it is recommended these progress letters be discontinued. No change is required in any Bureau manuals.

ACTION: REC-20

If approved, the attached airtel advising of discontinuance of these 90-day letters will be forwarded to offices participating in this program.

Enclosure
100-448006

WHA:sef (11)

APR 1 1971

APR 5 1971

Part Two: Violent Methods and Tactics

FBI counterintelligence employed its most violent and illegal tactics against third world liberation movements, especially the Black Panther Party. They sought to provoke street gangs and other organizations such as the United Slaves organization in Southern California to engage in violence against the BPP. During 1969, four Panthers, including leaders Bunchy Carter and John Huggins, were killed by U.S. members (or FBI provocateurs) in incidents which the FBI helped to provoke and claimed credit for.

In Chicago, the FBI contemplated inciting the Mafia against Dick Gregory, and intentionally provoked Blackstone Ranger leader Jeff Fort in the hope that he would violently "retaliate" against Hampton and other Panther leaders. The Bureau, through their informants, falsely labelled Panthers and other Blacks as informants, although they recognized that this could lead to physical harm. Their most trusted informants, such as William O'Neal and Darthard Perry, acted as provocateurs, encouraging and participating in illegal and violent acts such as robberies, bombings, building electric chairs, and bullwhipping those they branded as informants. Other illegal tactics included forgery, wiretapping, burglaries, unauthorized use of Internal Revenue Service materials, interception of mail, and assassination.

One of their most violent counterintelligence policies was the use of raids on offices and homes of the Black Panther Party and other organizations throughout the country. In June of 1969, the FBI raided several Panther offices across the country, purportedly looking for George Sams, who later turned out to be an FBI provocateur. They would never apprehend him, but they would brand each raid a counterintelligence success after seizing or destroying almost everything in the offices, making bogus arrests, and generally disrupting the BPP.

Later in 1969 the policy changed. The FBI no longer executed the raids themselves, but employed local police forces--already at a fever pitch against the Panthers--to do their dirty work. In Chicago, FBI informant O'Neal obtained a floorplan of Fred Hampton's apartment, showing the bed upon which Hampton slept, which the FBI then gave to Edward Hanrahan's police who assassinated Hampton at 4:30 a.m. while he slept on that very bed. Four days later, in Los Angeles, the FBI passed a floorplan of the Panther offices to 300 L.A. police, who raided the offices in the early morning hours, and pumped thousands of rounds at the Panthers inside, who defended themselves and thereby miraculously avoided death.

In sum, FBI tactics of counterintelligence, as practiced against the Black liberation movement, were, and are, so violent, so unconstitutional, and so illegal, as to make a mockery of the law which the FBI is sworn to uphold.

36

POLICE GIVEN DATA ON BOAST BY ROWE

7/14/78

Reports May Back F.B.I. Informer in Klan on Killing in South

By HOWELL RAINES
Special to The New York Times

BIRMINGHAM, Ala., July 13 — Police sources here said today that they had information that might support Gary Thomas Rowe Jr.'s contention that he killed a black man during racial unrest in Birmingham in 1963, while Mr. Rowe was on the Federal Bureau of Investigation's payroll as an informer within the Ku Klux Klan.

The sources said a former Klansman and another man described as a Klan sympathizer told the police, in separate accounts, that Mr. Rowe had boasted to them that "I shot some niggers" during rioting that followed a double bombing in a black neighborhood.

A Birmingham police officer has also told city investigators that he saw Mr. Rowe with a pistol stuck in his belt near a police barricade like the one described by Mr. Rowe in his account of the killing.

Missing Report Is Sought

The investigators are now combing police files here for a missing report that they believe contains information about at least three unsolved shootings during the 1963 disturbances.

Meanwhile, another document has come to light that may add to the growing controversy over Mr. Rowe's involvement in racial violence while he was getting monthly payments from the F.B.I. In a statement to a Senate investigator in 1975, Mr. Rowe accused John Doar, former Assistant Attorney General for civil rights, of forcing him to change his account of the killing of Viola G. Liuzzo in 1965.

In the interview, Mr. Rowe said that Federal investigators ignored his report that a black man was also killed in Mrs. Liuzzo's car when Mr. Rowe and three Birmingham Klansmen chased down the Detroit woman's automobile on the night after she took part in a civil rights march from Selma to Montgomery. Mr. Rowe further alleged that Mr. Doar ordered him to keep silent when Mr. Rowe told Government prosecutors that he could not positively identify a black man called as a key Government witness as having been in the car with Mrs. Liuzzo at the time of the shooting.

The Liuzzo case brought Mr. Rowe national attention as the F.B.I.'s chief informer against the Klan in Alabama. He was later relocated and given a new identity by the bureau, and lives in an undisclosed location.

Mr. Rowe also told Senate investigators that the Justice Department, under its witness protection program, got him a job with a United States Marshal and allowed him to attend the Department of Justice Training Academy with 90 other Federal officers. Mr. Rowe charged that, because of his dispute with Mr. Doar, he was subsequently forced to resign the job, and that Marshal who employed him filed "false affidavits" in order to get Mr. Rowe an extra month's pay on which to find a job outside the Government.

Questioned in Church Bombing

When the authorities in Alabama reopened their investigations into the unsolved racial killings in the early 1960's, they contacted Mr. Rowe for information on the 1963 bombing that killed four black children at Sixteenth Street Baptist Church. But Mr. Rowe himself became a suspect in that case after two polygraph, or lie-detector, tests showed that he was giving "deceptive" answers when he denied having been with the group that planted the bomb.

Since that time there have been disclosures that indicate that Mr. Rowe may have participated in and helped to plan the Klan violence he was hired to observe.

A former leader of the Ku Klux Klan in Birmingham said today that Mr. Rowe helped direct the attacks on the Freedom Riders at a Birmingham bus station on May 15, 1961.

Mr. Rowe himself said, in an interview with Alabama investigators last fall, that he participated in the firebombing of the home of A. G. Gaston, a black millionaire, according to investigative documents.

In the same series of interviews, Mr. Rowe was quoted as saying he killed a black man during a riot here and was told by the F.B.I. agent to whom he regularly reported to keep quiet about the shooting. The agent named by Mr. Rowe has denied the report as "an absolute falsehood."

According to the Senate document that came to light today, Mr. Rowe said he was assured by F.B.I. agents here that his participation in violence had the personal endorsement of "The Man" — the late J. Edgar Hoover, then Director of the bureau.

'War' on the Klan

Mr. Rowe stated that "the quote to me was 'The Man has declared war on the Ku Klux Klan and that you are man enough to do, do it.' " Mr. Rowe stated that the "agent quivered, literally" in delivering this message and said "we don't have to worry about covering you any more."

The Birmingham Police Department's information about a possible shooting by Mr. Rowe was obtained, sources said, before disclosure by The New York Times that Mr. Rowe had told investigators that such a shooting took place.

The police inquiry here now is focusing on Mr. Rowe's activities after bombings on the nights of May 11 and Sept. 4, 1963. Rioting of the sort described by Mr. Rowe took place on both nights. By the accounts of Mr. Rowe and others, according to investigative documents, Mr. Rowe was in the riot area on both occasions.

Account of Shooting

The documents show that Mr. Rowe told a state investigator that he came upon blacks attacking a taxicab on Eighth Avenue here and beating a woman passenger. When the rioters turned on him, Mr. Rowe is quoted as saying, he shot a black man through the chest. Then, Mr. Rowe is reported to have said, he went to a barricade and reported the shooting to a policeman and later, by telephone, to his F.B.I. "control" agent.

According to an investigative source, a Birmingham policeman has told detectives here that during the riot on May 11, "he came down Eighth Avenue and stopped and got out of his car and Rowe was standing there in the middle of the road in civilian clothes with a gun stuck in his belt."

Later that same night, according to an investigative document, a fellow Klansman saw Mr. Rowe and talked to him at a telephone booth at 3 A.M. "At that time, Rowe stated to him that he had been uptown shooting Negroes," the document stated.

In a separate interview, the companion of the Klansman who gave that report supported the account without prompting, investigative sources here said. Mr. Rowe was quoted as telling the two men: "There's been a bombing. The niggers are rioting. I shot some niggers."

However, the assault on the taxicab described by Mr. Rowe more closely matches an incident that took place on Sept. 4, after the bombings of the A. G. Gaston Motel and the home of the Rev. A. D. King, brother of the Rev. Dr. Martin Luther King Jr.

On that night, Mr. Rowe has told state investigators, he was riding with Birmingham policemen in the riot area when they came upon a taxicab whose driver and a woman passenger were under assault by rioters.

Chicago Tribune

BIRMINGHAM, Ala. [UPI]—A lawyer who defended three Ku Klux Klan members 10 years ago says an ex-FBI informer was involved with his clients in an attack resulting in the murder of civil rights worker Mrs. Viola Liuzzo.

"It was Gary Thomas Rowe who suggested the trip to Lowndes County to kill some of the civil rights workers," said Haynes, a former FBI agent and former Birmingham mayor.

"And we have him on record as saying in the courtroom that he had his gun out the window and was shooting along with the rest of them," he said.

UNITED STATES GOVERNMENT

Memorandum

TO : DIRECTOR, FBI (100-448006)

DATE: 11/29/68

FROM : SAC, LOS ANGELES (157-1751) (P)

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE

Re Los Angeles letter to Bureau dated 9/25/68.

I. OPERATIONS UNDER CONSIDERATION

The Los Angeles Office is currently preparing an anonymous letter for Bureau approval which will be sent to the Los Angeles Black Panther Party (BPP) supposedly from a member of the "US" organization in which it will be stated that the youth group of the "US" organization is aware of the BPP "contract" to kill RON KARENGA, leader of "US", and they, "US" members, in retaliation, have made plans to ambush leaders of the BPP in Los Angeles.

It is hoped this counterintelligence measure will result in an "US" and BPP vendetta.

Investigation has indicated that the Peace and Freedom Party (PFP) has been furnishing the BPP with financial assistance. An anonymous letter is being prepared for Bureau approval to be sent to a leader of PFP in which it is set forth that the BPP has made statements in closed meetings that when the armed rebellion comes the whites in the PFP will be lined up against the wall with the rest of the whites.

It is felt that this type of a letter could cause considerable disruption of the association between the BPP and the PFP.

In order to cause disruption between the BPP of Oakland, California, and the BPP of Los Angeles, an envelope is being prepared for Bureau approval which appears

REC-2

(2) - Bureau (RM)
1 - Los Angeles

LWS/dlc
(3)

38 DIRECTOR, FBI [redacted]

SAC, SAN DIEGO [redacted]

COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
(BPP)

III. TANGIBLE RESULTS

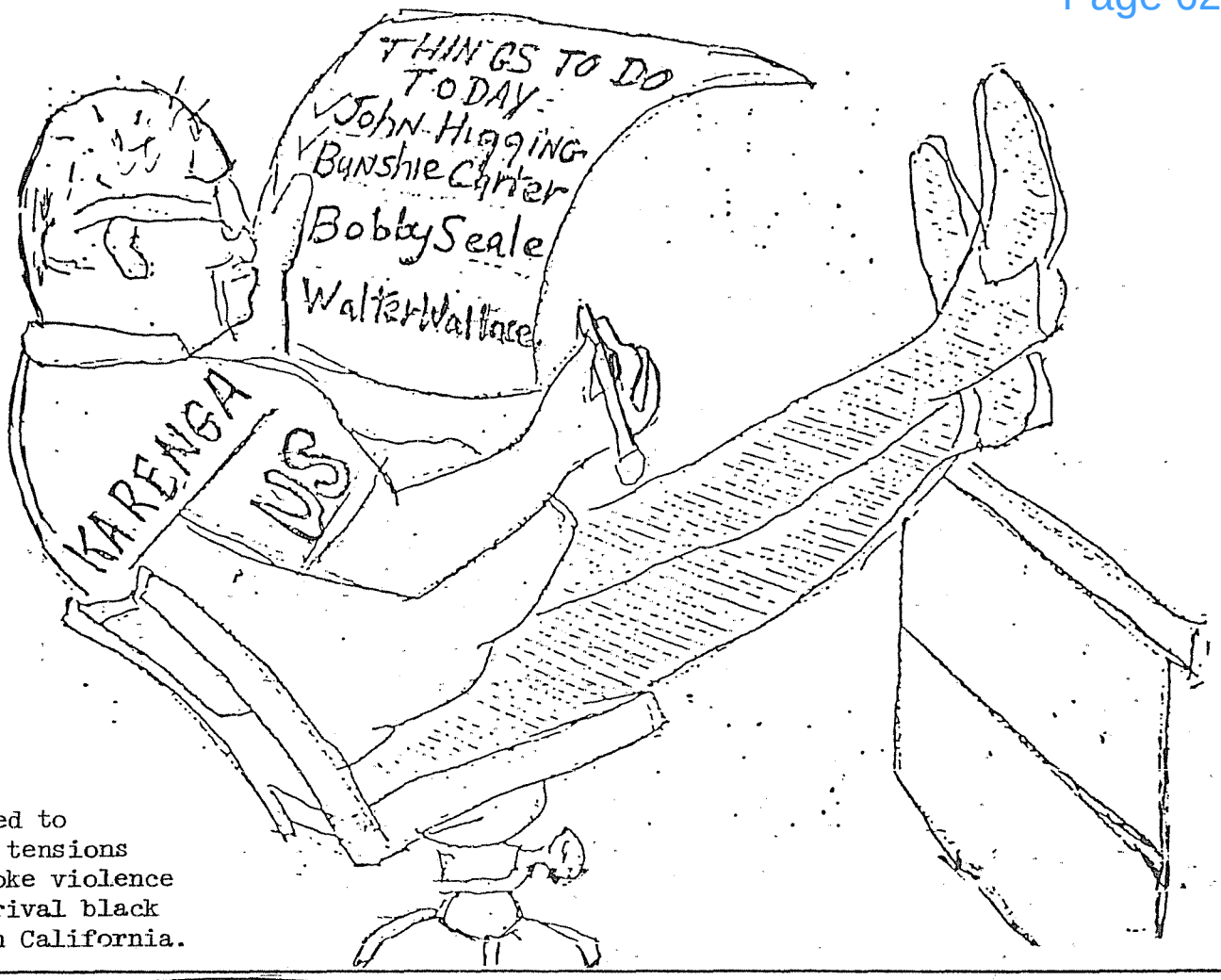
The BPP Breakfast Program appears to be floundering in San Diego due to lack of public support and unfavorable publicity concerning it. It is noted that it has presently been temporarily suspended. Therefore, it was felt that placing the above mentioned anonymous call to the Bishop at this particular time might be a significant factor in precluding the resumption of the program. The information to the Bishop appeared to be favorably received and he seemed to be quite concerned over the fact that one of his Priests was deeply involved in utilization of church facilities for this purpose. This matter, of course, will be closely followed for further anticipated developments concerning the Breakfast Program.

Shootings, beatings, and a high degree of unrest continues to prevail in the ghetto area of southeast San Diego. Although no specific counterintelligence action can be credited with contributing to this over-all situation, it is felt that a substantial amount of the unrest is directly attributable to this program.

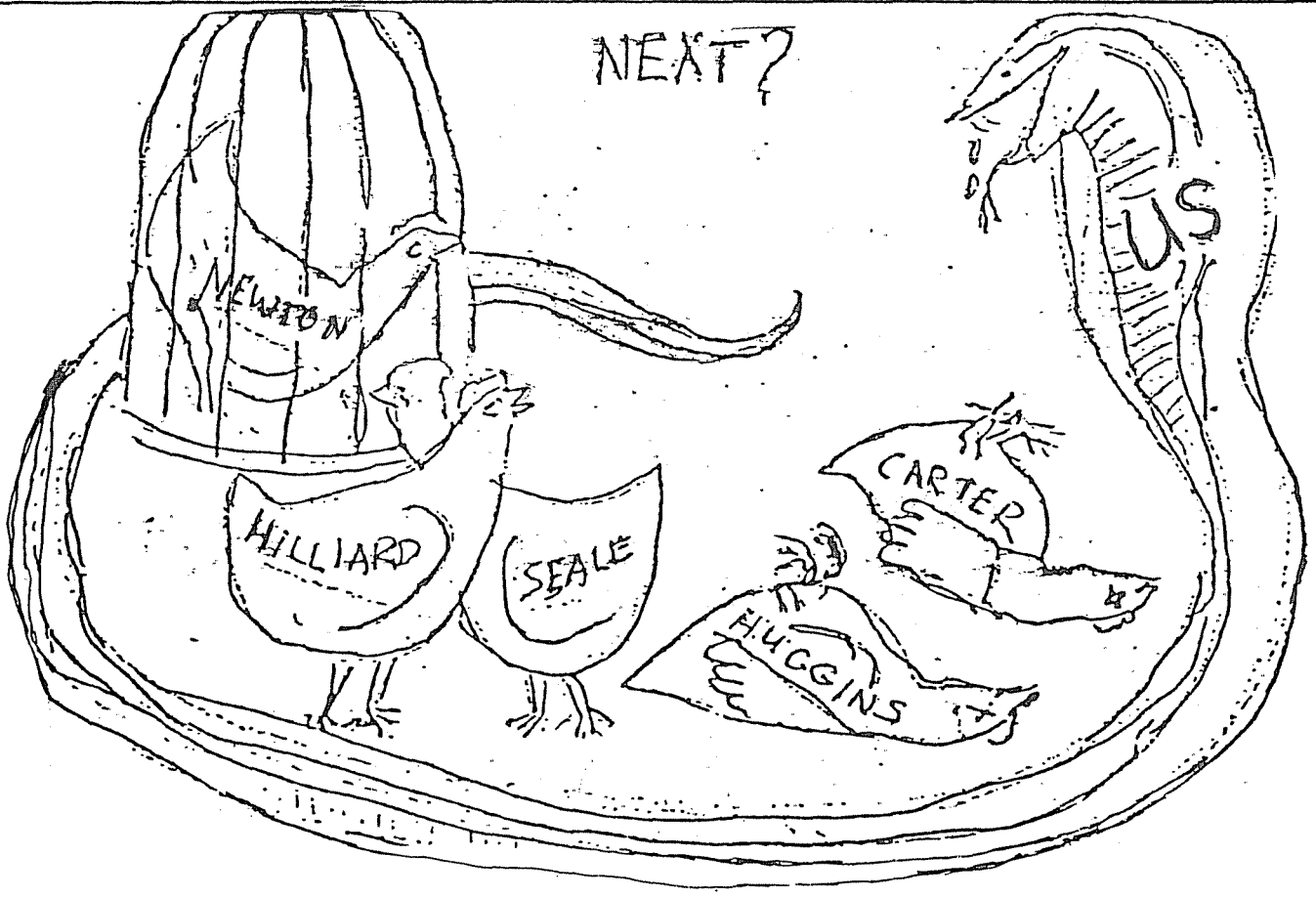
In view of the recent killing of BPP member SYLVESTER BELL, a new cartoon is being considered in the hopes that it will assist in the continuance of the rift between BPP and US. This cartoon, or series of cartoons, will be similar in nature to those formerly approved by the Bureau and will be forwarded to the Bureau for evaluation and approval immediately upon their completion.

IV. DEVELOPMENTS OF COUNTERINTELLIGENCE INTEREST

Due to the fact that the US members violently objected to being called "pork chops", a change in the order of the mailing of the cartoons was made in San Diego. One of the recently Bureau-approved cartoons depicting [redacted] holding a Black Panther off with his hand with the title "Pork Chop Karenga" was distributed on 4/7/69, due to the excellent timely release of this particular cartoon.



o FBI
rtoons
rculated to
crease tensions
d provoke violence
tween rival black
oups in California.



40

UNITED STATES GOVERNMENT

Memorandum

#11

TO : DIRECTOR, FBI

DATE: 1/13/69

FROM : SAC, CHICAGO

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
(BLACK PANTHER PARTY) (BPP)

DO NOT REMOVE

In the Chicago letter of December 16, 1968, a suggestion was made that an anonymous mailing be sent JEFF FORT, leader of the Blackstone Rangers, advising of BPP efforts to discredit him, and in effect to "take over" the Rangers. As events have subsequently developed, as set forth in referenced Chicago airtel and LHM, the Rangers and the BPP have not only not been able to form any alliance, but enmity and distrust have arisen, to the point where each have been ordered to stay out of the others territory. The BPP has since decided to conduct no activity or attempt to do any recruiting in Ranger territory.

It appears therefore that the letter as originally intended at this point would serve no useful purpose. The end in view appears to have been very quickly arrived at, in great measure by virtue of the inherent inability of two such volatile and power conscious groups to derogate any of their status or assumed authority to the other.

From information recently received, it appears, however that the BPP has not entirely abandoned all hope of utilizing the Rangers for their own purposes. Some feeling has been evident that FORT may not continue indefinitely in his position of leadership with the Rangers, most probably a reference to various criminal charges facing him. It is clear, however, that so long as he is in this position, any working arrangement between the two groups will be on Ranger terms.

JCS/vrg

ATTORNEY'S COPY

Consequently, Chicago now recommends the following letter be sent FORT, handwritten, on plain paper:

"Brother Jeff

"I've spent some time with some Panther friends on the west side lately and I know what's been going on. The brothers that run the Panthers blame you for blocking their thing and there's supposed to be a hit out for you. I'm not a Panther, or a Ranger, just black. From what I see these Panthers are out for themselves not black people. I think you ought to know what their up to, I know what I'd do if I was you. You might hear from me again."

"A black brother you don't know"

The above would be sent to FORT in care of the First Presbyterian Church, 6401 South Kimbark, the widely publicized headquarters of the Rangers.

It is believed the above may intensify the degree of animosity between the two groups and occasion FORT to take retaliatory action which could disrupt the BPP or lead to reprisals against its leadership.

Consideration has been given to a similar letter to the BPP, alleging a Ranger plot against the BPP leadership however, it is not felt this would be productive, principally since the BPP at present is not believed as violence-prone as the Rangers, to whom violent type activity, shooting, and the like, are second nature. There is also the possibility that if a future contact between the two were to take place, and it became apparent that both had received such communications, then an outside interest would be somewhat obvious.

Chicago will take no action regarding the above, pending Bureau authorization.

42

CHICAGO SUN-TIMES, Thurs., Feb. 12, 1976

Bob Greene

Laundered box score?

No hits, no guns, no terror

We appear to have a new definition for a time-honored Chicago term.

Marlin W. Johnson, former head of the Chicago FBI office, testified in federal court this week, and he was asked to define the words "a hit."

The reason Johnson was asked to do this was that Jeff Fort, the leader of a Chicago street gang, received a letter back in 1969 that said, "there is supposed to be a hit out for you."

The letter was intended to convince Fort that the "hit" was being ordered by members of the Black Panther Party. Recently uncovered evidence, however, has indicated that the letter was written not by Black Panthers — but by FBI agents, in an effort to turn black nationalist groups against each other.

SO JOHNSON WAS on the stand to testify about the FBI's role in the sending of the letter to Fort. Johnson admitted that he had once approved the mailing of the letter. But he denied that Fort should have construed the phrase, "there is supposed to be a hit out for you," to mean that Fort was in danger of foul play.

Johnson said that "a hit" — according to newspaper accounts of his testimony — was "something nonviolent in nature."

Now I may not have been raised in the big city, but I grew up watching The Untouchables on television just like everyone else, and I was pretty sure that "a hit" did not precisely mean "something nonviolent in nature."

Still, I didn't want to trust myself on this. So I went to a reference book call "The Dictionary of American Underworld Lingo" (Citadel Press, New York, 1962) and looked up the definition. It was brief and to the point:

"HIT — To shoot to kill."

Marlin Johnson had been a top FBI man, though, and I didn't want to rely on the say-so of one not very well-known book to call him wrong. So I got on the telephone and sought the advice of a number of experts in the field. I asked each of them, "Does a 'hit' mean something nonviolent in nature?" Here are their responses:

PETER MAAS, author of "Serpico" and "The Valachi Papers" — A hit means only one thing. It means a bullet in the back of the head. Nonviolent? Jesus Christ. Joe Valachi talked about 33 hits to me, and he wasn't referring to Broadway plays."

STEVE SCHILLER, executive director of the Chicago Crime Commission — "A hit means something very violent. A hit means being taken care of completely. A hit means somebody being exterminated. Taken out. Murdered. Killed. Dead. Final."

JAY ROBERT NASH, veteran crime-watcher and author of "Bloodletters and Bad Men"—"A hit has only one meaning, and that's assassination. That's all it is: planned, ordered-in-advance murder. Usually the weapon is a handgun. Often a silencer is used."

TONY PELLICANO, private eye—"A hit means that a contract is out. A hit means you're going to die. A hit means that your life has been offered up for sale by whoever wants to get you. It's not a very difficult concept. If there's a hit out on you, that simply means that someone has been hired to kill you."

GEORGE V. HIGGINS, former federal prosecutor in Boston and author of "The Friends of Eddie Coyle"—"What did you say? A hit is 'something nonviolent in nature'? That's a lot of crap. It was never like that in any parlance I ever heard. A hit has always meant one thing. It's a contract for murder. There's no two ways about it. It's murder."

RONALD EWERT, acting executive director of the Illinois Legislative Investigative Commission (formerly the Illinois Crime Commission)—"A hit's a hit. A guy's going to get killed. When someone says that there is a hit out for you, he means that the plans are for you to be dead soon."

So . . . I am certainly not going to quarrel with G-Man Johnson's definition of "a hit." In fact, I kind of like it. It adds yet another note of distinction to our civic history:

Only in Chicago can premeditated murder be defined as a nonviolent act.

Attached is a detail of the address at 2337 West Monroe Street, first floor apartment, as furnished by WILLIAM ONEAL on November 19, 1969, which information was orally furnished to the Chicago Police Department and Illinois State Attorney's Office:

SAC, CHICAGO

SA ROY MARTIN MITCHELL

BLACK PANTHER PARTY
RM-BPP

DATE: 11/21/69

43

44

12/11/69

AIRTEL

TO: DIRECTOR, FBI [redacted]

FROM: SAC, CHICAGO [redacted]

SUBJECT: [redacted]

Re Bureau airtel 12/8/69 and Chicago letter 11/24/69.

Information set forth in Chicago letter and letterhead memorandum of 11/21/69, reflects legally purchased firearms in the possession of the Black Panther Party (BPP) were stored at 2337 West Monroe Street, Chicago. A detailed inventory of the weapons and also a detailed floor plan of the apartment were furnished to local authorities. In addition, the identities of BPP members utilizing the apartment at the above address were furnished. This information was not available from any other source and subsequently proved to be of tremendous value in that it subsequently saved injury and possible death to police officers participating in a raid at the address on the morning of 12/4/69. The raid was based on the information furnished by informant. During the resistance by the BPP members at the time of the raid, the Chairman of the Illinois Chapter, BPP, FRED HAMPTON, was killed and a BPP leader from Peoria, Illinois, was also killed. A quantity of weapons and ammunition were recovered.

It is felt that this information is of considerable value in consideration of a special payment for informant requested in re Chicago letter.

[redacted]
1 - Chicago

RTP:pas

SEARCHED
SERIALIZED
INDEXED
FILED

[redacted]

FBI memo on Panthers bared

Charge FBI 'plot' to risk police lives

By Thomas J. Dolan/CST 1/17/76

Lawyers for families of two slain Black anther Party leaders Friday subpenaed FBI ocuments they say outlined an FBI plan to sk the lives of local police in clashes and ids involving Panthers.

"We have a reliable informant," said attorey G. Flint Taylor, "who has told us that ch a plan existed and he saw it in writing. e are demanding that those documents be ought into court."

Taylor made his comment after serving bpenas on four Federal Bureau of Instigation agents, or former agents, three of om are facing civil charges that they vioed the civil rights of Panther leaders Fred mpton and Mark Clark during a Dec. 4, 9, weapons raid on a West Side Panther artment. Hampton and Clark were killed in raid.

The subpenas demand all documents showan alleged FBI counterintelligence plan to or entice local law enforcement agencies neutralize the Black Panther Party. The penas said the plan:

". . . set (s) forth that local law enforcement agencies (are) to be employed by the FBI to raid Black Panther Party offices and homes wherein Panthers and police would be wounded and killed and Panthers arrested . . ."

The plan, according to the subpena, was drafted between January, 1963, and December, 1970. Sources close to the case said the existence of the plan has been made known to a U.S. Senate committee investigating the Hampton and Clark case, but Senate officials could not be reached for comment.

Sources close to the Hampton and Clark lawyers said the plan is being sought to show that the FBI intended that police should be killed or wounded in clashes with armed Panthers to publicly discredit the militant blacks.

Subpenaed were Marlin Johnson, former special agent in charge of the Chicago FBI office, and agents Roy Mitchell and Robert Piper. All are charged in the $47.7-million federal civil rights damages suit being tried before U.S. District Court Judge Joseph Sam Perry.

Panther raid 'success'--agent

4/30/76 Chicago Sun Times

y Dennis D. Fisher

FBI agent testified rsday that he considered police weapons raid on a ago Black Panther apart- t "successful" because no e were injured.

bert T. Piper, head of the s Chicago "racial matters d" at the time of the pre- raid Dec. 4, 1969, told a jury and U.S. District t Senior Judge Joseph Perry that information lied to local police by the was the key to the success e weapons search.

er, a defendant in a $47.7- on civil rights damage filed by the families of ton and Clark and other ants of the apartment, uestioned about a letter he wrote to FBI headquarters in Washington.

The one-page letter credited FBI undercover informant William M. O'Neal Jr. with providing a list of weapons and a detailed floor plan of the Panther apartment, including the exact location of Hampton's bed, which contributed to the saving of police lives. The letter was read to the six-member jury.

"It is felt that this information (O'Neal's) is of considerable value in consideration of a special payment for informant . . . ," the letter said. The local FBI office was seeking a $300 "reward" payment for O'Neal, who acted as the Chicago Panther's chief of security and sometimes as a per-

Piper conceded that he wrote the letter to obtain a bonus for O'Neal.

The raiding party had been supplied the apartment diagram by another FBI agent, Roy M. Mitchell, who was O'Neal's "operator."

(Panther leaders Fred Hampton and Mark Clark were shot and killed by Chicago police assigned to the state's attorney's office, who conducted the weapons search at 2337 W. Monroe.)

CST 2/28/76

By Dennis D. Fisher

A document that showed the FBI knew of an impending police action against a Chicago Black Panther apartment surfaced Friday in federal court.

The document was a bureau report initialed by Marlin W. Johnson, chief of the Federal Bureau of Investigation office here at the time.

Chicago police officers conducted a raid on the Panther apartment Dec. 4, 1969, the day after the FBI report was dated.

Johnson, now an executive with the Canteen Corp. and chairman of the Chicago Police Board, has testified that the first he heard of the weapons raid on the apartment was on radio the morning it happened.

In earlier testimony Johnson denied any knowledge that Chicago policemen assigned to the Cook County state's attorney's office planned the predawn raid in which Panther leader Fred Hampton and member Mark Clark were killed.

The FBI report was read to a jury and U.S. District Court Judge Joseph Sam Perry. The report dealt with an FBI counterintelligence program aimed at harassing and neutralizing "black nationalist-hate groups" that included the Black Panther Party.

Dated Dec. 3, 1969, the three-page report noted that the Chicago FBI office has "continued to advise local authorities of instances where BPP members appear vulnerable to arrest on local charges."

The report recites how the FBI gave information concerning weapons "reportedly purchased legally by local BPP members. This information has been furnished to local law-enforcement officials. Officials of the Chicago Police Department have advised (the FBI) that the department is currently planning a positive course of action relative to this (weapons) information."

Sun-Times Bureau 5-9-76

WASHINGTON — A Federal Bureau of Investigation memo says the 1969 raid in which two Black Panthers were killed in Chicago was "based on information" from an FBI informer, a Senate intelligence committee staff report disclosed Thursday.

Arthur Jefferson, head of the staff that produced the report, said the memo was "inconsist-

by former Cook County State's Atty. Edward V. Hanrahan, Chicago police and the FBI.

Jefferson said the Chicago raid was part of a nationwide FBI effort to "encourage police to raid the Panthers." The FBI justified the policy as a precaution against violence, he said, but "the real reason was they didn't like the political rhetoric and the political stance the Black Panther Par-

46 COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUP
RACIAL INTELLIGENCE
(BLACK PANTHER PARTY) (BPP)

TO : DIRECTOR, FBI 4/11/69
FROM : SAC, CHICAGO

Above is furnished for the information of the Bureau, and an indication of the use of this source in harassing and impelling the criminal activities of the BPP locally.

Explosives offer to Panthers told

CDN 7/2/76

By Rob Warden

A paid FBI informant offered explosives to members of the Black Panther Party here in 1969 and suggested they could blast their way into armories to seize weapons, according to a sworn statement filed Thursday in federal court.

The statement details testimony that former Panther Louis Truelock would give if he were permitted to testify in a landmark civil rights suit before U.S. District Court Judge Joseph Sam Perry.

Truelock would testify that in October, 1969, he and other Panthers went with FBI informant William O'Neal Jr. to the home of O'Neal's father on the West Side, the statement said.

THERE, ACCORDING TO THE statement, O'Neal showed the Panthers a satchel of putty, blasting caps and several plastic bottles of liquid, presumably high explosives.

"He said armories could be blown up this way and we could get their guns," Truelock's statement said.

The next month, the statement continued, Truelock and other Panthers again went to O'Neal's father's home, near 14th and Springfield.

"O'Neal showed us the explosives again and said there was a McDonald's we would rip off," Truelock was quoted as saying. "He (O'Neal) stated we could use the explosives on the safe door and blow it open."

The statement also said that O'Neal once tried to bring an apparently stolen electric typewriter into Panther headquarters at 2350 W. Madison.

Tell torture by FBI spy

Chicago Daily Defender 7/21/76

By ROBERT McCLORY

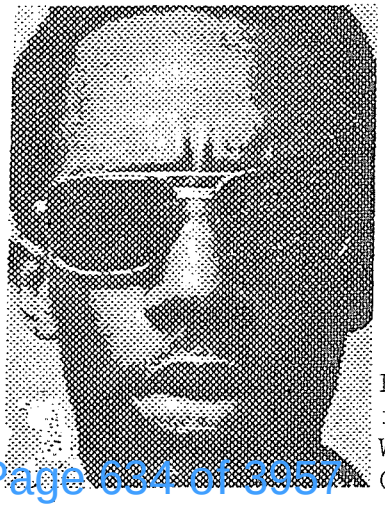
William O'Neal, the Black Panther double agent who helped arrange the 1969 raid on Fred Hampton's apartment, also had plans to blow up City Hall with a bomb carried in a radio-controlled model airplane, a witness testified this week before U.S. District Judge Joseph Sam Perry.

Ronald (Doc) Satchel, who was shot five times during the raid, said O'Neal's elaborate devices, including the plane and a home-made electric chair he built to "punish traitors," led the Panther high command in early 1969 to suspect him of being an agent provocateur. They voted to strip O'Neal of his position as chief of security, said Satchel, but decided not to oust him from the party — a decision which was eventually fatal for Hampton and Mark Clark.

Throughout 1969 O'Neal continued to feed the FBI with information about Panther weapons and security measures, finally triggering the Dec. 4 raid.

During his questioning of Satchel, Atty. James Montgomery, representing survivors of the raid, attempted to establish that much of O'Neal's information was blatantly false. Over the strenuous objections of attorneys representing O'Neal, Edward Hanrahan and 27 other men implicated, Montgomery asked Satchel about a report submitted in late 1968 by O'Neal's FBI contact, Roy Mitchell. In it, O'Neal claimed Panther headquarters at 2350 W. Madison were then equipped with devices to "electrocute unwanted intruders instantly" and to eject poison gas that "kills in a matter of seconds." O'Neal also told Mitchell that a bullet-proof steel door was in place and the windows were equipped with siren-alarms.

In fact, testified Satchel who frequented Panther headquarters daily, he never saw any of these devices. The airplane and the electric chair were real, however. Satchel said the Panthers never took seriously O'Neal's claim that the one-foot-long, plastic airplane equipped with a gasoline motor could actually blow up City Hall, and he never saw it in operation. Hampton, he said, explicitly ordered O'Neal to dismantle the electric chair after it has been constructed.



FBI informer William O'Neal

CDD 3/5/77

William O'Neal, the central figure in the Black Panther trial, engaged in terrorism, torture, robbery and theft, while he was collecting thousands of dollars from his FBI employers, a witness testified this week in the continuing federal trial.

Robert Bruce, 29, a former Panther himself, described many of O'Neal's peculiar projects, including the construction of a Panther electric chair to execute "traitors" and the designing of a radio-controlled model airplane to bomb City Hall. He also said O'Neal encouraged Panther members to commit crimes, personally took part in several burglaries and holdups, and viciously beat one suspected informant with a bullwhip.

The prosecution contends O'Neal was encouraged by his FBI superiors to discredit the party and justify the fatal raid.

Bruce, who was moved by the FBI to California three years ago following his testimony in the Stanley Robinson trial, said O'Neal contacted him last year and urged him not to appear in the Panther trial.

Charge FBI informer was 'hit man

By William J. Eaton
Of Our Washington Bureau

WASHINGTON — An FBI informer in the Black Panther Party in Chicago became part of a "murder-by-contract group" with apparent approval of FBI officials, a member of the Senate intelligence committee has charged.

The informer supplied the Panthers with weapons, trained them in their use and later joined a murder squad that stalked a victim and killed him, according to Sen. Walter D. Huddleston (D-Ky.).

Although Huddleston did not name the informer, he apparently is William O'Neal, a former FBI informer who was chief of security for the Chicago Panthers when Illinois Panther leaders Fred Hampton and Mark Clark were killed in a police raid six years ago.

O'Neal also testified for federal prosecutors in the 1973 trial of former Chicago policeman Stanley Robinson, who was convicted of murdering two persons. O'Neal testified that he accompanied Robinson when a contract killing was carried out on May 6, 1972, on the Dan Ryan Expressway.

Huddleston asked why the Chicago informer was able to provide weapons to the Panthers and associate with killers "presumably all with the knowledge of the FBI."

JOSEPH Deegan, chief of the FBI section on extremist organizations, did not challenge the senator's recital of the facts.

Chicago Daily News 12/3/75

Panther witnesses tell threat by O'Neal

Chicago Daily Defender 12/15/76

By ROBERT McCLORY

Two former Black Panthers have claimed William O'Neal warned them it would not be in their "best interests" to testify at the current federal trial.

The two, Robert Bruce and Nathaniel Junior, said they were contacted separately by O'Neal, the FBI informant who is now in his third week on the stand, and told to "forget about" unrequested visits O'Neal paid them last April. He also allegedly discouraged their scheduled appearances in the trial. As a result of these contacts, Junior and his family are reportedly in fear for their lives and are seeking to keep their present whereabouts unknown.

Bruce and Junior, former associates of O'Neal, have long criminal records, and are prepared to testify about O'Neal's own criminal history. Attorneys for the Panther plaintiffs believe their testimony would seriously discredit O'Neal's claim before the jury that he served as a paid informant only because he was "interested in law enforcement and what the FBI stood for."

Junior, in particular, has charged O'Neal with building an electric chair to scare Panther traitors, organizing groups to conduct robberies, bringing explosives and guns to Canada while Junior was a fugitive there, blowing up a car in suburban Argo, and urging other Panthers to engage in terrorist activities.

Meanwhile, O'Neal has admitted little under heavy questioning by Atty. Jeff Haas. He said his only purpose as an informant was to provide FBI agent Roy Mitchell with "general information" about Panther activities. The plaintiffs, however, are attempting to establish that O'Neal was paid by the government to act as an "agent provocateur" in the party, to encourage illegal acts and to provide justification for a crackdown on its leaders. This theory has gained considerable credibility in view of official FBI documents which urge agents to promote disruption by a host of illegal dirty tricks and the use of informers.

Fred Hampton: Gunned down at dawn by Chicago Police using information given to them by FBI informant and agent-provocateur William O'Neal.

Panther trial

New Times 2/18/77

When William O'Neal recently took the witness stand in the $47.7 million civil suit filed by survivors of the 1969 Chicago police raid, in which Black Panther leaders Fred Hampton and Mark Clark were slain; a chant of "pig, pig, pig" arose from the plaintiffs' side of the courtroom.

In 1969-70, O'Neal earned $30,000 as a paid FBI informant who so successfully infiltrated the Panthers that he became Fred Hampton's personal bodyguard. It was O'Neal who provided the FBI with a floor plan of Hampton's apartment, a plan that the 14-man police unit referred to when surprising the sleeping residents at dawn with a nine-minute spray of gunfire. An autopsy revealed abnormally high levels of barbiturates in Hampton's blood; the plaintiffs believe that O'Neal drugged Hampton the night before the raid. FBI documents in evidence show that O'Neal was rewarded for his efforts with a $300 bonus.

After three earlier "official" investigations of the raid, during which neither he nor the FBI was even mentioned, O'Neal is back on the government payroll, this time earning about $3,000 a month to testify in his own defense. (Other defendants in the case include the FBI, the Chicago police department and the Illinois State Attorney's Office.) The payments, which started in September 1975—on the day he served his deposition in the case—are for "subsistence," O'Neal says.

Though able to subsist comfortably on his government salary, O'Neal did have some uncomfortable moments during his six weeks of testimony. While being questioned about the floor plan and his request to be a pallbearer at Hampton's funeral, O'Neal disappeared during a lunch recess last December 8 and didn't turn up again for five days. The defense explained that his wife was ill, but upon returning, O'Neal failed to bring the medical note that the plaintiffs' attorneys had requested. Although the plaintiffs believe that O'Neal was really holding out for more government money, Judge Joseph Sam Perry would not permit them to question O'Neal about his absence, ruling that to do so would violate security—O'Neal's location is a well-kept government secret.

48 Chicago Tribune, Friday, June 27, 1975

Nation

Report to senators

FBI is accused of plotting terror

New York Times News Service

SAN DIEGO—The American Civil Liberties Union completed Thursday a report for Senate investigators alleging that the Federal Bureau of Investigation recruited a band of right-wing terrorists and supplied them with money and weapons to attack young antiwar demonstrators.

The 5,000-word account prepared for the Senate Select Committee in Intelligence contains what ACLU lawyers described as "newly established evidence" purportedly linking the FBI to at least two assassination plots here.

The lawyers, H. Peter Young and Mark D. Rosenbaum of the ACLU Foundation of Southern California, said the allegations to be sent, probably Friday, to the Senate committee "document in detail" the FBI's sponsorship in 1971 and 1972 of a San Diego group calling itself the "Secret Army Organization."

TOLD OF THE ACLU assertions, a spokesman for the FBI said that the bureau had had "nothing to do" with the establishment of the so-called Secret Army Organization, "nor did we have anything to do with the direction of its activities."

According to the ACLU report, the Secret Army Organization was set up "on instructions of FBI officials" to serve as agents provocateurs, inciting disorders as a means of exposing "domestic radicals," particularly campus leaders of the New Left protesting the war in Southeast Asia.

The organization was described by the ACLU as an outgrowth of an elaborate interagency espionage apparatus organized "at the direction of Richard M. Nixon" early in his administration to intimidate and silence domestic critics.

THE ACCUSATIONS contained in the report go considerably beyond those of a $10.6-million damage suit filed by ACLU attorneys in Federal District Court here last Jan. 6 on behalf of Peter G. Bohmer, a discharged economics professor at San Diego State University, and Paula Tharp, a companion.

Miss Tharp was wounded on Jan. 6, 1972, when shots were fired into Bohmer's Ocean Beach home here from an automobile carrying several members of the so-called Secret Army.

Bohmer, an avowed Marxist, and Miss Tharp, formerly employed by an underground newspaper twice wrecked in nighttime Secret Army raids, organized the San Diego Convention Coalition in mid-1971. The coalition was formed to bring thousands of youthful demonstrators to San Diego to disrupt the 1972 Republican National Convention before the convention site was shifted to Miami Beach.

THE ACLU report says that John Rasperry, whom it identified as an FBI informer, has admitted that, in the winter of 1971-1972, the bureau instructed him to assassinate Bhomer, but that the attempt was neved him to assassinate Bohmer,

Another FBI-directed plot to assassinate Bohmer was allegedly set up in April, 1972, with Gil Romero, a member of the San Diego Police Department's antisubversive "Red Squad," also described as an FBI undercover agent.

The plot was abandoned, Young reported, presumably when the Republican convention was moved to Miami Beach.

By JOHN M. CREWDSON
Special to The New York Times

WASHINGTON, Jan. 11 — Clarence M. Kelley, the director of the Federal Bureau of Investigation, denied today that his agency had played a significant role in financing or encouraging the activities of a group of right-wing San Diego terrorists known as the Secret Army Organization.

Despite Mr. Kelley's insistence today that the F.B.I. "did not sponsor, did not engage in and did not condone" any of the Secret Army Organization activities, information has been placed on the public record or gathered by the Senate Select Committee on Intelligence that shows substantial F.B.I. involvement with the San Diego groups.

Testimony on F.B.I. Funding

Howard B. Godfrey, the F.B.I. informat to whom Mr. Kelley referred, who was also one of the co-founders of the Secret Army Organization, has testified in a California court that the bureau gave him $10,000 to $20,000 worth of weapons and explosives for use by the group in addition to his $250-a-month salary as an informat.

In addition, a report by the American Civil Liberties Union, provided to the Senate committee last summer, quotes John Rasperry, a second F.B.I. informat, as alleging that bureau agents ha instructed him to kill Peter Bohmer, a San Diego economics professor and radical activist, but that he had

However, according to court testimony, members of the secret group, including Mr. Godfrey, did carry out such a murder attempt on Jan. 6, 1972, when they fired a pistol through the front window of Mr. Bohmer's San Diego home.

Mr. Godfrey said that he did not fire the pistol but that he was in an automobile with the men who did. Mr. Boehmer was unhurt, but Paula Tharp, a friend, was wounded in the elbow.

Senate committee investigators have discovered, according to sources familiar with their inquiry, that the pistol in question was later given by Mr. Godfrey to his controlling F.B.I. agent, Steven Christiansen, a member of the bureau's San Diego office.

Committee sources said that Mr. Christiansen concealed the weapon in his own home for half a year while the San Diego police searched for evidence in the Tharp shooting.

The sources said that Mr. Christiansen, who has since resigned from the bureau, was disciplined in some undescribed way by the F.B.I. for his handling of the secret group.

Part Three: Other Methods and Tactics

The FBI used over two hundred tactics against liberation and progressive groups during its counterintelligence program. A partial list includes: anonymous mailings of fictitious letters; exploiting hostility between groups; spreading malicious rumors; manipulating media; pressuring employers to fire progressive employees; engineering the cancellation of speaking engagements; arranging for local police to set-up or harass groups and their members; intimidation through frequent interviews and investigations; and having the Internal Revenue Service conduct illegal tax audits.

One tactic closely related to the illegal raids mentioned in the previous section was the use of false arrests and prosecutions. This was done either by the FBI acting alone or with the cooperation of local police and prosecutors, as well as representatives of the Justice Department. During the summer of 1967, almost the entire RAM organization in Philadelphia was falsely arrested and kept in jail through the counterintelligence efforts of the FBI and the Philadelphia Police Intelligence Unit.

Often, a contemplated result of the raid would be arrest and prosecution, whether there was any real evidence or hope of conviction. There were one hundred and thirteen arrests of BPP members in Chicago in 1969, with no more than a handful of convictions resulting. In Mississippi, in 1971, the police and the FBI raided an RNA home under very suspicious circumstances. Although he was not even in the building, RNA leader Imari Obadele was charged with conspiracy and sent to the penitentiary.

The use of FBI informers and agents-provocateur was, and is, widespread, but the FBI also attempted to spread rumors that certain respected and influential progressive leaders and group members were FBI or CIA spies. This tactic led to much divisiveness and even a potential for violence within several liberation groups.

The FBI also printed its own leaflets with false or malicious information. The FBI was very successful in using the media to discredit and slander activists and liberation struggles. Many "friendly" media sources were little more than pro bono FBI agents themselves, printing or broadcasting whatever the FBI requested. The FBI even supplied pre-written feature articles and screened television documentaries for "accuracy." Like so much of their broadly illegal political repression activities, this media manipulation continues today in a less overt form, adjustments having been necessary due to the damaging revelations exposing the FBI's illegal Cointelpro operations.

50

UNITED STATES GOVERNMENT

ROUTE IN ENVELOPE

Memorandum

1 - Mr. C. D. DeLoach
1 - Mr. W. C. Sullivan

TO : Mr. W. C. Sullivan

DATE: May 14, 1970

1 - Mr. T. E. Bishop
1 - [redacted]
1 - [redacted]

FROM : G. C. Moore

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE

This is to recommend that the Counterintelligence Program against black extremists be continued.

The Counterintelligence Program against black extremist organizations and individuals was initiated August 25, 1967, and on March 4, 1968, it was expanded from 27 to 42 participating field divisions. The goals of this program are to prevent violence by black extremists, to prevent the growth and/or unification of extremist groups, and to prevent extremist groups from gaining respectability in the Negro community. Some of the excellent results of counterintelligence action during the past year are set out below:

To create friction between Black Panther Party (BPP) leader Eldridge Cleaver in Algiers and BPP Headquarters, a spurious letter concerning an internal dispute was sent Cleaver, who accepted it as genuine. As a result, the International Staff of the BPP was neutralized when Cleaver fired most of its members. Bureau personnel received incentive awards from the Director for this operation.

To show the criminal nature of the BPP a write-up concerning the convictions of its members was prepared and received publicity in a Robert S. Allen and John A. Goldsmith syndicated column of March 31, 1970. Previously we exposed the BPP Breakfast For Children Program in these writers' column of June 14, 1969.

Articles concerning the BPP based on information furnish a news media source in Mississippi resulted in the closing of a BPP Chapter in Cleveland, Mississippi.

Counterintelligence action against other extremist organizations has also been effective. In San Diego, California, an anonymous telephone call to the landlord of the US organization resulted in the group being evicted from its Headquarters. In Miami Florida, a television source was helped in the preparation of a program exposing the Nation of Islam. The excellent results of this program were contained in a memorandum from G. C. Moore to Mr. William Sullivan, October 21, 1969, on which the Director noted "Excellent."

100-448006
TJD:mbm
97 JUN 10 1970

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE.

CONTINUED - OVER

25 JUN 5 1970

Memorandum to Mr. W. C. Sullivan
Re: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
100-448006

Counterintelligence action has also been effective against individual black extremists. In St. Louis, the circulation of a spurious newsletter caused four extremists to begin fighting among themselves. An anonymous letter to a radio station caused the removal of [redacted] from the show where he had been preaching black extremist philosophy. The Jackson Division prepared a spurious letter from a college group to a black extremist who was attempting to recruit the group. As a result, the extremist left the area, severing all contact with the group.

ACTION:

In view of the tangible results evidenced by this program with a minimum expenditure of manpower, it is recommended the Counterintelligence Program be continued.

52

UNITED STATES GOVERNMENT

Memorandum

TO : Director, FBI

DATE: 8/30/67

FROM : SAC, Philadelphia (157-2371)

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
INTERNAL SECURITY

Re Bureau airtel to Albany dated 8/25/67.

The following suggestions are presented for general consideration:

I. RAM

This division during the summer of 1967 has had the opportunity to observe an attempt by an extremist Negro group (RAM) to affect the peace of a city. Some of the steps taken against RAM may be of possible use elsewhere under the current program. It is pointed out that in a fast moving series of situations, the police may have to "play it by ear," which may reduce Bureau control of the action taken. Actions herein set out were carried out by either the Intelligence Unit or the Civil Disobedience Unit (CDU) of the Philadelphia PD, the largest role being played by CDU.

In September 1966, [redacted] of RAM returned to his native city, Philadelphia, [redacted] that he was going underground to "cool it" and to throw off any police attention. He settled in the heart of the Negro ghetto with his common-law wife and two children.

Heads of the Intelligence Unit

This tactic worked. The police had forgotten [redacted] and had no prior experience with or knowledge of RAM. The SA contacting the Intelligence Unit secured spot check coverage of [redacted] by Negro officers as a personal favor after explaining RAM and [redacted] position in it to police officials.

1 910 91D

ST-108 [illegible]

2 - Bureau
1 - Philadelphia (157-2371)

REC-64

22 SEP 1 1967

MBD:MMR
(3)

57 SEP [illegible] 1967

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

INTSEC

Buy U.S. Savings Bonds Regularly on the Payroll Savings Plan

PH 157-2371

When activity started with the appearance of known Negro extremists native to Philadelphia at the [redacted] residence, a full-time surveillance by police went into effect. Police disruptive action was also initiated.

Cars stopping at [redacted] residence were checked as to license numbers. When they left the residence area they were subject to car stops by uniformed police. The occupants were identified. They then became the target for harassment. As an example, the following case is cited:

[redacted] He was located passing out RAM literature at a local school. He was interrogated. He was arrested as a narcotic user on the basis of alleged needle marks. He was fingerprinted and photographed. He was subsequently released by a magistrate.

Any excuse for arrest was promptly implemented by arrest. Any possibility of neutralizing a RAM activist was exercised.

[redacted] was arrested for defacing private property when he painted "Black Guard" on a private building. His companion was also arrested. A charge of carrying a concealed deadly weapon, aswitch-blade knife, was pushed against the companion. His probation officer was contacted, his parole revoked, and he was returned to prison for several years.

When surveillance reflected the arrival of a new group in town, they were brought in for investigation and their residence searched.

Certain addresses used by [redacted] as mail drops in Philadelphia had been determined to be the addresses of known Negro extremists. When a young Negro was arrested for passing out RAM printed flyers and was charged with inciting to riot these addresses appeared in his statements to the police. Search warrants were secured. While the search of the first four only eliminated their use as mail drops, the fifth contained RAM and Communist literature and a duplicating machine with a RAM leaflet on the plate. Three persons were arrested at this last address.

Legal searches of the home of [redacted] and other RAM members produced a volume of literature of such a nature that the District Attorney authorized the arrest of [redacted] and five other RAM members. They are still in prison.

Other RAM people were arrested and released on bail, but were re-arrested several times until they could no longer make bail.

The above local actions appear for the present to have curtailed the activities of this [redacted] group. It was apparently a highly frustrating experience for the persons involved.

[redacted] was advised that he was again under arrest and that his wife and sister were also under arrest, he lay down on the floor of his residence, beat the floor with his fists and cried.

[redacted] has been returned to New York to answer charges growing out of a RAM plot in that city to kill moderate civil rights leaders. Most of the RAM activists are still in jail in Philadelphia at this time.

The above action by local police units is cited as an example of an effective disruptive counterintelligence technique. In other cities where close police cooperation exists, it may be possible to suggest similar operations and to supply to police officers interested in such a violence-prone organization not only information concerning it but ideas relative to its vital or weak sections and profitable points of attack.

III. Future Action Planned by Philadelphia

1. Pursuant to Bureau instructions, this office will commence interviewing RAM members. About a dozen are presently incarcerated in Philadelphia and these will be the first interviewed.

2. Philadelphia is presently reviewing and analysing a list of names and addresses compiled from three private address books taken from [redacted] at the times of his three arrests since he returned to Philadelphia. Selective interviews will be made and the analysis may lead to other counterintelligence suggestions.

3. [redacted] and most RAM activists in Philadelphia appear to be in prison. Philadelphia will have to evaluate the situation more fully to determine the extent of vitality remaining in RAM in this area before it will be in a position to advance further suggestions under this program.

THE NEW YORK TIMES, THURSDAY, MARCH 13, 1975

Security Aide for Indians Says He Was F.B.I. Informer

By JOHN KIFNER
Special to The New York Times

CHICAGO, March 12—The American Indian Movement's chief security officer during the trial of the leaders of the Wounded Knee take-over said today that he was a paid informer for the Federal Bureau of Investigation.

The Government, in a sworn affidavit at the trial, had appeared to contend that it had no informer in the defense ranks.

The informer, Douglass Durham, was the chief aide and confidante of Dennis J. Banks, one of the two defendants and a co-leader of the American Indian Movement. In addition to being the organization's national security director, he became, in effect, its chief bureaucrat.

"I exercised so much control that you couldn't see Dennis or Russell [Means, the other defendant and co-leader] without going through me, you couldn't contact any other chapter without going through me, you couldn't contact any other chapter, without going through me, and if you wanted money you had to see me," Mr. Durham said.

Cash Payments Raised

During the trial, Mr. Durham was the only person, other than defendants and lawyers, with regular access to the room in which defense strategy was planned. He said that his proximity to the A.I.M. leadership had caused his cash payments from the F.B.I. to be raised from $900 a month to $1,100.

He said he was given a special telephone number during the trial, which was held in St. Paul, to call a three-man F.B.I. team headed by Ray Williams.

Reached at the Minneapolis office of the F.B.I., Special Agent Ray Williams said, "We are unable to comment on that."

Following the 71-day occupation of the village of Wounded Knee on the Oglala Sioux reservation of Pine Ridge in South Dakota by more than 200 Indian militants in the late winter and early spring of 1973, Mr. Means and Mr. Banks were indicted on Federal charges of conspiracy, larceny and assault on government officers.

Charges Dismissed

The charges were dismissed after an eight-and-a-half-month trial last Sept. 17 by Judge Frederick J. Nichol of Federal District Court when a juror became sick and the Government declined to proceed with a jury of 11. A Government appeal on the case was argued yesterday in St. Louis.

In dismissing the charges, Judge Nichol assailed the prosecution, contending that it had deliberately deceived the court. He was particularly critical of the F.B.I., whose agents, he said, had given testimony that was not true, and had withheld documents or furnished altered documents to defense attorneys.

"It's hard for me to believe that the F.B.I., which I have revered for so long, has stooped so low," the judge said.

In an interview last night, the 37-year-old Mr. Durham described what he said ware his activities as an F.B.I. informer.

His cover was broken on Friday, he said, when, after some members of the group became suspicious, he was confronted with law enforcement documents that proved his role as an informer.

He said he was "relieved" because he had come to respect Mr. Banks and to believe that A.I.M. was a "legal, social organization that wasn't doing anything wrong."

Mr. Durham, a large man with his black, shoulder-length hair, recounted his career as a police undercover agent in his native city of Des Moines, Iowa.

He said that after serving in the Marine Corps, he joined the Des Moines police force, working in a burglar-infested neighborhood, but left the force after his wife died.

He later worked in and thsn managed a series of restaurants, some of which became hangouts for burglars, Mr. Durham said.

At the same time, he added, he was learning to fly a plane and to scuba dive, and was developing skills as a photographer, studying locks and burglar tools and reading about psychology—all abilities that would eventually serve him as an informer.

He said that he began passing the information to the F.B.I. and the local police, and eventually became a police undercover operative on criminal cases in several Midwestern cities.

He said he was taking photographs for an underground paper called Pax, whose editor asked him to go to Wounded Knee during the Indian take-over.

Reporting this to the F.B.I., he entered the encampment with press credentials, took photographs and gave a report on the Indian group's defenses.

After returning to Des Moines, he said, the F.B.I. suggested that he get in touch with Harvey Major, the leader of the local A.I.M. chapter. Mr. Durham became the publicity officer and later the assistant director of the chapter.

Mr. Durham's swarthy skin, dark eyes, and high cheekbones gives him an Indian look, and appearance heightened by the large turquoise ring and beaded belt buckle he wears and by the headband he wore around his hair when he was the Indian group's chief security officer. He told the A.I.N. members that he was one-fourth Chippewa.

At one point, he said he helped lead an armed take-over of the Grimes State Office Building in Des Moines. He said he first informed the state police of the impending take-over, and that they paid a $100 fine he received for disturbing the peace.

It was his skill as a pilot that first brought him close to Mr. Banks, he said, and the F.B.I. encouraged him to maintain the relationship.

Mr. Banks had gone into hidding in Canada after the indictment and before the bond was raised. He got a message to Mr. Durham to meet him in Yellow Knife, in the Northwest Territories. Mr. Durham did, and Mr. Banks gave him two rolls of movie film that Mr. Durham turned over to the F.B.I.

Then, with the F.B.I.'s knowledge, Mr. Durham again flew to Canada in a rented plane and spirited Mr. Banks to Rapid City, S.D., in time to avoid forfeiting bond on state charges.

Later, Mr. Durham said that he flew Mr. Banks around the country on speaking trips and that at one point the F.B.I. gave him a $1,000 "bonus," made out to the charter service, to pay for the plane.

OFFICE OF THE DIRECTOR FEDERAL BUREAU OF INVESTIGATION MAR 16 1973

As of March 13, 1973, available information indicates an estimated 350 to 400 individuals are at Wounded Knee, Pine Ridge Indian Reservation, South Dakota, taking part in the occupation of that community under the leadership of the American Indian Movement. Previous estimates of the number of individuals at Wounded Knee have ranged as high as 1,000, many of whom are reportedly armed with assorted weapons, including automatic rifles and machine guns. The exact number of individuals at

56

ROUTE IN ENVELOPE

1 - Mr. Atkinson
1 - Mr. Morrissey

9/16/70

1 - [redacted]
1 -
1 -
1 -

Airtel

To: SACs, Baltimore (157-2520) New Haven (157-785)
Detroit (157-3214) San Francisco (157-601)
Los Angeles (157-4054) Washington Field (157-1292)

From: Director, FBI (100-448006) REC-41 2002

COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
BLACK PANTHER PARTY (BPP)
RACIAL MATTERS

Rebuairtel 8/27/70 and San Francisco airtel 9/8/70, copies furnished all recipients.

Bureau concurs with observations of San Francisco concerning proposals submitted by Baltimore, New Haven, and Washington Field. In event these offices have specific proposals to make in line therewith, they should be separately submitted in detail requesting specific Bureau authority to implement them.

MAILED 8 COMM-FBI

Concerning the first proposal submitted by Detroit, counterintelligence action by San Francisco to capitalize on Huey P. Newton's favorable stand toward homosexuals has already been authorized by the Bureau. The second Detroit proposal to consider directing an anonymous communication to Newton accusing David Hilliard of stealing BPP funds and depositing them in foreign banks does have merit and the Bureau does not concur with San Francisco's observation that this would have little effect since there is no record that Hilliard is skimming large amounts of money. Purpose of counterintelligence action is to disrupt BPP and it is immaterial whether facts exist to

1 - 105-165706 (BPP)

SEE NOTE PAGE THREE

ABF:mlm/bjr (20)

SEP 19 1970

MAIL ROOM TELETYPE UNIT

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE.

Airtel to SAC, Baltimore et al
RE: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
BLACK PANTHER PARTY (BPP)
100-448006

substantiate the charge. If facts are present, it aids in the success of the proposal but the Bureau feels that the skimming of money is such a sensitive issue that disruption can be accomplished without facts to back it up.

Accordingly, Detroit immediately furnish Bureau and San Francisco with specific suggestions and wording to this effect and San Francisco should then review same and submit specific proposal in this regard for approval by Bureau.

With respect to two anonymous letters proposed by Los Angeles, Bureau concurs with San Francisco that to include the card of a member of a rival black extremist group in a letter to Hilliard indicating Newton is marked for assassination could place the Bureau in the position of aiding or initiating a murder by the BPP. Accordingly, Los Angeles' proposal identified as "letter A" is not approved. Los Angeles should reword this letter to convey the same thought without directly indicating that it is from a specific member of a rival group. The letter could imply that the writer would soon get in touch with Hilliard to see what he would pay to have Newton eliminated. Resubmit the revised letter to the Bureau for approval.

Concerning the second anonymous letter identified as "letter B" submitted by Los Angeles to be directed to Newton apparently from dissident and expelled Los Angeles BPP members and aimed at undercutting previous leadership, this proposal is authorized. Los Angeles mail same in such a manner that it cannot be traced to the Bureau. Advise Bureau and San Francisco when mailed and of any positive results.

58

TO : DIRECTOR, FBI (100-448006) DATE: 7/9/68

WFO inclined to feel the best way to implement the suggested counter-intelligence program against CARMICHAEL is by inaugurating a "whispering campaign" that he is an agent of the U. S. Government and doing organizing work among Negroes solely for the purpose of helping the government identify racial militants and future racial radicals. Further,

TO : DIRECTOR, FBI (100-448006) DATE: 7/10/68

FROM : SAC, NEW YORK (100-161140) (P)

It is suggested that consideration be given to convey the impression that CARMICHAEL is a CIA informant.

One method of accomplishing the above would be to have a carbon copy of informant report reportedly written by CARMICHAEL to the CIA carefully deposited in the automobile of a close Black Nationalist friend. The report should be so placed that it will be readily seen.

It is hoped that when the informant report is read it will help promote distrust between CARMICHAEL and the Black Community. It is suggested that carbon copy of report be used to indicate that CARMICHAEL turned original copy into CIA and kept carbon copy for himself.

It is also suggested that we inform a certain percentage of reliable criminal and racial informants that "we heard from reliable sources that CARMICHAEL is a CIA agent". It is hoped that these informants would spread the rumor in various large Negro communities across the land.

TO : DIRECTOR, FBI (100-448006) DATE: 9/9/68

On 9/4/68, a pretext phone call was placed to the residence of STOKELY CARMICHAEL and in the absence of CARMICHAEL his mother was told that a friend was calling who was fearful of the future safety of her son. It was explained to Mrs. CARMICHAEL the absolute necessity for CARMICHAEL to "hide out" inasmuch as several BPP members were out to kill him, and it would probably be done sometime this week. Mrs. CARMICHAEL appeared shocked upon hearing the news and stated she would tell STOKELY when he came home.

UNITED STATES GOVERNMENT

Memorandum

59

TO : DIRECTOR, FBI (100-448006)

DATE: 12/2/68

FROM : SAC, SAN FRANCISCO (157-601) - P

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
(BLACK PANTHER PARTY)

Re Bulet 11/25/68.

On 11/19/68, a group of members of the BPP held up a service station in San Francisco and then, when stopped by the San Francisco Police Department, engaged in a shooting fray, in which three police officers were wounded. Participating prominently were two local [redacted] of the BPP, [redacted]. Only [redacted] was armed and did all the shooting, which took place close to Police Headquarters. The truck in which the Panthers were riding was clearly marked as a BPP vehicle. ELDRIDGE CLEAVER was reported in the press as being astounded at such an episode, with so little chance of success, and which received very bad publicity for the BPP. It was so illogical, he charged, that there must have been a police plant in the truck, and suspicion centered on [redacted] because he was the man in charge; likewise he had gone "to the men's room" during the holdup, and the BPP suspected he may have gone to phone the police.

[redacted] In order to help this idea, the San Francisco Office arranged through the SFPD to give [redacted] special privileges at City Prison, such as more lenient visiting hours, and to have the guards show him "extra" courtesy in front of other prisoners. Also, with Bureau concurrence, an anonymous letter was sent to BPP Headquarters via Omaha, where [redacted] was in August, 1968, organizing a new BPP branch, and where he had been temporarily detained and interviewed by police, suggesting

(2) - Bureau (RM)
1 - San Francisco

WAC/jr
(3)

[redacted]

EX-103 REC-52

DEC 6 1968

[redacted]

54 DEC 18 1968

[redacted]

EXHIBIT K

60

[redacted]

SF 157-601
WaC/jr

that the brothers in Omaha were suspicious of [redacted], who had easily gotten out of jail on a local charge.

The success of this operation is unknown, however, it is certain to have added to the suspicions of the BPP toward [redacted] who is actually an important man in the San Francisco BPP.

The San Francisco Office wishes to point out that opportunities such as the above are rare, and fast action is necessary to successfully implement them. It cannot be expected that a planned disruption in the average case would be of such probable value.

It is believed that the BPP is becoming sensitive to the possibility of informers. This office will try to ascertain those Panthers who have been arrested and who the BPP thinks might start to talk. We would then formulate some plan to cast suspicion on the man. We must bear in mind that if the plan is successful, a gang-type murder may be the result.

Recently, the San Francisco Office ascertained that ELDRIDGE CLEAVER was "dating" teenage girls and neglecting his wife, the dynamic and handsome KATHLEEN CLEAVER. With Bureau permission, the dating information was made available to Mrs. CLEAVER. Results of the above are not known.

Attention will be given to this program on a continuous basis.

[redacted]

K.p.2

UNITED STATES GOVERNMENT

Memorandum

TO : Mr. W. C. Sullivan

FROM : Mr. [redacted]

DATE: October 8, 1963

.1 - Mr. Belmont
1 - Mr. Mohr
1 - Mr. Sullivan
1 - Mr. Callahan
1 - Mr. [redacted]
1 - Mr. [redacted]

SUBJECT: GROUPS SEEKING INDEPENDENCE FOR PUERTO RICO
COUNTERINTELLIGENCE PROGRAM
SUBVERSIVE CONTROL SECTION

CONFIDENTIAL

Federacion de Universitarios Pro Independencia (FUPI) is a Marxist oriented student organization at the University of Puerto Rico (UPR) which is affiliated with the communist controlled International Union of Students.

Special Agent [redacted] of the San Juan Office recognized newspaper photographs taken at the "Solidarity with Cuba" rally in Brazil during April, 1963, as including [redacted] and [redacted] officials of FUPI. He sent the newspaper photographs to the Bureau along with a suggested text in Spanish language to be used in a counterintelligence leaflet to be distributed at the UPR.

The leaflet was prepared at the Bureau and 4,000 copies sent to the San Juan Office where they were distributed anonymously in bulk on 9/5/63 to known anti-FUPI and anticommunist groups at UPR and also in the College of Agriculture and Mechanical Arts in Mayaguez, Puerto Rico. The leaflet clearly shows the communist influence in FUPI

The counterintelligence results from this leaflet were highly successful.

105-93124-1098

(1) "El Mundo," a leading Spanish language daily newspaper in Puerto Rico, reproduced the photographs and part of the text from the leaflets on the front page of the 9/16/63 issue of that paper, thus giving the widest possible dissemination of the damaging information regarding FUPI. REC-3

NOT RECORDED
108 OCT 21 1963

(2) The leaflet created panic and discussion among the ranks of FUPI who believe the leaflet was prepared by an anticommunist organization active on the campus of UPR.

(3) As a result of this panic, FUPI has suspended efforts to recruit new members. They had been in the midst of a recruiting drive at the time.

CONFIDENTIAL

105-93124
BGLP:erc
(7)

Classified by 6060
Exempt from GDS, Category
Date of Declassification Indefinite

JAN 29 1964

See Addendum Administrative Division page 2a.

Memorandum to Mr. W. C. Sullivan
RE: GROUPS SEEKING INDEPENDENCE
FOR PUERTO RICO
105-93124

CONFIDENTIAL

(4) The leaflet has made new students aware of the true nature of FUPI as evidenced by the several complaints received by local police from new students and their parents concerning efforts on part of FUPI to recruit new members.

CONCLUSIONS:

Special Agent [redacted] exhibited outstanding initiative in recognizing the officials of FUPI in newspaper photographs and also in recognizing the counterintelligence potential of the photographs. Not only did he recognize the potential but he followed through in submitting his suggested Spanish language text to the Bureau and in the distribution of the completed leaflets.

RECOMMENDATION:

It is recommended that an appropriate incentive award be made to Special Agent [redacted] in an amount to be determined by the Administrative Division.

ADDENDUM: 10/8/63

SA [redacted] is assigned to the Subversive Control Section of the Domestic Intelligence Division and is charged with the supervision of pro-Puerto Rican Independence groups and the supervision of investigations thereof. SA [redacted] displayed outstanding performance in connection with the discharge of his supervisory duties in this matter. He gave instructions and guidance to the field which were clear and concise and made suggestions to the field which were instrumental in bringing this matter to a successful conclusion.

JFB:mjt

CONFIDENTIAL

- 2 -

OVER

UNITED STATES GOVERNMENT

Memorandum

~~ROUTE SLIP~~

TO : Mr. W. C. Sullivan

DATE: October 10, 1968

FROM : Mr. G. C. Moore

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE -
(BLACK PANTHER PARTY)

PURPOSE:

To recommend attached item be given news media source on confidential basis as counterintelligence measure to help neutralize extremist Black Panthers and foster split between them and Student Nonviolent Coordinating Committee (SNCC).

BACKGROUND:

There is a feud between the two most prominent black nationalist extremist groups, The Black Panthers and SNCC. Attached item notes that the feud is being continued by SNCC circulating the statement that:

"According to zoologists, the main difference between a panther and other large cats is that the panther has the smallest head."

This is biologically true. Publicity to this effect might help neutralize Black Panther recruiting efforts.

ACTION:

That attached item, captioned "Panther Pinheads," be furnished a cooperative news media source by the Crime Records Division on a confidential basis. We will be alert for other ways to exploit this item.

Enclosure
100-448006

1 - Mr. C.D. DeLoach
1 - Mr. W.C. Sullivan
1 - Mr. T.E. Bishop
1 - Mr. G.C. Moore
1 - [redacted]
1 -
1 -
1 -
1 -

61 OCT 23 1968

64

UNITED STATES GOVERNMENT

Memorandum

TO : Mr. W. C. Sullivan

DATE: May 21, 1969

FROM : G. C. Moore

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
(BLACK PANTHER PARTY)

Attached is an article concerning the criminal activities of the Black Panther Party (BPP) for the Crime Records Division to furnish a cooperative news media source on a confidential basis.

The extremist and highly violent BPP has been involved in criminal activities since its inception. The BPP has been involved in robberies, attacks on police officers, and other serious crimes. Many individual members have long criminal records. Details of this activity have been compiled in the attached article.

Exposure of these activities by nationwide news media would show the true nature of this extremist group.

ACTION:

That attached article be furnished a cooperative news media source on a confidential basis by the Crime Records Division to expose the criminal nature of the BPP.

Enclosure

100-448006

ENCLOSURE

TJD:ekw (9)

1 - Mr. DeLoach
1 - Mr. W. C. Sullivan
1 - Mr. Bishop
1 - Mr. G. C. Moore
1 - [redacted]
1 - [redacted]
1 - [redacted]

55 JUN 11 1969

JUN 6 1969

TELETYPE

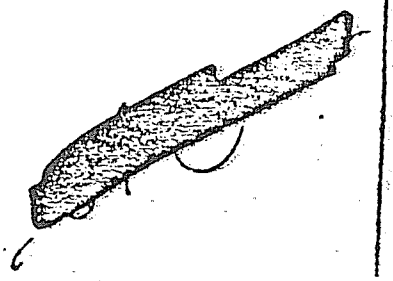
NR008 SE CODE

6:13 PM NITEL 3-16-73 DCB

TO ACTING DIRECTOR

MINNEAPOLIS

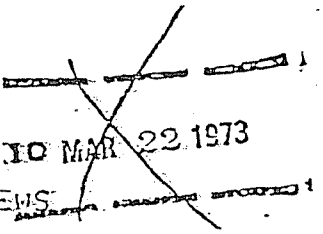
FROM SEATTLE (P) 4PG



Mr. Thompson
Mr. Walters
Tele. Room 65
Mr. Kinley
Mr. Armstrong
Mr. Bowers
Mr. Herington
Ms. Herwig
Mr. Mintz
Mrs. Noonan

RE BUREAU TELETYPES TO MINNEAPOLIS AND SEATTLE DATED 3/9 AND 3/13/73.

[redacted] RADIO STATION KIXI, SEATTLE, WASHINGTON, ADVISED ON 3-14-73 STATION'S BLACK NEWS



END PAGE ONE CC — [redacted]

SE PAGE TWO

REPORTER, CLARENCE MC DANIELS, HAD RETURNED TO SEATTLE FROM WOUNDED KNEE (WK), SOUTH DAKOTA, BUT AT THE REQUEST OF UPI, NEW YORK, HAD AGREED TO RETURN TO WK. ACCORDING TO UPI, NEW YORK, WK INDIANS WILL NOT TALK TO THEIR CORRESPONDENT; HOWEVER, THEY HAVE IMPLICIT TRUST IN MC DANIELS AND WILL TALK TO HIM. MC DANIELS LEFT SEATTLE 3-13-73 EN ROUTE WK, WAS LAST HEARD FROM 160 MILES FROM WK STUCK IN SNOW STORM, HAD NOT REACHED WK AS OF 10:00 AM, 3-16-73. MC DANIELS IS EXPECTED TO CONTINUE FURNISHING COMPLETE COVERAGE OF ACTIVITIES AT WK TO KIXI BY PHONE AND TAPES. HE WILL BE REQUESTED TO DO SPECIAL STORY ON SEATTLE AREA PARTICIPANTS. HE IS UNAWARE THAT HIS STORIES ARE NOT BEING PUBLICIZED IN FULL OR THAT THE INTELLIGENCE INFORMATION AND HIS TAPES ARE BEING FURNISHED THE FBI. KIXI OFFICIALS REQUEST HE NOT BE CONTACTED AT WK; HOWEVER, IF ANY SPECIFIC INFORMATION IS NEEDED BY FBI, KIXI WILLING TO PASS ON REQUEST AS NORMAL DUTY ASSIGNMENT WITH NO REFERENCE TO FBI. MC DANIELS WILL BE MADE AVAILABLE TO FBI, SEATTLE, FOR FULL INTERVIEW UPON RETURN TO SEATTLE AT WHICH TIME IT IS HOPED ALL OF THE SEATTLE AREA PARTICIPANTS WILL BE IDENTIFIED WITH

66

Charles Abourezk says FBI report a 'fabrication'

6/26/76

GLADSTONE
River Editor

Charles Abourezk declared in Rapid City Friday that the Federal Bureau of Investigation report released about him this week is "fabricated to serve the FBI's own purposes."

He said he was referring to the investigative report made available by his father, Sen. James Abourezk, Tuesday to the Washington Star. The senator declared at that time that the allegations about his son were part of a smear campaign" to discredit him.

Charles, who said he is employed as an Oglala Sioux tribal attorney, read a prepared statement prepared by himself, Sam Moves Camp, an Oglala Sioux medicine man, and Rene LeDeaux, Rapid City.

It was near LeDeaux's home that Rapid City police began digging Thursday in a search for arms and ammunition.

The three said they feel the FBI memo "released by it to all law enforcement agencies and others of this ~~Bureau~~ served as a method of provoking already tense law enforcement people, who have been told to expect anything this summer, to a point where fear and violence could be their only possible reaction."

Young Abourezk was flanked by Moves Camp and LeDeaux as a Wounded Knee Legal Defense/Offense Committee worker announced that Abourezk would read the statement but "no questions would be answered."

The statement went on; "We know of no such organization as 'Dog Soldiers,'" a term used in the report, provided the senator, and that "none of us has ever transported or stored ammunition, guns or explosives and we have no knowledge of any 'gun running.'"

"This statement is further proven by the fact that Moves Camp is an Oglala Sioux medicine man and cannot carry any kind of weapons, only the Sacred Pipe.

"We feel that this is only one of many such memos and that they serve several purposes: that because of the detailed descriptions of our addresses and vehicles, it serves as a disguised 'hit list' for the various law enforcement agencies across the country, inviting open harassment of the individuals named in it and at worst, providing possible targeting for political assassinations.

"We feel this memo is evidence of a massive domestic intelligence and para-military operation currently in existence within this nation against those who are working for the rights of Native Americans. These memos can only serve to justify escalation of these domestic operations.

"Moves Camp," the statement continued, "was recently a victim of one of these disrupting programs by the government. He was tailed by the FBI all the way to Canada where he was attending a conference of Indian spiritual leaders. This information was purposely leaked by the FBI to a contact participating in the conference, seeking to cause anger and disruption among those attending. Later an FBI teletype similar to this one was released with the same fabricated allegations.

"We strongly feel that we may already be victims of the purpose and intent of this memo.

"Two days ago, an all points bulletin was issued for Charles Abourezk concerning an incident that supposedly occurred in Scenic while at the time he was at a legal office in Rapid City.

"Yesterday and today, Rene LeDeaux's residence was under surveillance by the FBI and local police and they are continuing to dig a large hole outside her yard, supposedly searching for guns. One of her neighbors was offered $500 to give the police information and when she hesitated they offered to increase that ten times.

Stan Zakinski, Rapid City assistant police chief, said the department had offered no reward to anyone for information which led to the digging. He said, "the tip came from what we will have to say is an anonymous source and we paid nothing for it."

The statement read by Abourezk concluded: "We know that the all points bulletin and the search for guns are fabricated setups by the police, and only the beginning of the harassment that we may be receiving in the future, possibly worsened because of the release of this statement."

The report which the senator said was an FBI memo alleges that the "Dog Soldiers" were to meet June 25 or immediately thereafter at the residence of Howell (LeDeaux) for "final assignments to the Dog Soldiers for targets throughout the state on the Fourth of July weekend."

The memo also alleged that Moves Camp, "an acting American Indian Movement member, allegedly transports the weapons from Redman Strebt (number unknown), Omaha, to the residence of Charlie Abourezk."

Rapid City police reported they began the digging near the LeDeaux residence because they had been told that guns, ammunition and explosives were buried in the lot.

State Radio, the Pennington County Sheriff's office, Rapid City Police Department and local office of the U.S. Marshal's Service all said they had heard no all points bulletin for young Abourezk recently.

(Ed. Note: As with other groups targetted by the FBI, the Bureau's analyses and recommendations for action concerning AIM seem contradictory. The FBI memos excerpted below suggest a self-fulfilling prophecy regarding violence, especially through the use of "extremist informants" who often become agents provocateur.)

Airtel to Albany
Re: American Indian Movement (AIM)
(5/4/73)

A forceful and penetrative interview program of individual activists should be instituted. Conduct interviews in accordance with existing instructions under SAC authority if facts necessitating Bureau approval are not present. Such a program should present excellent opportunity for developing extremist informants among Indian activists dedicated to violence and confrontations best exemplified by the Wounded Knee situation.

MP 157-1458
(1975)

The goals and objectives of AIM remain essentially the same, as those stated in the past.

The objectives most frequently espoused in public are:

1. Abolish the Bureau of Indian Affairs (BIA).
2. Establish AIM Indian Survival Schools throughout the country.
3. Cause the U.S. to honor its treaties with the Indian tribes.
4. To acquire separate and independent nation status for Indian tribes occupying federal reservations.
5. To halt strip-mining and similar exploitation of natural resources on Indian land.
6. To generate unification within the Indian people.
7. To bring the economic status of the Indian Americans up to that of the general community.

(1975) Any full investigation involves a degree of privacy invasion and that of a person's right to free expression. Informant coverage is the least intrusive investigative technique capable of producing the desired results. Thus, because of specific factors surrounding this case, it is recommended that a full investigation be conducted.

68

TO : Mr. Gebhardt

FROM : J. E. O'Connell

SUBJECT: THE USE OF SPECIAL AGENTS OF THE FBI IN A PARAMILITARY LAW ENFORCEMENT OPERATION IN THE INDIAN COUNTRY

DATE: 4/24/75

1 - Mr. Gebhardt
1 - Mr. Bates
1 - Mr. O'Connell
1 - Mr. Gordon
1 - Mr. Wannall
1 - Mr. Mosher
1 - Mr. Gallagher
1 - Mr. Mintz
1 - Mr. Mooney
1 - Mr. McDermott

Files & Com.
Gen. Inv.
Ident.
Inspection
Intell.
Laboratory
Plan. & Eval.
Spec. Inv.
Training
Legal Coun.
Telephone Rm.
Director Sec'y

PURPOSE: This position paper was prepared for use of the Director of the FBI to brief the Attorney General and the Deputy Attorney General (DAG) on the role of the FBI in the event of a major confrontation in Indian country (Federal jurisdiction) where (1) the President decides against the use of troops; and (2) the FBI is ordered by the President and/or the Attorney General to deploy FBI Special Agents in a paramilitary law enforcement situation, in lieu of the use of troops.

Throughout the operation there was a definite lack of continuity as each senior representative replaced another. Colonel Volney Warner (now General), Chief of Staff, 82nd Airborne Division, was dispatched to Wounded Knee at the outset to assess the situation and to recommend whether or not troops should be utilized. The AG issued instructions there was to be no confrontation and negotiations with the militants by representatives of the DOJ were to be entered into to resolve the matter and have the hostages released.

There was a divided authority among the many agencies present at Wounded Knee, including church and social groups. The senior Government representative, Departmental Attorneys, and members of the USA's Staff issued conflicting instructions. Each representative present on the scene took instructions for the most part from superiors of his own agency. For example, on March 4, 1973, after consulting with Colonel Warner, Ralph Erickson issued orders that the use of deadly force by the law enforcement officers on the scene could only be used in self-defense to avoid death or serious bodily harm. In the application of force the officers, including FBI Agents, were to aim to wound rather than kill. This was in direct conflict with the policy of the Bureau that an Agent is not to shoot any person except when necessary in self-defense, that is, when he reasonably believes that he or another is in danger of death or grievous bodily harm. Special Agents are not trained to shoot to wound. Special Agents are trained to shoot in self-defense to neutralize the deadly force. The SACs on the scene and officials at FBIHQ strenuously objected to orders such as this which had previously been approved by the AG without consultation with any FBI official.

The FBI encountered extreme problems, both in the field and at FBIHQ, in adapting to a paramilitary role. The FBI was not equipped logistically to operate in a paramilitary situation in open terrain which ultimately ended in a 71-day siege. The FBI and USMS had to be equipped with military equipment, including Armored Personnel Carriers (APCs), M-16s, automatic infantry weapons, chemical weapons, steel helmets, gas masks, body armor, illuminating flares, military clothing and rations. Authority had to be obtained from both the AG (and/or his representative) and from the General Counsel, Department of Defense, prior to requesting the military logistics adviser, Colonel Jack Potter, to obtain the weapons and material through the Directorate of Military Support (DOMS). This clearance was often not forthcoming when clearance had to be obtained during the night hours. This phase of the operation required the FBI to maintain a constant 24 hour vigilance so as to equip our Special Agents and the other law enforcement officers with the weapons and material needed for a defensive operation.

RECOMMENDATION: The Director meet with the AG and DAG to brief them on the Wounded Knee incident so that they fully understand if such an incident occurs in the future or an incident similar to Wounded Knee and the FBI is involved, the FBI will insist upon taking charge from the outset and will not countenance any interference on an operational basis with respect to our actions. They should understand the FBI due to its long years of experience and training is able to make law enforcement decisions without over-reacting to protect the general public, its Special Agent personnel, and the violators of the law. The AG and DAG should be advised it is our broad policy in such instances as this to "get in and get out as quickly as possible" with complete regard for the safety of all concerned. The FBI furthermore would seize control quickly and take a definite, aggressive stand where necessary. It should be clearly stated that the FBI does not desire to become involved in any political situations and definitely not participate in any discussion where it is obviously political in nature.

Dissemination (from 1975 FBI Memo on AIM)

Reports are disseminated when appropriate, to interested agencies, including the Department of Justice, CIA, Secret Service, DIA, and Military Intelligence. In view of foreign travel by AIM leaders and interest in AIM abroad, periodic reports from and to foreign agencies, for information relative to above activities, as well as an interchange of information between the FBI and the CIA, is necessitated.

Due to the AIM's violence potential, which is frequently directed toward local and state governments and police officers, timely dissemination of specific intelligence information affecting their agencies, is of utmost importance.

70

Memorandum

TO : SAC, LOS ANGELES (157-8781) DATE: 3/29/79

FROM : [redacted] b(7)(c)

SUBJECT: ERNIE LOUIS PETERS
DS - AIM
OO: LA

Pursuant to instructions from Supervisor of Squad 11, it is recommended that this case be reassigned to an Agent on Squad 11 currently working Domestic Security investigations. It is further recommended that this case be assigned to [redacted] who has been briefed on all pertinent facets regarding the AIM investigation. b(7)(c)

3-29-79

1975 FBI Memo

MP 157-1458

JOHN FRANCIS TRUDELL

JOHN FRANCIS TRUDELL continues as the National Chairman of the AIM and of the National Leadership has been involved in radical Indian activities longer than any other AIM leader. TRUDELL is an intelligent individual and is an eloquent speaker who has the ability to stimulate people into action. TRUDELL is known as a hardliner who openly advocates and encourages the use of violence although he himself never becomes directly involved in any fighting. [redacted] TRUDELL had established a semi-permanent residence in So. Paul, Minnesota, but his closest and immediate family ties remain in Nevada.

TRUDELL has appeared numerous times on the Lecture Circuit in behalf of AIM and is usually well-received.

TRUDELL, a Santee Sioux, continually attacks the system wherever he goes and is a close friend of AIM National Press Secretary GEORGE ROBERTS. TRUDELL has been active in AIM-type confrontations with authorities at Eagle Bay, New York; Kenora and Ottawa, Ontario, Canada; and Shiprock, New Mexico.

JOHN TRUDELL has been involved in the area of Indian conflicts/demonstrations longer than any other AIM member. He is intelligent and extremely eloquent when he speaks. TRUDELL has the ability to meet with a group of "pacifists" and in a short time have them yelling and screaming "right-on". In short, he is an extremely effective agitator.

TRUDELL is an ardent racist and has been active in supporting a variety of racist groups such as the Puerto Rican Nationalist Party (PRP) through appearances and speeches. TRUDELL favors the forming of coalitions among minority activist groups for increased "political clout".

TRUDELL has spent some time in Lincoln, Nebraska, assisting in the review of Indian Treaties by the federal court.

TRUDELL is a former U.S. Navy Veteran and served in the Vietnam conflict aboard a destroyer.

How Many More? Death at Duck Valley

Water rights activist, Tina Manning Trudell, pregnant wife of American Indian Movement National Chairman, John Trudell, was killed in a fire on 12 February 1979 along with their children and her mother Leah Manning. Arthur Manning, Tina's father and past Tribal chairman, was critically injured in the blaze. All five were killed in an apparent arson attack on their home on the Duck Valley Reservation in northern Nevada.

The apparent attack follows a pattern of threats, repression and murders carried out against members of the American Indian Movement.

Tina Trudell had been a leading organizer in the struggle to retain the water rights to the Wildhorse Reservoir which was built in the 1930's by the Bureau of Indian Affairs for the exclusive purpose of supplying irrigation water to the Duck Valley reservation. Wildhorse Reservoir is the only potential source of water for the reservation but local non-Indians have begun using the reservoir for recreational purposes and have applied to the state of Nevada for exclusive rights to the water as well as the surrounding lands. Tina also worked with John to organize the Minnesota Citizens' Review Commission on the FBI in Minneapolis.

John Trudell, as one of the coordinators of the Leonard Peltier Defense Commitee, was in D.C. when he was notified of the deaths. John had been a featured speaker at the rally on 11 February 1979 in front of the FBI building where he spoke of the abuses perpetrated by the FBI against the Native American people and other movements for social change. At approximately 2:00 pm, during the speech, Trudell burned the American flag as a symbol of the contempt and anger at the continued policy of genocide of the United States government against the Indian people. At 2:00 am, some twelve hours later, the Trudell home was burned by a fire which consumed the cinder block structure. Local people on the Duck Valley Reservation believe that the fire was intentionally set.

In December 1977, while serving 60 days for cursing at a U.S. Marshal in the hallway outside an adjourned court, word came to John Trudell from the FBI that if he didn't cease his activities on behalf of the people or leave the country, the FBI would get him or his family.

AIM has called for a "Red Alert of all our members in what seems to be an escalation of the war against Indian people to rip off all our energy resources and water following the critical situation facing the United States following their defeat in Iran."

72 (Ed. Note: In 1975 a number of investigations were launched into FBI handling of Native American matters. That same year the FBI stepped up a campaign of armed confrontation with AIM members; on several occasions the FBI surrounded homes of AIM members and began firing weapons. In one instance, when AIM members defended themselves and their families, two FBI agents were killed. Almost immediately the investigations of FBI abuses concerning AIM were quietly shelved.)

Chicago Tribune, Friday, March 14, 1975

AIM activist FBI informer

By William Mullen

A KEY AIDE to Dennis Banks, leader of the American Indian Movement, Thursday admitted he was a paid informant for the Federal Bureau of Investigation while he worked for Banks.

Douglas Durham, 37, told reporters at a press conference in the lobby of the Dirksen Federal Building that he had been on the FBI payroll since joining AIM in March, 1973.

Durham said he became so closely involved with AIM leadership that he often wrote position papers for the militant organization, established its national offices, and was privy to secret strategy sessions while he informed on AIM.

At one point, Durham said, he even used $1,000 provided by the FBI to rent a small plane and secretly fly Banks to Canada following the 71-day 1973 AIM occupation of Wounded Knee, S. D.

DURHAM, A FORMER Des Moines policeman, said he became an official AIM spokesman at the same time he was being paid roughly $1,100 a month by the FBI to pass on travel schedules and plans of AIM leaders.

"I was supposed to give the government any information I could find about foreign involvement in AIM," Durham said. He said his spy role bothered him as he came to admire AIM's involvement in Indian civil rights struggles.

"I find it to be a morally upstanding organization that has done nothing illegal," he said.

Joseph Trimbach, special agent in charge of the Minneapolis FBI office, said in response to Durham's statement, "Our policy is not to comment on matters which are subject to a pending litigation." R. D. Hurd, assistant United States attorney for South Dakota and chief prosecutor at the AIM trial in Minneapolis, said he would not comment.

DURHAM'S ACTIVITIES came to light last Friday when AIM officials confronted him in Des Moines with intercepted documents he had been sending to the FBI.

Durham admitted he gave the FBI secret information from defense strategy meetings during the trial of AIM co-leaders Banks and Russell Means when they faced charges from the Wounded Knee incident.

He said he had acted as AIM's security chief during the trial and was privy to the defense strategy meetings. During the trial the federal government produced a sworn affidavit contending the government did not have any informants in the AIM defense team.

Kenneth Tilsen, attorney for AIM, who was with Durham at the press conference along with other AIM officials, said Durham's involvement may have prejudiced other cases now pending against AIM members.

When the government finally withdrew the Wounded Knee case from the courts, Durham continued to work for Banks, acting most recently as Banks' liaison between AIM and police in the Gresham, Wis., monastery occupation in January.

AIM officials have asked Sen. Frank Church [D., Idaho], chairman of the Senate Select Committee on Intelligence, to investigate FBI involvement.

Memorandum

TO : Mr. J. B. Adams
FROM : Legal Counsel
SUBJECT: SENSTUDY 75

DATE: 6-27-75

Attached is a letter from the Senate Select Committee (SSC), dated 6-23-75, addressed to the Honorable Edward H. Levi. This letter announces the SSC's intent to conduct interviews relating to Douglas Durham, a former Bureau informant. The request obviously relates to our investigation at "Wounded Knee" and our investigation of the American Indian Movement (AIM). This request was received 6-27-75, by Legal Division.

On 6-27-75, Patrick Shea, staff member of the SSC requested we hold in abeyance any action on the request in view of the killing of the Agents at Pine Ridge Reservation, South Dakota.

Memorandum

TO: DIRECTOR, FBI (100-448006) DATE: 5/8/69

FROM: SAC, NEW YORK (100-161140) (P)

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL MATTERS
(RNA)

ReNYlet, 4/22/69.

As noted in re NY letter the NYO sent out 32 postcards to RNA members in NYC area advising them to attend meeting of all members at Hotel Diplomat, Saturday, 4/26/69, at 2:00 PM.

[redacted] advised that the RNA members received stamped cards advising them of the meeting scheduled for 4/26/69. An RNA member called [redacted] to verify meeting and [redacted] stated that she did not schedule any meeting on that date. They deduced that police department had stamp duplicated and scheduled meeting to get all RNA members together so they could make mass arrest. [redacted]

At another meeting of RNA all members were requested to submit handwriting specimens with their own pens and in the exact words used in postcards. The RNA officials are trying to determine if this "trick" could have been pulled by an RNA member.

The NYO plans to schedule additional meetings of the RNA, as conditions warrant. The Bureau will be kept advised.

1-806 REC-43

(2) Bureau (RM)
1- New York (43)

JJD:tf
(3)

RACIAL MATTERS SECT

MAY 9 1969

Savings Bonds Regularly on the Payroll Savings Plan

74

Memorandum

TO : DIRECTOR, FBI (100-448006)

DATE: 3/11/71

FROM : SAC, JACKSON (100-980) (P)

SUBJECT: COINTELPRO
BLACK EXTREMISTS
RM

Re Jackson quarterly progress letter to Bureau, 12/2/70

QUARTERLY PROGRESS LETTER

I. OPERATIONS UNDER CONSIDERATION

Jackson informants and other investigation by the Jackson Division has resulted in information being developed that the Republic of New Africa (RNA), which up until this time has only had a small inactive consulate in Miss., has recently been making intense efforts to obtain land in Miss. In this regard, they have recently obtained temporary use of several acres of land owned by a Negro male in a rural area on U. S. Highway 22 near Brownsville, Miss., which is located about 15 miles west of Jackson. The RNA supporters have begun construction of some buildings on this property and the RNA leaders have announced a National People's Center Council meeting will be held at this location on the weekend of 3/26-28/71.

In view of these developments and the potential that this situation has for rejuvenating the membership and the activity of the RNA, Jackson feels that this development warrants counterintelligence action.

Jackson Division is currently evaluating several possibilities for counterintelligence proposals in this regard and it is anticipated that requests for approval of a proposal will be forthcoming in the future.

2 - Bureau (RM)
2 - Jackson
TF/pap
(4)

REC 79

8 MAR 15 1971

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE.

RACKLEY, SECT.

MAR 22 1971

Buy U.S. Savings Bonds Regularly on the Payroll Savings Plan

1 - [redacted]

8/17/70 61C(5)

1 [redacted]

Airtel

ROUTE IN ENVELOPE

To: SAC, Jackson

From: Director, FBI PERSONAL ATTENTION

COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
(REPUBLIC OF NEW AFRICA)

ReJNairtels 8/3,4 and 5/70 which advised the Republic of New Africa (RNA) regional conference in Jackson had been disrupted and support by residents of Jackson had been curtailed as result of articles printed in the "Jackson Daily News," Jackson, Mississippi.

In reairtels Detroit and New Orleans were requested to advise of any additional tangible results which could be attributed to these articles concerning the RNA. Upon analyzing all tangible results of this counterintelligence operation, you should consider recommending commendations for appropriate personnel.

MAILED 25 AUG 17 1970 FBI CONNELL

JA:sef
(6)

NOTE:

REC-42

AUG 18 1970

Jackson recommended and Bureau authorized that office to furnish public source data concerning violent nature of RNA to a trusted news source on a confidential basis. [redacted] exposing the violent nature of RNA which were printed on the front pages of the "Jackson Daily News," only state-wide evening newspaper in Mississippi.

Tolson
Sullivan
Mohr
Bishop
Bowman
Callahan
Casper
Conrad
Felt
Gale
Rosen
Tavel
Walters
Soyars
Tele. Room
Holmes
Gandy

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE.

NOTE CONTINUED PAGE TWO

AUG 26 1970

MAIL ROOM TELETYPE UNIT

(Ed. Note: In 1971 the police and the FBI raided the Mississippi home occupied by citizens of the Republic of New Africa. The raid was conducted under extremely suspicious circumstances and many people believe it was a staged set-up. RNA leader Imari Obedele was in the RNA offices away from the home at the time of the raid. Despite this fact, Obedele - referred to as "Henry" in the FBI memos - was arrested and convicted on charges of conspiracy to assault an FBI agent involved in the raid. While the charges were still pending, the Jackson office of the FBI agitated vigorously to have Obedle tried on the conspiracy charges, even though the Justice Department was worried it had a weak case. Obedele was convicted of the charges and spent years in the penitentiary, being released in late 1979.

Whenth

When the FBI decided to close its case file on the RNA, one of the reasons cited in a 1976 memo was that the shootout in Mississippi and other incidents were "spontaneous" and "not pre-planned or agreed upon by the leadership," thus showing the original conspiracy charges against Obedele to be a fiction created by the FBI itself in order to remove Obedele as an organizer, and disrupt the RNA.)

4:54 PM IMMEDIATE 7/12/73 VCG TELETYPE

TO DIRECTOR (184-38)

FROM JACKSON (89-24) 7P

IT IS APPARENT TO JACKSON THAT SOMEONE ON A HIGH LEVEL IN THE DEPARTMENT OF JUSTICE IS RELUCTANT TO PURSUE THIS MATTER, WITHOUT GIVING JUSTIFIABLE REASONS, IN SPITE OF ASSURANCES TO THE DEPARTMENT BY U.S. ATTORNEY, JACKSON AND DEPARTMENTAL ATTORNEYS IN JACKSON THAT SUFFICIENT EVIDENCE EXISIS TO CONVICT SUBJECT HENRY AND OTHER SUSPECTS AS WELL AS TO OVERCOME THE CURRENT MOTION TO SUPPRESS.

[redacted] AND [redacted] FEEL STRONGLY THAT THIS CASE SHOULD PROCEED IN COURT AND HENRY AND THE OTHER [redacted] SUBJECTS BE HELD ACCOUNTABLE FOR CONSPIRING TO ASSAULT AN FBI AGENT. THEY ARE CONCERNED THAT A MISCARRAGE OF JUSTICE IS ABOUT TO TAKE PLACE. THEY ARE AWARE THE JUSTICE DEPARTMENT HAS SENT ATTORNEYS TO JACKSON DURING PAST SEVERAL YEARS TO HANDLE CASES BELIEVED BY THEM TO BE OF LESS GRAVITY. [redacted] ADVISED HE HAS APPOINTMENTS WITH U.S. SENATORS JAMES O. EASTLAND AND JOHN STENNIS, FRIDAY, 7/13/73, TO REQUEST THEM TO

INTERVENE WITH THE DEPARTMENT OF JUSTICE TO REMOVE WHATEVER OBSTACLES ARE BLOCKING THE ORDERLY PROCEDURE OF THIS CASE INTO USDC FOR TRIAL.

THE BUREAU IS REQUESTED TO DISCUSS THIS MATTER WITH THE DEPARTMENT ON WHATEVER LEVEL IS REQUIRED TO REMOVE ALL OBSTACLES TO PROSECUTION.

IF THIS CASE IS NOT VIGOROUSLY PURSUED AND CHARGES ARE DROPPED, PUBLICITY IN THE MATTER WILL BE SPREAD TO ALL EXTREMIST ORGANIZATIONS THROUGHOUT THE UNITED STATES BY THE RNA. HENRY'S PREVIOUS PUBLIC STATEMENTS CAN LEAVE LITTLE DOUBT THAT HE WOULD UTILIZE SUCH ACTION TO INCREASE HIS OWN STATURE. THE RESULT COULD SERIOUSLY INCREASE SIMILAR ASSAULTS ON AGENTS ACROSS THE UNITED STATES.

TO: DIRECTOR, FBI (62-116451)

FROM: SAC, DETROIT (66-4906) (P)

ATTORNEY GENERAL GUIDELINES FOR FBI
INFORMATION - GATHERING AND RETENTION POLICIES

DOMESTIC SECURITY INVESTIGATIONS

Re Bureau airtel to Albany, 5/21/76.

UACB, Detroit intends to place its national case file on the RNA (Defile 157-2413) in pending inactive status, in view of the recommendation set forth in summary for discontinuance of investigation of the RNA, its leaders and members.

The following can characterize the above mentioned events:

Violations of the State law by the RNA were not planned and resulting shootouts were spontaneous.

Violations of Federal law were by members. Their actions were not pre-planned or agreed upon by the leadership. These violations dealt primarily in the firearms area.

PAUL N. McCLOSKEY, JR.
12TH DISTRICT, CALIFORNIA

COMMITTEE ON
GOVERNMENT OPERATIONS
AND
COMMITTEE ON
MERCHANT MARINE
AND FISHERIES

Congress of the United States

House of Representatives

Washington, D.C. 20515

205 CANNON BUILDING
WASHINGTON, D.C. 20515
(202) 225-5411

DISTRICT OFFICE:
305 GRANT AVENUE
PALO ALTO, CALIFORNIA 94306
(415) 326-7383

September 21, 1979

Mr. William H. Webster
Director
Federal Bureau of Investigation
10th and Pennsylvania Avenue, N. W.
Washington, D. C. 20535

Handcarried PERSONAL

Dear Director Webster:

Re: Geronimo Pratt Case

I hope you will give this letter your immediate attention, as it raises a very serious matter.

I have finally had the chance to review your letter of July 12 on the above case and to compare it with the documents previously made public by the FBI. I am deeply disturbed to find a statement in your letter that is patently untrue. You say (at page 5):

"Pratt was not the target of the FBI's COINTELPRO".

This may be true as to December, 1968, when the murder allegedly committed by Pratt occurred, but it is clearly not true as to the period of Pratt's arrest and trial, the period when it would have been easiest to frame Pratt.

FBI documents are precise and explicit. A Memorandum from the Special Agent in Charge (SAC) of the FBI's Los Angeles Field Office to the FBI Director, dated January 28, 1970, captioned, "COUNTERINTELLIGENCE PROGRAM, BLACK NATIONALIST -- HATE GROUPS, RACIAL INTELLIGENCE, BPP", proposes that the FBI write and distribute two fake "counterintelligence leaflets" and an anonymous underground newspaper "to attack, expose, and ridicule the image of the BPP in the community and foment mistrust and suspicion amongst the current and past membership." Referring to the first leaflet, the Memo states on page 2:

> "Operation Number One is designed to challenge the legitimacy of the authority exercised by ELMER GERONIMO PRATT, BPP Deputy Minister of Defense for Southern Calirornia."

The second example is contained in an Airtel from SAC Los Angeles to the Director of the FBI, dated August 10, 1970, which bears the same COINTELPRO caption. This Airtel proposes that the Bureau send fake letters to Panther leader Huey Newton, upon his release from prison, charging that during Newton's absence Party members in Los Angeles had been "brutalized and mistreated" by Pratt and David Hilliard, then National Chief of Staff of the BPP. The letters were designed to promote a split in the Party, and to turn Newton against Pratt and Hilliard. If the FBI was willing to jeopardize Pratt's life by this kind of action, is it not reasonable to suppose that the FBI might have been pleased to ask an informer to contend Pratt had committed a specific crime? Or to advise the victim of that crime that Pratt was located at a certain point in a "line up" of potential suspects? It was only four months later that Pratt was "identified" for a crime that had occurred two years earlier!

My primary concern is the question of fairness when an individual accused of a capital crime is tried and convicted of that offense without being informed that he was a target at the time of a strong covert "attack" program such as COINTELPRO, accompanied, as it was, by the use of informers and secret campaigns to discredit the defendant/target. In such a case, it seems to me there is a basic obligation on the government's part to bend over backwards to prove that the defendant was in no way prejudiced by the government's secret program.

An Airtel of October 28, 1969, from the FBI office in San Antonio states:

> "All offices be alert for any information or situations pertaining to these active members of the BPP mentioned above which would lend itself to counter intelligence measures."

In June, 1970, the Los Angeles FBI office prepared a report on Pratt covering an investigating period from 5/6/69 - 6/21/70 which states:

> "Constant consideration is given to the possibility of the utilization of counterintelligence measures with efforts being directed toward neutralizing PRATT as an effective BPP functionary."

I appreciate that the FBI is no longer engaged in deliberate attempts to blacken the reputations of political dissenters or potentially-violent activists. It is hard to escape the conclusion, however, that an organization which would attempt to blacken the reputation of a young pregnant woman, Jean Seberg, by publicizing the suggestion that she had become pregnant, not by her husband but by a member of the Black Panther Party (BPP), would take some pleasure in seeing a Black Panther leader convicted of a crime.

I think it is incumbent upon the government to explain why Mr. Pratt or his attorney were not informed, from the time Pratt was indicted on December 4, 1970 to the time of his conviction on July 28, 1972, that he was a target of COINTELPRO during that period, and that the FBI was using both informers, some of whom were subsequently discredited (as in the case of Darthard Perry) as well as secret campaigns to discredit the defendant/target. If one FBI informer, Darthard Perry, was discredited as you persuasively point out, what about the informer who pointed the finger at Pratt over a year after the crime was committed for which he was indicted? The FBI's position on protecting informants by FOI Act action can only be justified if we can be assured informers weren't used improperly in the COINTELPRO program.

The more I have gotten into this case, the more disturbed I have become at the FBI's actions, both during COINTELPRO and in its FOI posture with respect to COINTELPRO's actions, particularly in the cases of COINTELPRO targets who suffered injury, i.e., being convicted of crimes, without being advised of COINTELPRO.

From your letter, I am forced to the conclusion that the FBI is only acting defensively on COINTELPRO; there is no sense of duty on the FBI's part to search out its records and membership and explain any possibility that Pratt could conceivably be innocent. You properly acknowledge, at page 6 of your letter, that

> "If we had been able to retrieve evidence from our records that might exonerate Pratt, we would have made such evidence available not only as a matter of law, but also as a matter of professional obligation."

I would accept your statement but for the obvious discrepancy between your statement that Pratt was not a target of COINTELPRO and the FBI records which clearly show your statement to be untrue.

As I mentioned in my earlier letter, Pratt's defense attorney, now a highly-respected prosecutor in Los Angeles, believes Pratt to be innocent. It would have been incredibly easy for an FBI informer to both identify Pratt to the police as the tennis court murderer and to assist in his lineup identification. Unless the FBI is satisfied that this did not occur, ordinary rules of criminal justice and burden of proof would dictate that he be granted a new trial and that the jury be advised of COINTELPRO and its possible impact on the facts of the case.

The only way I can satisfy myself that there has not been a miscarriage of justice in this case is to personally examine your complete files, and to discuss the case squarely with the individuals involved. You may be assured that I will treat as privileged any information you contend is privileged under the FOIA from disclosure to persons other than the Congress.

 81

I will call your secretary on Tuesday, September 25, to get your preliminary response to these requests.

Sincerely,

Paul N. McCloskey, Jr.

Memorandum

TO DIRECTOR, FBI (100-448006) DATE: 1/28/70

FROM SAC, LOS ANGELES (157-4054)(P)

SUBJECT: COUNTERINTELLIGENCE PROGRAM
BLACK NATIONALIST - HATE GROUPS
RACIAL INTELLIGENCE
BPP

It is anticipated that this counterintelligence proposal could serve as one phase of a continuous attempt to deny unity of action in the effort of the LA BPP by calling to question the actions of the organization and the legitimacy of its leadership.

It is felt that the production and distribution of these leaflets could be such that the identity of the FBI as the source of the proposed organization could be effectively concealed.

In this respect, Bureau approval is requested in the preparation and dissemination of leaflets similar to the enclosed in the vicinities of 4115 South Central, 9818 Anzac, and 1810 East 103rd Street, locations of BPP activities in Los Angeles. It would be the intention of the Los Angeles Division to distribute leaflet No. 2 seven to ten days following the introduction of leaflet No. 1, as any follow up should not only make the effort a topical one, but stimulate increased reaction within the Los Angeles BPP.

Operation Number One is designed to challenge the legitimacy of the authority exercised by ELMER GERARD PRATT, BPP Deputy Minister of Defense for Southern California, and JOHN WILLIAM WASHINGTON, an active member of the BPP in Los Angeles.

82

TO: DIRECTOR, FBI (100-448006)

FROM: SAC, LOS ANGELES (157-4054) (P)

RE: COINTELPRO
BLACK NATIONALIST HATE GROUPS
RACIAL INTELLIGENCE - BPP

REVIEW IS UNCLASSIFIED
EXCEPT WHERE SHOWN
OTHERWISE

(1970)

In addition, it is suggested the following handbill be anonymously sent to NEWTON and all existing BPP Offices in an effort to further provoke NEWTON's displayed instability:

WANTED

for

CRIMES AGAINST THE PEOPLE

HUEY P. NEWTON

NEWTON has been found guilty of avaricious exploitation of the masses, use of the revolution for personal wealth and recognition, selling out the people to white mother country liberals and wreckless vamping on Elmer Pratt and other revolutionary brothers.

DANGER

NEWTON is known to be emotionally unstable and on the brink of mental breakdown. Use caution when approaching.

ALL POWER TO THE PEOPLE

AND IMMEDIATELY RETURN GERONIMO

TO THE PEOPLE'S VANGUARD

As usual, if the above proposal is approved, appropriate measures will be used to insure the Bureau's identity is not revealed as the source. Results of the proposal will be immediately forwarded to the Bureau.

Page 670 of 3957

Part Four: Deception and Cover-Up

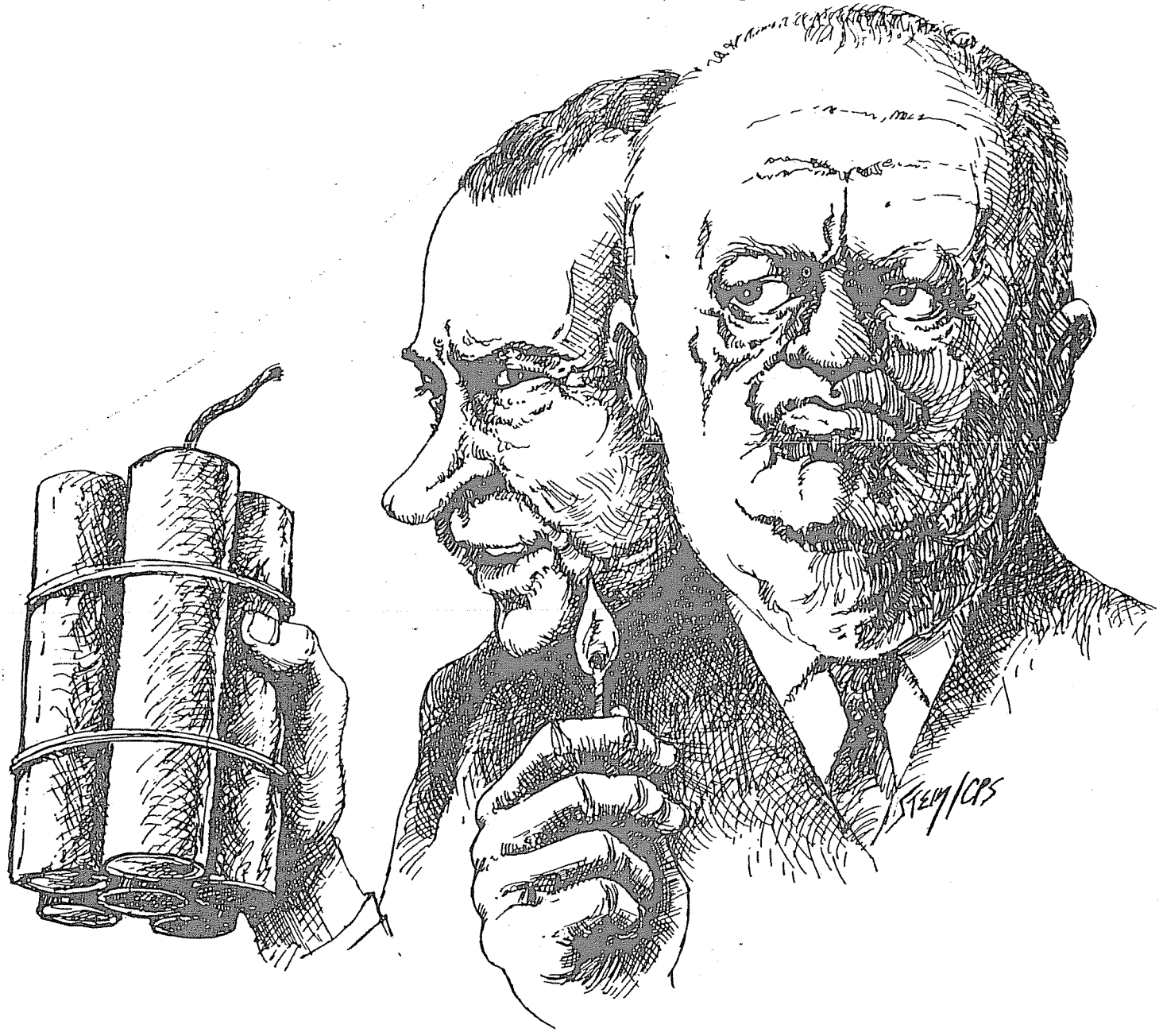
The illegality of FBI counterintelligence tactics and operations creates a great need for concealment and cover-up, an art they have perfected to a high degree. As with many false prosecutions, the Department of Justice has been a willing partner in many cover-ups and manipulations of the judicial system.

In 1969, Richard Nixon appointed Jerris Leonard as chief of the Civil Rights Division of the Justice Department, while Leonard also secretly headed up a broad based political intelligence apparatus within the government known variously as the Inter-divisional Intelligence Unit(IDIU) and the Special Disturbance Group (SDG). The Civil Rights Division then became a focal point of government cover-up operations. After the Hampton raid, Leonard was sent to Chicago by John Mitchell to "investigate" the police action. Leonard empaneled a Federal Grand Jury, which heard four months of testimony but returned no indictments of Hanrahan or his police, despite the overwhelming evidence that the raid had been a "search and destroy" mission against the BPP. Leonard, the FBI, and Hanrahan also kept the FBI's role in the raid secret from this Grand Jury. Leonard also headed up the first Grand Jury investigation into the Kent State murders, which similarly returned no indictments after Richard Nixon had instructed Leonard that no guardsmen should be charged.

The FBI and the Justice Department collaborated to suppress over 200 volumes of inculpatory documents in the Hampton civil rights trial; perjured themselves at Wounded Knee trials and the case against the Vietnam Veterans Against the War at Gainesville, Florida; destroyed evidence germane to the King assassination, and evidence of their illegal actions in pursuing the Weather Underground; covered up their role in the assassinations of King and Malcolm X; repeatedly lied to judges in the Hampton and Socialist Workers Party cases; and concealed damning counter-intelligence evidence from the Senate Select Committee on Intelligence.

In conjunction with such varied and extensive wrongdoing in legal proceedings, the FBI and Justice Department often worked secretly with judges to further their aims. Judge Irving Kaufman worked directly with the Justice Department and the FBI to assure that the Rosenbergs would be executed, and later joined with them to spread pro-government propaganda about the case; the current Chief Judge of the Northern District of Illinois, James Parsons, while a District Court Judge, made derogatory public statements concerning the Nation of Islam and the BPP at the instigation of counterintelligence agents; former Chief Judge William Campbell intervened in the Chicago 8 Conspiracy trial to assure J. Edgar Hoover that a defense subpoena for surveillance documents would be quashed, and secretly passed information from Judge Hoffman to the FBI concerning possible contempt citations against the defendants and their lawyers. Hoff-

man also met secretly with FBI agents and U.S. Attorney Thomas Foran to discuss these contempt citations. In the Hampton trial, Judge J. Sam Perry met secretly with both the FBI and police lawyers to discuss documents which were to be turned over to the Panther plaintiffs. Perry also wrote ex parte letters to then Attorney General Levi praising the conduct of FBI agents and their attorneys who had withheld important documents, and told the Assistant U.S. Attorney investigating charges of misconduct to let the court dispose of the matter at the end of the trial. An Appeals Court Judge, Wilbur Pell, who issued a stinging dissent protesting the ordering of a new trial in the Hampton case, turned out to be a former FBI agent himself, and a long-time member of The Society of Former Special Agents, which was fundraising to defend FBI agents charged with misconduct while the judge was hearing the case.



SAC, Newark (100-50166) 1/9/70

REC-[illegible]
Director, FBI (100-449698) -895

1 - [redacted]

COINTELPRO - NEW LEFT

Reurlet 12/22/69.

Authority is granted to make the anonymous mailing as suggested in relet.

In preparing the letter, all necessary steps are to be taken to protect the identity of the Bureau as the source of the letter. Advise of any results noted.

RHH:jes
(4)

New York should insure use of unwatermarked bond stationery in connection with the above and utilization of mailing procedures which will not allow the Bureau's identification as the origin of this correspondence.

You must insure that Racial Matters Supervisor, Special Agent Coordinator for this program and Agents assigned to Racial Matters investigations are aware of continued objectives of this program and that meaningful proposals are submitted to the Bureau on a timely basis. Insure that such Supervisor and Coordinator are aggressively and enthusiastically ramrodding this program and that Agents are exercising ingenuity and initiative to accomplish this program's objectives.

You are reminded that counterintelligence operations must be approved by the Bureau. Proposals submitted must be designed to insure there is no possibility of embarrassment to the Bureau.

86

1 - Mr. C.D. Brennan

SAC, Los Angeles (100-71737) 8/9/68

Director, FBI ~~(100-449698)~~ 311 1 - Mr. Jackson
1 - Mr. R.H. Horner

EX-105 REC-122 100-449698-267

~~COINTELPRO~~ - NEW LEFT

Neurlet 7/31/68.

It is felt that the mailing of a letter under the caption "Black Nationalists for Freedom," a fictitious organization, as recommended in relet has merit and should be pursued. Prior to taking this action, you should alter your letter in the following respects:

Since it is not likely that a militant black nationalist would have information about [redacted] attendance at meetings of the CP held in Los Angeles, you should delete this particular reference from your letter.

Your characterization of SDS too closely follows the published Bureau description of that organization. For this reason, you should paraphrase the last line of paragraph three so that it will not appear to have been taken from a Bureau document. In this regard, a statement such as "If you don't know it man, the head whitey of the Communist Party in the United States told newsmen in San Francisco that SDS was one of the Party's sould brothers," should be substituted.

1 MAILED 6 AUG 8 1968 COMM-FBI

After making the above changes, you are authorized to make the mailing as suggested.

You should take all possible steps to assure that the Bureau is not identified as the originator of the letter. In this regard, the letter should be prepared on locally obtained stationery that cannot be traced to the Bureau or to the Government.

Advise promptly of any results obtained.

RHH:jes
(6)

Tolson
DeLoach
Mohr
Bishop
Casper
Callahan
Conrad
Felt
Gale
Rosen
Sullivan
Tavel
Trotter
Tele. Room
Holmes

NOTE:

[redacted] Los Angeles, and is a [redacted] is very active in the SDS, supports SDS [redacted] Vietnam demonstrations, has been active and was [redacted]

NOTE CONTINUED PAGE TWO

61 AUG 12 1968 TELETYPE UNIT

FBI Veiled Illegal Break-Ins

wp. 4/25/75

By George Lardner Jr.

With top-level approval, the FBI carried out hundreds of illegal break-ins under an elaborate "Do Not File" system that kept all trace of the burglaries out of regular bureau files.

Members of the Senate intelligence committee, which began delving into the so-called "black bag jobs" yesterday, said they were shocked by the devious manner in which the burglaries of "domestic subversives" were authorized.

"It's really the perfect cover-up," declared Sen. Richard S. Schweiker (R-Pa.).

"Pure frightening," Sen. Howard H. Baker Jr. (R-Tenn.) agreed later.

The statistcs on the burglaries, admittedly incomplete, were not supplied to the committee until the night before yesterday's hearing, staff members said.

Chairman Frank Church (D-Idaho) said the report showed 238 break-ins between 1942 and April of 1968 against 14 so-called "domestic subversive targets."

In addition, at least three other "domestic subversive targets" were subjected to numerous entries from October, 1952, to June, 1966. Of these, the FBI said, "since there exists no precise record of entries, we are unable to retrieve an accurate accounting of their number."

The Washington Post reported in July that the FBI until 1966 conducted dozens and occasionally more than 100 burglaries of all kinds each year, against targets ranging from domestic extremist groups and the Communist Party to foreign embassies and ordinary criminal cases.

The Church committee did not make public any information concerning FBI break-ins at foreign embassies and consulates. For its part, the FBI apparently did not bother to submit a count of the break-ins involved in criminal cases, on grounds that all these were done simply for the purpose of installing "authorized" eavesdropping devices.

Elaborating on the procedures used to approve "black bag jobs," the Sullivan memo said the system then in effect required detailed requests from FBI bureau chiefs for eventual submission in memorandum form to either Hoover or his longtime aide, the late Clyde Tolson, for approval.

"Subsequently, this memorandum is filed in the assistant director's office under a 'Do Not File' procedure," Sullivan explained. Meanwhile, "in the field, the special agent in charge prepares an informal memorandum showing that he obtained bureau authority and this memorandum is filed in his safe until the next inspection by bureau inspectors, at which time it is destroyed."

Testifying at yesterday's hearing, Sullivan's successor former Assistant FBI Director Charles Brennan, said the system meant that the headquarters memos reflecting Hoover's or Tolson's approval would be tucked away in the safe of the appropriate assistant director. There, he said under questioning by Schweiker, it would be kept out of the regular bureau files

Schweiker pointed out that regular FBI files carry serial numbers. As a result, those records cannot be destroyed without leaving a missing number, a telltale sign that something has disappeared.

The system also guaranteed peace of mind for agents in the field offices, knowing that authorizing memos could be shown to bureau inspectors and at the same time knowing that those memos were going to be destroyed, Schweiker marveled.

"It looks to me as though the bureau has perfected a better technique . . . a lot more sophisticated and refined than the 'plausible denial' of the CIA," Schweiker said. "I think we've just touched the tip of the iceberg."

The three-page Sullivan memo ended with an edict in Hoover's handwriting decreeing that "no more such techniques must be used."

Under questioning by Schwarz, Brennan said the FBI director had never shown any legal qualms about such illicit operations in earlier years. Instead, he suggested that Hoover began to grow uneasy after reaching mandatory retirement age (70) in 1965 about any operations that might be embarrassing to the bureau and thus force his ouster.

Although President Johnson waived Hoover's retirement, Brennan said that from 1965 on the FBI director was holding his job largely on an "annual renewal" basis. "That put him into a somewhat vulnerable position," Brennan told the committee.

(See Sullivan "Black Bag Job" Memo on next two pages)

88 Memorandum

: Mr. C. D. DeLoach

DATE: July 19, 1966

: W. C. Sullivan

DO NOT FILE

1 Mr. DeLoach
1 Mr. Sullivan

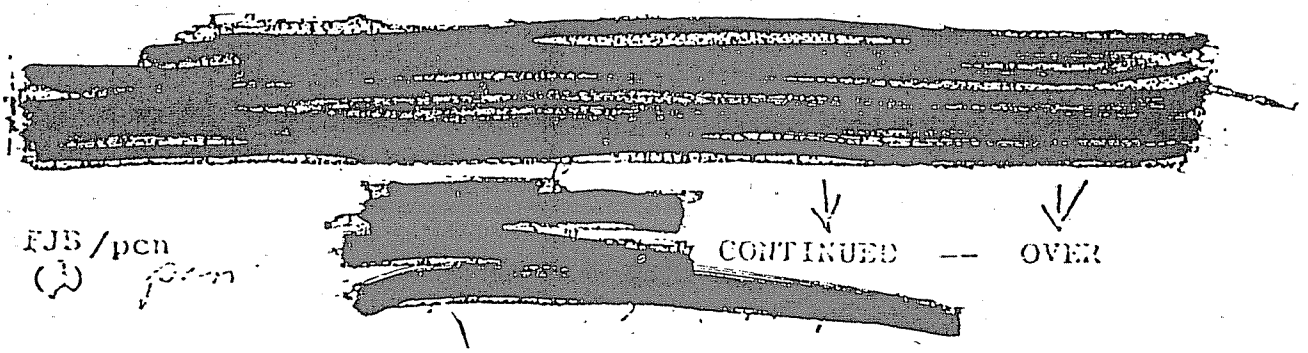
SUBJECT: "BLACK BAG" JOBS

The following is set forth in regard to your request concerning the authority we have for "black bag" jobs and for the background of our policy and procedures in such matters.

We do not obtain authorization for "black bag" jobs from outside the Bureau. Such a technique involves trespass and is clearly illegal; therefore, it would be impossible to obtain any legal sanction for it. Despite this, "black bag' jobs have been used because they represent an invaluable technique in combating subversive activities of a clandestine nature aimed directly at undermining and destroying our nation.

The present procedure followed in the use of this technique calls for the Special Agent in Charge of a field office to make his request for the use of the technique to the appropriate Assistant Director. The Special Agent in Charge must completely justify the need for the use of the technique and at the same time assure that it can be safely used without any danger or embarrassment to the Bureau. The facts are incorporated in a memorandum which, in accordance with the Director's instructions, is sent to Mr. Tolson or to the Director for approval. Subsequently this memorandum is filed in the Assistant Director's office under a "Do Not File" procedure.

In the field the Special Agent in Charge prepares an informal memorandum showing that he obtained Bureau authority and this memorandum is filed in his safe until the next inspection by Bureau Inspectors, at which time it is destroyed.



FJB/pcn
(3)

Memorandum to Mr. C. D. DeLoach
Re: "BLACK BAG" JOBS

[redacted]

We have used this technique on highly selective basis, but with wide-range effectiveness, in our operattions. We have several cases in the espionage field, [redacted]

Also, through the use of this technique we have on numerous occasions been able to obtain material held highly secret and closely guarded by subversive groups and organizations which consisted of membership lists and mailing lists of these organizations.

This applies even to our investigation of the [redacted] You may recall that recently through a "black bag" job we obtained the records in the possession of three high-ranking officials of a [redacted] organization in [redacted] These records gave us the complete membership and financial information concerning the [redacted] operation which we have been using most effeftively to disrupt the organization and, in fact, to bring about its near disintegration.

In short, it is a very reliable weapon which we have used to combat the highly clandestine efforts of subversive elements seeking to undermine out Nation.

RECOMMENDATION:

For your information.

No more such techniques must be used.

L

90

Hoover's secretary destroyed his personal files

CHICAGO SUN-TIMES, Tues., Dec. 2, 1975

WASHINGTON (AP) — J. Edgar Hoover's long-time secretary told Congress Monday that when the FBI director died in 1972, she systematically destroyed his personal files "as Mr. Hoover indicated he wanted."

Helen W. Gandy told the House government information subcommittee that she and another secretary went through all the files in Hoover's offices, destroying all marked "personal."

"There were 30 or 32 file drawers," she testified. "I tore them up and put them in cartons. They were then taken to the Washington FBI field office to be either incinerated or shredded."

Mrs. Gandy denied that the files she destroyed contained any official FBI business or information on the personal lives of public officials.

But former FBI Asst. Director William C. Sullivan said Hoover's personal files were filled with political and personal information on public figures.

Miss Gandy also said that she did not consider her actions in violation of an order by then acting-Atty. Gen. Richard G. Kleindienst that Hoover's offices be sealed.

Asked whether he thought Miss Gandy's action violated his order, Kleindienst said that "I'll just have to leave that up to you to draw your own conclusions."

Miss Gandy testified that official files were retained by the FBI.

"Mr. Hoover would not have allowed them (his personal files) to be used if he had been living," she testified. "I had my instructions."

Miss Gandy repeatedly said she found nothing in the personal files that did not relate strictly to Hoover's personal matters.

She said Acting FBI Director L. Patrick Gray III leafed through the personal files before telling her it was "perfectly all right" to destroy them. Gray succeeded Hoover.

Rep. Toby Moffett (D-Conn.) told Miss Gandy that her testimony contradicted with what Gray had told the subcommittee staff. Miss Gandy offered no explanation.

Sullivan, who is in poor health, gave his statement in a taped interview with a committee staff member. On Hoover's files on public figures, Sullivan said: "I think we all know that it was there. I've seen on a sufficient number of occasions that the door was open on those special little filing cabinets on the wall to know that they were really filled with material . . . they were just loaded."

Key evidence destroyed by FBI

Chic. Sun Times, 1978

By Ronald J. Ostrow
Los Angeles Times Special

WASHINGTON—Potentially crucial evidence in the FBI break-in case was destroyed by the FBI after it had been turned over to the agency by Justice Department prosecutors, court records disclosed Tuesday.

The lawyer for former Assistant Director Edward S. Miller, one of three ex-FBI officials indicted in the case, said that up to 40 per cent of the material originally seized by investigators at FBI offices in Washington and New York had been destroyed.

Miller's attorney, Thomas A. Kennelly, said he had been "informally advised" of the evidence destruction by FBI agents, but had been given no explanation as yet for the action.

HE CITED the destruction of the evidence in arguing that the case against Miller should be dismissed.

Other sources familiar with the case said the destroyed records were "ticklers" — in FBI parlance, copies of documents — that bore handwritten notations that could have been read to indicate that break-ins had been committed. The existence of such evidence would help the defense in its efforts to show that break-ins were a relatively commonplace tactic well-known throughout the Federal Bureau of Investigation.

IT COULD NOT be learned why the Justice Department prosecutors returned such potential evidence to the FBI before it was used in court.

The material was destroyed under FBI rules that require the destruction of "ticklers" after periods ranging from 30 days to six months, according to the knowledgeable sources.

An FBI spokesman would not comment on the disclosure and Terrence B. Adamson, the Justice Department's director of public information, said: "We'll have to answer that in court."

Miller, former acting FBI Director L. Patrick Gray III and W. Mark Felt, No. 2 man under Gray, were indicted April 10 on charges of ordering the FBI break-ins to try to track down fugitive members of the Weatherman terrorist organization. Kennelly said he could not specify the nature of the destroyed records other than to note that they "related directly to the matters alleged" by the indictment.

"I CAN ONLY assume that if the [Justice] department thought enough of it to send agents to seize it, they must have thought it was important," Kennelly said. Kennelly described in his court motion another document that he said he had been "informally advised" had disappeared.

This was a three-page White House memorandum on a May 26, 1971, meeting between then-President Richard M. Nixon, former Atty. Gen. John N. Mitchell, former FBI Director J. Edgar Hoover and then-presidential aides John D. Ehrlichman and Egil Krogh.

THE MEETING took place the same day as a phone call between Nixon and Hoover in which the former President allegedly directed Hoover to "do something" about terrorists who claimed responsibility for murdering several New York policemen and added that he wanted "no punches pulled."

Such evidence could aid the defense in establishing that the break-ins had been approved by higher authorities.

Miller, in the court filing Tuesday, also said he had a witness who will testify that Miller on two occasions between May and July, 1973, discussed "surreptitious entries" with then-acting FBI Director William D. Ruckelshaus, who later became No. 2 man in the Justice Department.

FBI lied on Socialist data, judge says

NEW YORK (AP) — A federal judge Wednesday said that the FBI lied when it said it received information on the Socialist Workers Party without resorting to burglaries.

U.S. District Court Judge Thomas P. Griesa said the government was guilty of intentionally omitting information to protect itself. The party is suing the government for $37 million and is seeking government files before the trial.

The dispute involved Timothy Redfearn, a Federal Bureau of Investigation informant in Denver. The government told the party last month that Redfearn, then identified only by a code number, got leaflets from a "college campus," phone lists, other lists and financial data "as they were made available" to party members.

But Friday, FBI files from 1973 were turned over by court order to party lawyers. The files showed that materials were "stolen" and "removed" by Redfearn from an office, a bookstore and the home of three women affiliated with party.

Griesa said the FBI's original statement "was false, and the response failed to disclose the thing that is crucial . . . namely, that documents had been obtained by means of entries into premises, something which the plaintiff would characterize as 'burglaries' — and they want to try that issue."

"Their haste was no excuse," snapped Griesa. "I can draw no other conclusion than that the person making that answer intentionally omitted materials that were unfavorable to the government when he tried to summarize that file.

"Let's face it. Let's not waste time talking about haste. That was absolutely inexcusable."

Was King Slaying Data Destroyed?

Associated Press

The House Assassinations Committee is investigating an unconfirmed report that documents relating to the murder of Dr. Martin Luther King have been destroyed, according to chief counsel Richard Sprague.

Speaking with reporters after a closed meeting of the committee yesterday, Sprague said the information about the missing documents was uncovered by staff investigators in Memphis, where King was killed in 1968.

Sprague cautioned that the information was "completely unverified." He said he had not yet determined that the documents had, in fact, been destroyed or that they related to the King murder.

Sprague's comment appeared considerably more cautious than his earlier statement about the missing documents.

After a morning session, Sprague told reporters that the documents were "relevant to our investigation" and that "I have been advised that the destruction has been since it was announced (in September) that this committee would be investigating" the King and Kennedy slayings.

Sprague would not say which law enforcement agency had the documents allegedto have been destroyed. However, committee member Rep. Henry Gonzalez, D-Tex., told a reporter he believed the documents had been in the possession of authorities in Tennessee, where King was killed in 1968.

THE MEMPHIS Police Department has denied that any documents relating to the King case have been destroyed. Lt. William Schultz said that all of the King files were turned over to the state attorney general in Memphis.

There have been published allegations that some of these had been burned in September when the department destroyed records of its intelligence division. These records were burned as the department faced lawsuits filed by individuals on whom the department had allegedly conducted surveillance during the 1960s.

At the unexpected public session of the House Committee on Assassinations, Gonzalez asked staff attorney Robert Ozer if he had any reason to believe that documents relating to the King case had been destroyed "since the constitution of this committee."

"Yes, sir," Ozer replied. "I believe there are some documents that have been destroyed."

The hearing, originally expected to be held in secret, was opened to the public after a motion to go into executive session failed on a 6-6 vote. Rep. Christopher Dodd, D-Conn., led the argument to open the hearing.

Files on Panthers withheld

CHICAGO SUN-TIMES, March 25, 1976

By Dennis Fisher

The Justice Department has withheld massive amounts of evidence from lawyers for the survivors of a police raid on a Chicago Black Panther apartment in which two Panthers were killed, testimony in U.S. District Court showed Wednesday.

The surprising disclosure could mean the survivors will win the part of their damage suit that pertains to federal defendants, attorneys in the case said.

The documentary evidence — files on the Black Panther Party, informants and plaintiffs in the complicated suit — takes up more than 30 feet of file space.

After two days of testimony from Federal Bureau of Investigation agent William Deaton and in several conferences in the chambers of U.S. District Court Judge Joseph Sam Perry, attorney for the plaintiffs James D. Montgomery said he will consider seeking sanctions against the federal defendants and their lawyers.

Montgomery described the turn of events as highly prejudicial to his clients in the trial, now in its third month.

The sanctions could include contempt-of-court citations, fines, the costs of Montgomery's preparation for the case over the last six years and, most significant ,a default judgment against the federal defendants.

Judge Perry had ordered the complete files turned over as the trial began last Jan. 5. He said repeatedly during hearings Tuesday and Wednesday on the withheld documents that there was no excuse for such flouting of the rules.

By the close of court Wednesday, defense lawyers in the case had agreed to make copies of all of the withheld materials and to begin Thursday to go through the lengthy process of reviewing each document to determine its relevancy. That could take days, lawyers said.

92

Panthers urge foes be held in contempt

Chicago Daily News 3/30/76

By Rob Warden

Black Panther lawyers argued Tuesday that FBI and Justice Department officials should to be held in contempt of federal court for trying to conceal a 30-foot stack of subpenaed documents.

The documents are potential evidence in a Panther lawsuit asking damages of $47.7 million for the 1969 West Side raid in which Fred Hampton and Mark Clark were killed.

U.S. District Court Judge Joseph Sam Perry ordered all FBI files on the local Panthers produced weeks ago, and Justice Department lawyers assured him repeatedly that they had complied fully with the order.

But it was discovered accidentally last week that only a small percentage of the documents had been produced. Of about 1,600 documents in Hampton's file, for instance, the FBI and Justice Department turned over only 57.

Because the files contain information that might identify FBI informants, the judge permitted the FBI to remove that information before producing the files.

But in this he relied solely on the defendants to decide what they should produce to be used in the case against them.

The deletion process was supposed to be supervised by FBI Agent Robert T. Piper, a defendant in the case, and his Justice Department lawyers, Edward S. Christenbury and Arnold Kanter.

CDN 4/30/76

THIS WEEK IT WAS revealed in court that one of the documents initially withheld described the FBI's role in planning the Dec. 4, 1969, raid, which was carried out by Chicago police under the control of then State's Atty. Edward V. Hanrahan.

The document — an FBI memo initialed by Piper and dated Dec. 8, 1969 — stated that the raid was based on information supplied by informant O'Neal.

The memo, addressed to FBI Director J. Edgar Hoover, said the Chicago office of the FBI had supplied local authorities with a detailed floor plan of the apartment to be raided and an inventory of weapons kept there.

"The raid was based on information furnished by the informant," the memo stated.

This is important in view of the fact that all three FBI agents denied flatly on the witness stand that they had anything to do with the raid.

CHICAGO Sun-Times Editorials

Monday, Aug. 25, 1975

Panther case revisited

During the Nixon years, the same government official publicly in charge of protecting civil rights was privately named the co-ordinator of all government snooping on political dissidents.

Indications of that apparent conflict of interest are buried in Chapter 10 of the Rockefeller Commission's report on the Central Intelligence Agency's domestic activities. This was the setup:

In 1969, Jerris Leonard was publicly named assistant attorney general in charge of all civil rights under Atty. Gen. John N. Mitchell. In that job Leonard was concerned mostly with the protection of rights for minority group members.

In 1969, Mitchell secretly named Leonard head of two justice Department units charged with supervision and co-ordination of the clandestine gathering of information on groups that supposedly posed a threat to peace in the nation's streets — the anti-war protesters of the day and militant minority groups, for example.

In that job, Leonard was to work with the CIA, the FBI, military intelligence groups and other government units.

So publicly we had Leonard-the-protector-of-the-Constitution and, privately, Leonard-the-co-ordinator-of-spying-information.

The problem in this is best highlighted by Leonard's activities in the Chicago Black Panther case. After the 1969 raid, Leonard was named to head an investigation of possible civil rights violations by Chicago police which was, at the time, the only known agency involved in the raid. No indictments resulted.

We now know that the FBI had infiltrated the Panthers and recently Thomas J. Dolan of the Sun-Times staff reported that at least one report was routed to Leonard's intelligence-co-ordinating Interdepartmental Information Unit. Leonard denies he ever saw that report.

He also denies that any conflict of interest existed. We're not so sure. Leonard will be giving a civil-suit deposition here next month and the conflict should be explored. Further, Chapter 10 of the Rockefeller Commission report should be reread by the congressional committees investigating the CIA.

Judge still trusts the FBI

By Rob Warden

The judge in a landmark Black Panther civil rights damage suit has announced that his confidence in the FBI hasn't been shaken by charges that it covered up its role in the death of Fred Hampton.

U.S. District Court Judge Joseph Sam Perry told lawyers in the case Wednesday that his "confidence in the FBI is such" that he was entrusting to its care 94 volumes of irreplaceable documents that conceivably could prove or disprove that there was a cover-up.

WHEN Panther lawyer G. Flint Taylor Jr. asked Perry at least to direct the FBI not to destroy the documents, the judge replied angrily:

"I don't need to direct them. I don't want to presume that they would destroy them."

Judge's actions cited in Panther lawyer's defense

By Dennis D. Fisher

Lawyers for survivors of the 1969 raid on the Black Panthers here filed a lengthy list Thursday of the trial judge's actions, which, they said, were so prejudicial that a contempt citation against one of the attorneys should be set aside.

G. Flint Taylor Jr. and Jeffrey Dennis Cunningham attached to the list submitted to the U.S. Court of Appeals a sworn statement by a former assistant U.S. attorney that quoted the trial judge as saying the FBI never would be found guilty of conspiring to violate the civil rights of the Black Panthers.

Sheldon Waxman, the former assistant U.S. attorney, who was the government's lawyer in the case at one time, made the affidavit Dec. 22, 1975, two weeks before the trial began.

Waxman said under oath that he had two conversations with the U.S. District Court senior judge, Joseph Sam Perry, one in November, 1975, and one a week later on Dec. 1.

In the first conversation, Waxman said, he asked Perry at a political dinner whether the judge had seen newspaper articles about revelations from the Senate intelligence committee concerning an FBI counterintelligence program that focused on the Panthers.

The former prosecutor said the judge told him he had not seen the articles and that the committee's report wasn't relevant too the Panther case before him.

In the second conversation, in the Dirksen Federal Building, Perry told Waxman, according to the latter, "They (the Panther lawyers) will never be able to prove that the FBI killed those fellas." The reference to killing was to the police slaying of Panther leaders Fred Hampton and Mark Clark on Dec. 4, 1969, in an apartment at 2337 W. Monroe.

Perry cited Panther attorney Taylor for contempt last Nov. 11 after the lawyer knocked over a glass water pitcher, which broke on the courtroom floor, while the jury was absent. There is a dispute over whether the incident was intentional. Perry jailed Taylor for five hours.

The FBI's involvement in the deaths of Hampton and Clark is central to the conspiracy trial over which Perry has presided for the last year.

Survivors of the raid, assertedly conducted in a search for illegal weapons, charged that FBI agents and an FBI informant violated their civil rights intentionally in helping to plan and carry out the raid. They seek $47.7 million in damages.

Minister tells talk with Panther judge

By Dennis D. Fisher

Lawyers for the Black Panther plaintiffs renewed charges that the trial judge is prejudiced and filed an affidavit from a minister Wednesday to support their request that the judge remove himself.

G. Flint Taylor Jr., a plaintiffs' lawyer, asked U.S. District Court Senior Judge Joseph Sam Perry to declare a mistrial in the case.

Taylor charged that Perry, 80, "has prejudged the issues and committed countless prejudicial errors in his efforts to make the evidence and verdicts conform with his pre-set opinions."

The lawyer attached a two-page affidavit by the Rev. Thomas W. Strieter, pastor of Grace Lutheran Church, Glen Ellyn, a former Maywood village trustee, to support the bias charges and request for a mistrial.

Mr. Strieter said that he was a chaplain for an American Legion parade last May 31 in Glen Ellyn. During the Memorial Day festivities, the minister rode in a car with Judge Perry and "engaged in a lengthy conversation," he said.

During the talk, Mr. Strieter recalled, "Judge Perry volunteered in substance the following: If only the lawyers would stick to what happened on Dec. 4, 1969, they might make a case. But this conspiracy involving the FBI and Hanrahan is impossible. This cannot be true. There is no earthly way to establish that."

The conspiracy reference involve charges in the lawsuit that Federal Bureau of Investigation agents teamed up with former State's Atty. Edward V. Hanrahan to violate intentionally the civil rights of the Panthers and to kill Hampton and Clark.

Judge Perry dismissed Hanrahan and the FBI as defendants from the case last month without explaining his decision to the jury.

Mr. Strieter said that when he read Hanrahan was dismissed from the case, he was reminded of his conversation with Judge Perry last Memorial Day.

94

Perry ex parte messages in Panther case revealed

CHICAGO LAWYER December, 1979

By Chip Berlet

Judge Joseph Sam Perry, while presiding over the Black Panther civil case, wrote a series of ex parte letters to government officials exonerating the FBI defendants and their attorneys from charges that they wrongfully withheld key documents — charges made by the plaintiffs' attorneys in sanction and contempt motions which were pending before the judge when he wrote the letters.

Judge Perry also suggested in one letter that a much-publicized Justice Department investigation into the charges of wrongdoing be "left to the court" to deal with after the end of the trial.

According to the Panther attorneys, the letters were part of an attempt to "whitewash" the defendants' actions in withholding material; and further, that they show Judge Perry "advocated the Defendants' cause" while hearing the case.

In a motion filed in mid-November, the Panther attorneys ask the U.S. Court of Appeals for the Seventh Circuit to immediately issue its mandate ordering a hearing "to determine what sanctions to impose against the FBI defendants and their lawyers." The Seventh Circuit previously had issued the order along with a call for a new trial, but the defendants have requested a stay on all matters while they ask the U.S. Supreme Court to grant a review.

The Panther attorneys, from the Peoples Law Office, also have asked that disciplinary action be taken against Perry for his ex parte letter writing in the middle of the controversial case. The letters, marked "confidential" and written on Perry's court stationery, are important not only because they show improper actions by the judge, charge the Panther attorneys, but also because they are part of a chain of events whereby the Justice Department was able to postpone its investigation into misconduct by the FBI defendants and their attorneys, knowing in advance that Judge Perry would eventually exonerate the men. The Justice Department apparently closed the investigation, citing the Judge's ruling at the end of the trial.

Because of this investigative shell game, there has never been either a hearing or probe into the charges that the FBI agents and their attorneys conspired to withhold crucial evidence. The evidence links the FBI Counterintelligence Program (COINTELPRO) to the assault on Chicago Panther headquarters

After reviewing the FBI files and determining they were relevant to the case, the Panther attorneys alleged bad faith and moved for a "mistrial, default judgment, contempt, and other sanctions" against the defendants and their attorneys. Judge Perry denied the mistrial and said he would hear the sanctions motions after the case was concluded.

Meanwhile, two black state legislators, Sen. Richard Newhouse and Rep. Harold Washington, wrote a letter to then-U.S. Attorney General Edward H. Levi charging the three Justice Department attorneys with a "massive, illegal cover-up" of the FBI's role in Hampton and Clark's death. The letter went on to call for the firing of the three attorneys, saying they had utilized their offices to "violate the law and the public trust."

In response to the letter by Newhouse and Washngton, the Justice Department ordered an internal investigation led by assistant U.S. Attorney Charles Kocoras. Kocoras sent a copy of the legislators' letter to Perry on April 21, 1976, and invited "any comments you might have . . . with respect to the propriety or impropriety of the conduct of the government lawyers in this case . . . your observations would be of great significance in determining the validity or invalidity of the charge."

Two days later, without informing the plaintiffs, Perry responded to Kocoras and dismissed the charges out of hand. "The fact is that the charges about the conduct of [the attorneys] were and are wholly unwarranted," wrote Perry. Perry also said the withholding of the FBI documents "could not have been intentional" and added, "I am positive that it was an unavoidable error and that all of the attorneys for the agents of the FBI who participated in the case acted in good faith." In the letter, Perry contends that there was only one document in the 30,000 pages of FBI documents belatedly produced that was relevant to the case.

This view is not shared by plaintiff's attorneys, nor the Seventh Circuit, which reversed Perry's order exonerating those involved and ordered a hearing on whether sanctions should be imposed against the FBI Defendants and counsel representing them at the first trial for disobeying court orders to produce documentary materials. Judge Luther Swygert went further and stated:"It is clear that the federal defendants . . . and their counsel rather than promptly furnishing relevant documents as requested, deliberately impeded discovery and actively obstructed the judicial process, thus denying plaintiffs the fair trial to which they were entitled. Regrettably the trial judge permitted these tactics."

Perry not only exonerated the defense attornerys; he praised them. The same day Perry wrote to Kocoras, he sent a copy of the Kocoras letter to Attorney General Levi with a cover letter marked confidential. The letter concluded by saying: "All of the Attorneys and present and former Agents of the FBI mentioned in the [charges] should be complimented for their high standard of conduct in the case." Perry also noted he did not "know Senator Newhouse personally but I do know Representative Washington, who pleaded guilty [in a civil case] before me about two years ago."

The controversy over the FBI's conduct in withholding evidence continued to grow in early May, 1976, with the NAACP's Roy Wilkins calling the FBI's actions "outrageous" and "intolerable" and seeking an independent probe into the alleged federal coverup.

An outside investigation was not launched, but Kocoras, who had ties with several of the defendants, was removed from the investigation. Kocoras was replaced by assistant U.S. Attorney Stephen Kadison. Kadison did seek to interview the FBI agents involved, but apparently was told by the Criminal Division of the Justice Department that the agents could not be interviewed until after the trial ended.

Kadison then wrote the Executive Office of the U.S. Attorney saying he had been forbidden to interview the agents, and asked that he be "permitted to continue with the inquiry rather than be required to wait until the conclusion of the trial." There is no answer to this letter in the correspondence concerning the matter obtained by the plaintiffs' attorneys under the Freedom of Information Act.

Perry's letters were initially refused under the FOIA request, and were recently produced under appeal. Among them is the one addressed to Kocoras which suggests the investigation wait until the trial is over.

According to the Panther attorneys, the scenario shapes up like this: The FBI agents and their attorneys were caught withholding key evidence, and contempt and other sanctions were sought in court. The Justice Department launched a widely publicized investigation, but the presiding judge informed the investigator that the individuals charged were not guilty of wrongdoing and to wait for the end of the trial when the charges would be "disposed of." A new investigator pursued the investigation, but the Justice Department, knowing the judge would exonerate the men at the end of the trial, stalled the investigation. At the end of the trial, the judge dismissed the charges, and on the basis of this dismissal, the Justice Department dropped the investigation. The net result is that no investigation has ever taken place, and given the view of the Seventh Circuit that wrongdoing may have occurred and that a sanctions hearing should be held, the Panther lawyers are seeking an early scheduling of that hearing.

UNITED STATES DISTRICT COURT
219 SOUTH DEARBORN STREET
CHICAGO ILLINOIS 60604

TEL: 431-9400
EXT. 336

95

Mr. Charles P. Kocoras
First Assistant U.S. Attorney
April 23, 1976
Page 4

Attorneys Edward Christenbury, Arnold Kanter and Alexandra Kwoka have represented all of the present and former FBI agents and the former informant for the FBI in the highest tradition of the Bar. They are to be commended for their conduct in a most difficult case.

Very truly yours,

Joseph Sam Perry

JSP:rz

cc: Honorable Edward H. Levi
Attorney General of the United States
Washington, D.C.

CONFIDENTIAL

Honorable Edward H. Levi
Attorney General of the United States
Department of Justice
Washington, D.C. 20530

April 23, 1976

Dear Attorney General Levi:

I am sending you a copy of a letter that I have just written to the Office of the District Attorney in Chicago

All of the Attorneys and present and former Agents of the FBI mentioned in the caption should be complimented for their high standard of conduct in the case of Hampton, et al. vs. Hanrahan, et al., No. 70 C 1384.

Respectfully yours,

Joseph Sam Perry

JSP:rz

96

UNITED STATES DISTRICT COURT
219 SOUTH DEARBORN STREET
CHICAGO, ILLINOIS 60604

CHAMBERS OF
SENIOR JUDGE JOSEPH SAM PERRY

TEL: 431-9400
EXT. 336

May 6, 1976

CONFIDENTIAL

Mr. Charles P. Kocoras
First Assistant United States Attorney
for the Northern District of Illinois
Room 1500, United States Court House
Chicago, Illinois 60604

Re: Hampton, et al. vs. Hanrahan, et al., No. 70 C 1384 and
Assistant United States Attorney Arnold Kanter,
Assistant United States Attorney Alexandra Kwoka, and
Edward Christenbury, Special Attorney from the
Department of Justice in Washington; and
Special Agents of the Federal Bureau of Investigation:
Richard G. Held, Roy Martin Mitchell, Robert Piper
and former Special Agent Marlin Johnson.

Dear Mr. Kocoras:

A controversy arose in the captioned case when the plaintiffs filed one motion asking the court to hold the three first-named persons in contempt and another motion for sanctions against all of the above named individuals. Those motions were taken under advisement. When this case is concluded and a verdict is returned, I will dispose of them. The defendants have filed a motion to hold certain of the plaintiffs' attorneys in contempt. That motion will likewise be taken under advisement.

There are other collateral matters that can best be dealt with after the verdict. This case has been on trial for four months. I cannot take time out to hear collateral motions which can better be disposed of after verdict.

There is still another potent reason for so doing. That is the question of prejudice of the jury which is not segregated, the case being civil and not criminal. Already there has been publicity that may be harmful.

It would seem that this whole matter might very well be left to the court where it is pending.

Very truly yours,

Joseph Sam Perry

JSP:rz

ATTACHMENT H

CHICAGO LAWYER November, 1979

Panthers demand Pell recusal in Hampton

By Chip Berlet

Attorneys in the Black Panther civil suit have filed a motion in the Seventh Circuit Court of Appeals asking that Judge Wilbur F. Pell be recused from "participation in the Court's deliberations and actions" in the case because the judge is a former FBI agent who until late 1977 was a member of the Society of Former Special Agents of the FBI.

The attorneys, all affiliated with the People's Law Office, say that Pell's relationship to the FBI and the society "is not contained in his official biography" issued to them by the court clerk's office, and that they were not aware of Pell's FBI ties until after the latest round of legal motions in the appellate court. Pell's connections have been made public, however, for example in *Who's Who in America*.

Given these relationships, the attorneys say, Pell should not have heard the recent appeal in which two appellate judges ordered a new trial in the Hampton case, while Pell dissented and issued a stinging attack on the plaintiffs and their attorneys.

The defendants in the Hampton case have already cited Pell's dissent in an attempt to have the Seventh Circuit rehear their appeal *en banc*, but this attempt failed in a tight 3-3 vote with two judges recusing themselves. The defendants have indicated that they intend to cite the dissent, and the "close" vote to rehear, in petitions for certiorari they apparently intend to file with the Supreme Court.

At one point in his dissent, Pell characterized the Hampton case as a "wide-ranging witch-hunting type of assault on public servants across the board," and complains, "Unfortunately many who decried the excesses of McCarthyism do not seem equally concerned by the development of the extremity of present day witch-hunting directed toward law enforcement officials."

Comments like these, say the Hampton attorneys, are similar to those made by defenders of FBI practices, including the Society of Former Special Agents of the FBI, which opposes prosecution of FBI agents and has been raised funds for the defense of FBI agents indicted on charges of illegal activity during operations against radical groups. The charge that law enforcement agencies acted illegally while seeking to "neutralize" the Black Panther Party is central to the plaintiffs' case.

Judge Pell was an FBI special agent from 1942 to 1945, according to the 1978-1979 edition of *Who's Who in America*, which also lists him as a member of the Society of Former Agents.

Pell has told reporters that he left the society in late 1977. Legal matters in the Hampton case were reaching the appeals court as early as May, 1975, when Pell voted on a Hampton plaintiff's petition for writ of mandamus. Pell was also a member of the society when he heard several other motions in the Hampton case, and the Hampton attorneys say his resignation came too late to avoid the appearance of a conflict of interest.

The Hampton case arose from a predawn police raid on the Chicago Black Panther headquarters the morning of December 4, 1969, which left Panther leaders Fred Hampton and Mark Clark dead and several other Panther members wounded. Revelations about the FBI's Counterintelligence program (COINTELPRO), which emphasized "neutralizing" the Black Panther Party, led the Hampton attorneys to add the FBI to the civil case.

Named as new defendants in an amended complaint filed on December 4, 1974, were Marlin Johnson, Special Agent in Charge of the Chicago FBI office at the time of the raid; special agents Robert Piper and Roy Martin Mitchell of the Chicago FBI's Racial Matters Squad; and William O'Neal, a paid FBI informant. FBI documents show that O'Neal drew a map of the floor plan of Panther headquarters, with a special notation fixing the location of the bed in which Hampton slept. This map was passed to the Chicago police, who used it in their raid. FBI memos and courtroom testimony by FBI agents show that the FBI provided substantial information which assisted in the planning for the raid, and encouraged the Chicago police to carry out the raid.

In the amended 1974 complaint, the Hampton attorneys alleged a conspiracy between the FBI and local law enforcement officials and police to illegally deprive the Panthers of their civil rights by attempting to destroy their organization, and, in the 1969 incident, killing and injuring them, then covering up the conspiracy.

The majority appellate decision, which ordered a new trial in the case, recognized that the plaintiffs had presented sufficient evidence of a conspiracy so that the case should be heard by a jury.

Given the importance of the FBI's role in the alleged conspiracy and the direct affiliation of four defendants with the FBI, the Hampton attorneys charge that Pell should have recused himself. This is especially the case because the law requires a judge to disqualify himself not only in cases of direct conflict of interest, but also in "any proceeding in which his impartiality might reasonably be questioned."

Pell's former membership in the Society of Former Special Agents of the FBI seems to be more distressing to the Hampton attorneys than his status as an ex-FBI agent.

"The Society is a powerful political organization and lobbying group, knowledgeably described as a 'civilian auxiliary of the FBI' composed of men and women 'whose devotion to former Director J. Edgar Hoover demands expression through something midway between a fan club and an organized religion,'" says the recusal brief, quoting from the book *The Private Sector* by George O'Toole.

A 1975 internal society membership list obtained by the Public Eye, a research group affiliated with the National Lawyers Guild, shows that Pell was not the only figure involved in the Hampton case who was a member of the society. The list also includes one defendant, Marlin Johnson.

Pell has told reporters that the organization is just a fraternal club. Society documents state that the original purpose of the society was "the preservation of friendship and loyalty and the promotion of good will among the members." However, this was officially changed by majority vote of the members on October 9, 1976, to include a number of other objectives, including:

"To encourage respect for our Country and its traditions and to foster its security and freedom from destructive forces, foreign or domestic;

"To seek to elevate and strengthen the public image of the good law enforcement officer as an asset to his community and the image of the good law enforcement agency as a vital force for the good of our Country;

"To serve the Nation in any emergency calling for men with FBI training and experience and complete dedication to the principles of Fidelity, Bravery and Integrity."

The Hampton attorneys claim that, as part of this "emergency" assistance, "The Society reportedly had a long-standing

agreement with the Bureau" to assist in rounding up people for "preventive political detention" under the bureau's recently revealed and discredited "Security Index" or "Agitator Index" programs.

A policy statement issued by the society's board of directors, prompted by the indictments of several former FBI officials for alleged illegal activities during investigations into the Weather Underground, outlines the group's stand on indictments against FBI agents accused of misconduct:

"We affirm that any criminal prosecution of FBI Agents for actions taken totally without criminal intent, while performing their duties with honor and determination to protect the country from criminals and subversives, is completely unwarranted...Our Society is convinced that such ill-conceived attempts to prosecute FBI employees will be regarded by the American public as abhorrent to our nation's sense of fair play and justice."

Charles H. Stanley, president of the society, confirms that the group raises funds for the defense of indicted FBI agents and has helped organize demonstrations in their support.

The society claims to have raised more than $400,000 to defend FBI agents accused of wrongdoing through its Special Agents Legal Fund.

According to Stanley, "FBI Agents should never be prosecuted for carrying out tasks assigned to them by their superiors. It's just irresponsible. That may be a bit strong, but certainly we feel the prosecution of the NY agents [involved in the Weather Underground probe] is wrong."

The Hampton attorneys call this position "morally and constitutionally dubious" and say that this defense has frequently been used by attorneys for the FBI defendants in both the trial and appellate proceedings. Further, the Hampton attorneys charge in their motion that Pell's dissent on the appeal decision "is an almost purely political statement, generally bereft of legal argument, which repeatedly mirrors and adopts the constitutionally bankrupt positions taken by the FBI defendants and the Society of Former Agents."

In his dissent, Pell excuses the COINTELPRO operations of the FBI, which have been found unconstitutional and illegal by the Justice Department, Congress and other courts, by saying, "It is doubtful that in 1969 attempts to discredit groups thought to be presenting a clear and present danger of violence was a violation of First Amendment Rights."

Pell goes on to say that he assumes law enforcement authorities at the time thought "it would be in the public good to neutralize the Black Panther Party" and that "the community would be a safer place for law abiding citizens to live and work if Fred Hampton and his cohorts were not on the scene," Pell says, "It might not be surprising if those entering the premises overreacted in view of the knowledge that they were entering as 'pigs,' some of their colleagues having been killed by a BPP member."

The Hampton attorneys charge in their motion that Judge Pell "could not have written an opinion of this character in a case with this record, unless he had embraced the purposes and goals of the Society of Former Agents and adopted the position of the Agent defendants." They go on to say that Pell's alleged conflict of interest "which appears from his background as an agent, and his membership in the Society, is confirmed by his treatment of the case in his dissent.'

The motion filed by the Hampton attorneys asks that Judge Pell recuse himself or be recused from all further proceedings in the Hampton case. Future motions could require decisions on certification of bills for fees and costs, which could be as much as $1 million for the appeal work. There are precedents granting fees to the prevailing side in civil rights cases.

Recusal alone will not satisfy the Hampton attorneys, though; they are also asking that Pell's opinion in the dissent on the appeal, and his vote for an initial hearing and re-hearing *en banc*, be with drawn or stricken from the record, an that "an appropriate addendum or not be added to the published decision of th appeal, fully setting forth the backgroun and function of the Society of Forme Agents, and the circumstances of the re cusal."

However, according to Judge Pell, th standard procedure for recusal motions i the Seventh Circuit is that they ar sub mitted to the judge being challenged. Pel said that, because the motion was pend ing, he could not discuss specific points but he did state that the"only matte pending is their claim for attorneys fees."

Pell said that his relationship with the FBI and the Society have never been se cret and that he feels free to discuss them in detail.

"I was in the FBI from August of 194 —engaged in war-related activities — un til October or November of 1945, when I left and went back into the private prac tice of law," said Pell. When he left, he joined the Society of Former Specia Agents, which he saw as an organizatio primarily for "keeping in touch" with other former members. "We would get a magazine that would say so-and-so is now doing this or that," said Pell.

"During the time I was a member, the society was not engaged in any political activities, and the entire time I was a member I attended one meeting," Pell said.

Pell said that the first indication he received that the organization was involved in political activity was a fundraising letter he received asking for donations to support the defense of the NY FBI agents indicted in the Weather Underground surveillance case. He said this letter prompted him to leave the society: "When it appeared they were getting into political activities I sent in my letter of resignation."

He concluded that, when people "don't like what someone has to say, then they smear him with this, and that's what this is."

AD HOC

Citizens' Legal Defense Fund For The FBI

Enclosed is a study of the Weatherman organization which was prepared and distributed by the Society of Former Special Agents of the Federal Bureau of Investigation to its members. Because our Fund works in close cooperation with the Society -- and its Special Agents Legal Fund -- we were given permission to give this important study even wider distribution.

Three top FBI men are now under indictment for alleged actions taken in line of duty against this terrorist organization: L. Patrick Gray III, the former acting director of the Bureau; W. Mark Felt, his number two man; and Edward S. Miller, who was chief of counter-intelligence. Through the generous participation of thousands of Americans, our Fund is helping to cover the enormous expenses required to provide these men with the best legal defense possible in order to combat the massive resources of the U.S. Government leveled against them.

THE SPECIAL AGENTS LEGAL FUND, INC.
SUITE 2754, GRAYBAR BUILDING
420 LEXINGTON AVENUE
NEW YORK, N.Y. 10017
212-687-6222

99

March 12, 1979

ad hoc Citizens' Legal Defense Fund for the FBI
Suite 808
95 Madison Avenue
New York, NY 10016

My dear Friends:

I acknowledge receipt of your latest check in the amount of $100,000 made payable to The Special Agents Legal Fund, Inc.

The money expended on the John Kearney case, about $158,000, resulted in a tremendous victory for all of us early last year when the Justice Department's indictments were thrown out of court. But that was just the beginning. Our cash requirements now have been trebled and even quadrupled. We are covering the legal expenses of three FBI men currently fighting indictments certainly as unfair as the one brought against Kearney -- L. Patrick Gray III, the former acting director of the Bureau; W. Mark Felt, who was his number two man; and Edward S. Miller, who was chief of counter-intelligence. We also helped Wally LaPrade, former head of the Bureau's New York office, in his legal fight against his scandalous dismissal.

There are still other FBI men, both active and retired, who are being made scapegoats of the vendetta against the FBI. We see the Bureau, of which we are all so proud, being brought to its knees and almost irreparably harmed by those who would welcome weakened law enforcement and vital intelligence-gathering in our country. Never, in all its history, has the FBI been in such jeopardy. The only way we can save the Bureau is to fight for it by providing legal help for every agent threatened with legal harassment, which is the major weapon of the opposition.

We will deeply appreciate anything you can do. I thank you on behalf of all the former agents in our own organization and, I daresay, for every man and woman actively engaged in the law-enforcement and intelligence work of the FBI.....still the greatest and proudest organization of its kind in all the world.

Sincerely,

The Special Agents Legal Fund, Inc.

Chicago Sun-Times, Wednesday, May 31, 1978

A judge FBI spy at Chicago 7 trial

By David Jackson

Attorney William Kunstler charged Tuesday that William J. Campbell, former chief judge of U.S. District Court in Chicago, acted as an "FBI informant" during the Chicago 7 conspiracy trial.

Kunstler, who was the chief defense attorney during the 1969-1970 trial, showed reporters FBI documents obtained through Freedom of Information Act requests that indicated Campbell had discussed with Marlin Johnson, then the FBI's Chicago bureau chief, how he thought trial Judge Julius J. Hoffman would rule in the case.

Campbell also told Johnson he would "ensure" that a subpena seeking surveillance data, served on former FBI Director J. Edgar Hoover, would be quashed, Kunstler said, quoting another FBI document.

"I THINK it's a crime," Kunstler said of Campbell's alleged communications with the FBI. "It violates his oath of office, (and) it certainly is in contempt of court."

He said Campbell "was apparently the chief informant in the courthouse for the FBI."

Campbell, now a senior federal judge, was not available for comment. Johnson, who retired from the FBI in May, 1970 and currently is vice president of the Canteen Corp., declined to comment on Kunstler's charges.

Kunstler said other newly-released documents show that the FBI kept a "total surveillance" on the defendants and their attorneys, even during post-trial strategy meetings. He said the documents indicated that the attorneys' meetings either were infiltrated or bugged because exact comments made by the attorneys are reproduced in the confidential documents.

He said one document recorded what occurred during a March 5, 1970, conference in defense attorney Leonard Weinglass' Newark (N.J.) office, where appeal strategy was discussed. The government, Kunstler said, "knew what our strategy was going to be, who was going to do what and when."

"EVERYTHING was leaked," Kunstler said.

The first FBI document involving Campbell was a memo dated Oct. 29, 1969, from Alex Rosen, a high FBI official, to Cartha (Deke) DeLoach, described by Kunstler as the "No. 3 man in the FBI" at that time.

The memo states that Judge Campbell contacted Marlin Johnson that day before court began and "confidentially advised" him that "he believed that U.S. District Court Judge Julius J. Hoffman, who is conducting the trial, had 'had enough' of the conduct of the defendants, and that it was possible that Judge Hoffman might today hold the eight defendants as being in contempt of court, as well as some of the attorneys, and sentence them to jail."

Despite Campbell's warning, Hoffman did not do so that day.

A second memo displayed by Kunstler, who met reporters at O'Hare Airport during a stopover between flights, concerned a subpena served on Hoover seeking records of surveillance of the defendants and their attorneys. The subpena was served on Hoover on Dec. 2, 1969. The memo, dated Dec. 3, 1969, also was from Rosen to DeLoach.

IN IT, Rosen reported that Campbell had said he "will insure that the subpena is quashed." The subpena later was quashed by Hoffman.

Defendant Jerry Rubin, who is writing a book, obtained both memos through Freedom of Information Act requests, Kunstler said.

Kunstler also said that he misplaced his address book during the trial, but a Jan. 5, 1970 FBI document indicates that the FBI had it and the names of witnesses, attorneys and others listed inside it.

He said the new information showed that judges and the government—rather than the defendants and their attorneys, as some have claimed—made a "circus" of the lengthy trial. "No process of the judicial procedure was left untrammelled. . . . To me, it's an unparalleled perversion of the legal process," Kunstler said.

The defendants and their lawyers were charged with more than a dozen citations of contempt. Kunstler said he would file a motion to have the records of the contempt actions expunged and that he was considering suing Campbell, former U.S. Atty. Thomas Foran, the prosecutor, and Hoffman, among others, for damages.

Friday, December 28, 1979 DAILY LAW BULLETIN—3

Ten years later, "Chicago Seven" attorney William Kunstler is still charging that the real conspiracy involved in that trial included the judge, prosecutors and the FBI.

In documents made public Thursday, Kunstler's federal court motion claimed that evidence indicates the FBI forged threatening letters purportedly written by the Black Panthers to prospective jurors who might have been sympathetic to the defendants. He bases his charge on an FBI memo he obtained through the Freedom of Information Act. The memo reportedly says that U.S. District Judge Julius Hoffman concurred with an FBI order not to investigate the letters without permission from top agency officials. Kunstler is trying to overturn contempt of court convictions against the defendants.

Chicago Tribune 4/78

FBI used black judge to discredit Muslims

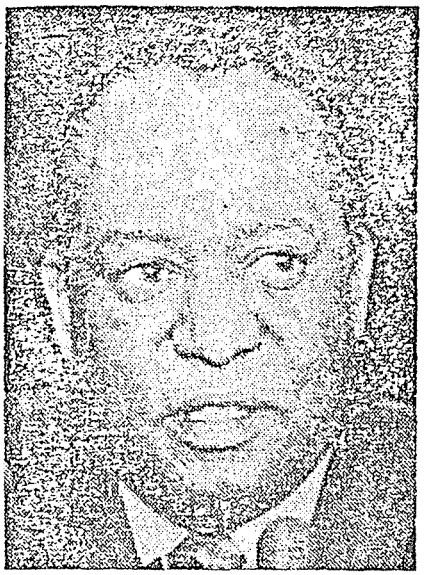
By Rob Warden

CHIEF JUDGE James B. Parsons of U.S. District Court was "utilized" by the FBI in a counterintelligence program to discredit the Black Muslims in the 1960s, according to bureau documents obtained by The Tribune.

The documents, released under the U.S. Freedom of Information Act, are memos to the late FBI Director J. Edgar Hoover from Marlin W. Johnson, special agent in charge of the bureau's Chicago office at the time.

The memos say Parsons, at FBI's behest, repeatedly criticized the Black Muslims, then known as the Nation of Islam, as racist and violent.

Parsons, 66, the first black ever named to the federal bench, denied Thursday that the FBI asked him to make the statements.



Judge James Parsons

"IT IS TRUE that I sought information about the Muslims from the FBI and that there were occasions quite early in the '60s when I was critical of the Muslim movement, but under no circumstances did the FBI ever ask me to speak," he said.

One of the memos, dated Jan. 22, 1969, says in part: "Over the years considerable thought has been given, and action taken with bureau approval, relating to methods through which the NOI [Nation of Islam] could be discredited in the eyes of the general black populace or through which factionalism among the leadership could be created.

"Factional disputes have been developed—the most noteable [sic] being Malcolm X Little. Prominent black personages have publicly and nationally spoken out against the group—U.S. District Court Judge James Benton Parsons being one example.

"Chicago, as the bureau is aware, has always been on the alert for methods by which the NOI could be directed or disrupted. As is evidenced by the present co-operation with Parsons this policy continues."

ANOTHER MEMO, dated Dec. 12, 1968, says that "Chicago continues to maintain periodic contact" with Parsons, who was "approved by the bureau for counterintelligence usage sometime ago."

Parsons, the memo adds, "will certainly continue to speak out in such fashion and the contact by Chicago productive of such will continue."

A third memo, dated Aug. 29, 1969, says that "several years ago Chicago utilized a local federal judge to speak out against the NOI. He has not been utilized in this regard since the murder of Malcolm X Little as it was not the bureau's desire to involve him in a name-calling contest."

Parsons, interviewed by telephone in Delavan, Wis., where he was attending a judicial conference Thursday, said he has "no reaction" to the statements in the memos. "To me the language 'utilized' is understandable, but from a public standpoint it will not be understood.

"I think the documents reflect the fact that I had been threatened back in '63 by the Muslims. I was anxious to be constantly informed about them, and I had a complete FBI file on them. At no time did anybody ask me to speak out against or use my influence against anyone. I am responsible for what I said."

THE THREAT, Parsons said, "was that I was to be physically disciplined."

He said the threat was not made directly to him, but that he learned about it from the FBI. "Frankly, I was quite frightened when it occurred," he said.

He said his view of the Muslims has changed and he no longer criticizes them.

Chicago Tribune, Friday, April 28, 1978

Bell curbed probe of FBI, task force leader charges

WASHINGTON [AP]—Atty. Gen. Griffin Bell undermined the Justice Department's investigation of the FBI and blocked possible indictments against eight middle-level FBI officials, the man who led the probe said Thursday.

William L. Gardner told a Senate appropriations subcommittee that Bell effectively halted the investigation by refusing to let prosecutors seek perjury indictments against an unspecified number of FBI officials who the task force believed were lying.

Without the threat of perjury charges, Gardner said, his task force had no leverage with which to force agents to tell the truth about allegedly illegal FBI activities.

GARDNER SAID BELL also refused to let prosecutors seek indictments of eight mid-level officials on charges of wiretapping, mail theft, break-ins or black bag jobs, perjury, and false statements to a government agency.

He said the officials, some of whom still work for the FBI, include three squad leaders, four special agents in charge of divisions and one assistant director.

Gardner did not name any of the officials. He resigned as head of the task force in December but remained as head of the criminal section of the department's civil rights division.

Bell, out of town until Monday, had no immediate comment. But an aide, Terence B. Adamson, said the attorney general stands by his handling of the case and does not want to get into a debate with the task force lawyers.

ADAMSON described Bell's philosophical framework for prosecuting the so-called black-bag abuses as "giving the highest priority to those with the greatest degree of culpability." Adamson said that Bell "was handed a difficult task when he arrived" and that "he gave it his full attention and best efforts, and he did his duty as he saw it."

Adamson said FBI officials and employes are still subject to disciplinary procedures for any role they may have had in the allegedly illegal surveillance activities.

Gardner testified that the task force not only learned that FBI agents were involved in burglaries but also turned up a class in breaking and entering that was given by a "guest lecturer" at the FBI training academy in Quantico, Va.

ANOTHER FORMER member of the task force, Stephen Horn, told the subcommittee that Bell pleaded with an FBI official to recant his testimony after the task force told the attorney general it wanted to indict the official for perjury.

"He told him he did not want to prosecute him because he was an FBI agent," Horn said of Bell. "He said it would be a disgrace to the FBI."

The statements by Gardner and Horn, and by two other task force members who resigned last year after a dispute with Bell, prompted Sen. Lowell Weicker [R., Conn.] to question Bell's fitness for office.

"It seems clear that the attorney general, despite the advice of top Justice Department prosecutors, willfully selected not to pursue a complete investigation," Weicker said. "What has transpired here this morning rightfully calls into question the suitability of Griffin Bell to continue as attorney general of the United States."

HOWEVER, SEN. Ernest Hollings [D., S.C.] said such talk was "sanctimonious" and said what really was at issue was that Bell and his subordinates disagreed on how to proceed with a difficult investigation.

Gardner said that when his task force recommended indictments of eight officials, four of them no longer were with the bureau, and four still worked at the FBI.

He said Bell objected to indicting so many agents and that the attorney general said several times that "he had to manage the bureau but couldn't do it with their officials on trial so often."

BELL EVENTUALLY decided, Gardner said, to indict only one man, John J. Kearney, the former director of the FBI bureau in New York.

Since then, the Justice Department has dropped that indictment and has announced indictments against former Acting FBI Director L. Patrick Gray III and two other executive-level FBI officials on charges resulting from allegedly illegal break-ins ordered by the agency in the early 1970s.

Gray has pleaded innocent to the charges, as did the other two defendants —W. Mark Felt, a former acting associate director, and Edward S. Miller, a former assistant director of the domestic intelligence division.

Bell also has taken administrative action against another FBI executive, J. Wallace LaPrade, until recently head of the FBI's New York office.

GARDNER TESTIFIED that Benjamin Civiletti, then head of the department's criminal division, agreed in an April 2, 1977, meeting that the eight cases should be presented for grand jury indictment.

Gardner also testified that the nature and extent of recent intelligence agency abuses were hidden from Congress and that the Senate committee investigation headed by Sen. Frank Church [D., Idaho] was deceived.

SEVEN DAYS SPECIAL REPORT 5/7/78

(Second of Two Parts)

Inside the FBI

FBI Informers Beg, Borrow and Steal

This has been a bad month for the FBI. First, three top FBI officials—former Acting Director L. Patrick Gray, 3d, former Acting Associate Director W. Mark Felt, and the former chief of the Bureau's counterintelligence section, Edward S. Miller—were indicted by a Federal grand jury for conspiring to violate the civil rights of American citizens by ordering agents to break into their homes without warrants. The break-ins cited in the indictment occurred in late 1972 and early 1973 in New York City and Union City, New Jersey, against friends and relatives of Weather Underground fugitives.

Attorney General Griffin B. Bell also asked current FBI director William H. Webster to subject 68 FBI agents to administrative discipline for their role in the illegal entries. Such action could result in dismissal.

On April 13, three days later, J. Wallace LaPrade, chief of the FBI's New York office and an unindicted co-conspirator in the government's case, was transferred to Washington to answer Justice Department charges stemming from the same investigation.

LaPrade, a 27-year veteran of the FBI, lashed out at Bell, charging that illegal searches and surveillances continued under the Ford and Carter Administrations and are continuing today. William Safire in *The New York Times* alluded to two specific cases LaPrade might have had in mind. These, in addition to the elaborate surveillance undertaken in the current "spy" case of Ronald Humphrey and Truong Dinh Hung suggest that current indictments are merely a cover for continuing illegal surveillance. Some sources even go so far as to suggest that the Justice Department's decision to zero in on the FBI's Weather Underground investigations offers the FBI defendants an easy out, as they can claim their activities fell into the national security loophole. Recent allegations that the Weather Underground was in contact with the PLO indicate that this may be the case.

At the same time that these unprecedented indictments were being handed down, charges were dropped against John J. Kearney, a lower-level FBI official who had been under indictment for illegal wiretapping and mail openings. Bell said he dropped charges against Kearney after William C. Sullivan, former FBI number three man, testified that in 1970 J. Edgar Hoover had ordered him to urge Kearney to employ illegal measures against the Weather Underground.

If Kearney had gone to trial, it is believed Sullivan would have testified on his behalf. Sullivan also was reported to have been the key witness against Gray, Felt and Miller. He was a defendant in several multi-million dollar civil suits against the FBI and it was known that he intended to cooperate with the prosecution. A number of people, therefore, had good reasons for wanting Sullivan out of the way. Last year, shortly after he testified for nine hours before a grand jury investigating the FBI, he was shot in what was described as a hunting accident near his home in New Hampshire.

Attorney William Kunstler recently charged that Sullivan was murdered and called for a full investigation, citing a number of suspicious circumstances surrounding his death. According to Kunstler, Sullivan was shot 15 minutes before sunrise at 243 feet with a sniper rifle equipped with a scope that magnified objects three to four times their normal size. The killer, Robert Daniels, is the son of a state trooper and, says Kunstler, an expert hunter.

He allegedly mistook Sullivan, attired in a black and white mackinaw and white turtleneck sweater, for the white tail of a deer. According to officials who examined the body, however, Sullivan was wearing a black and red mackinaw. The only white item of clothing they found was a T-shirt entirely covered by outer garments. The autopsy report has the fatal bullet traveling in a downward path through Sullivan's body until deflected upwards by vertebrae, while the killer said he shot upwards over the brow of a hill.

The FBI did not investigate at the time of the shooting. "It was a local matter," says FBI press officer Tom Deakin. "We didn't see any reason to investigate then and we find no reason now."

Kunstler's charges are potentially the most explosive of all and could have extremely serious consequences for the FBI, dwarfing the current flap over illegal entries, wiretaps and mail openings. Here is Part II of Dave Dellinger's interview with a former FBI agent who sheds some light on the kinds of activities that led to the grand jury indictments against the three top FBI officials. *Peter Biskind*

104

65-69260-1

Airtel

July 15, 1964

APPROPRIATE AGENCIES AND FIELD OFFICES

CONFIDENTIAL

To: SACS, New York (100-129802)
Chicago (100-32864)
Washington Field (100-421FF) (Enc - 2)

PERSONAL ATTENTION

From: Director, FBI (100-3-104-Main)

1 - Mr. Belmont
1 - Mr. Sullivan
1 - Mr. D.E.Moore
1 - Mr. Baumgardner
1 - Mr. Branigan
1 - Mr. Smith (R.W.)
1 - Mr. Ryan

see above bracket

Since initiated in 1956, the Counterintelligence Program (Cointelpro), directed against the Communist Party, USA (CPUSA), and related organizations, through a variety of techniques has disrupted, exposed and neutralized the communists. Some successful Cointelpro operations such as anonymous letters and mailings, in spite of their simplicity, have caused unexpected consternation and disruption among the comrades. Cointelpro-initiated publicity has been a tremendous deterrent to the comrades, while at the same time it has alerted the general public to their insidious maneuvers. More sophisticated techniques and operations have caused defections and expulsions within Party ranks. (U)

SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY
AUTOMATICALLY DECLASSIFIED ON (INDEFINITE)

MAILED 4
JUL 15 1964
COMM-FBI

RECD-READING ROOM
JUL 14 4 33 PM '64

Over the years, our approach to investigative problems in the intelligence field has given rise to a number of new programs, some of which have been most revolutionary, and it can be presumed that with a continued aggressive approach to these problems, new and productive ideas will be forthcoming. These ideas will not be increased in number or improved upon from the standpoint of accomplishments merely through the institution of a program such as COINTELPRO which is given another name, and which, in fact, only encompasses everything that has been done in the past or will be done in the future. (U)

(C)

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DECEPTION: THEORY AND PRACTICE

by

James D. Monroe

June 2012

Thesis Advisor: Hy Rothstein
Second Reader: Kalev Sepp

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Deception: Theory and Practice			**5. FUNDING NUMBERS**
6. AUTHOR(S) James D. Monroe			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis explores the history of U.S. Army deception and doctrine, and combines the insights gained with the various works on deception, cognitive psychology, communications, and decision-making in order to distill a concise handbook for deception practitioners. A longitudinal review of U.S. Army doctrine reveals a wide variation in the treatment of deception, from emphasized to ignored. This variation can be primarily explained by the U.S. preference for the cumulative destruction style of war and the perceived balance of power between the U.S. and its adversaries. This thesis strives to fill the current doctrinal gap by distilling the existing body of work to create a theory of deception in the military context. The theory presented provides a cogent structure, taxonomy, and lexicon; as well as, emphasis on how deception functions within the frameworks of communications and decision-making. Next, a synthesis of the practice of deception is presented, with a focus on deception planning and the essential elements of deception practice. Examples of U.S. use of deception from the Revolutionary War to Operation DESERT STORM are presented to provide illumination on the utility and use of deception. Finally, the thesis provides recommendations on how to organize for deception operations.

14. SUBJECT TERMS Military Deception, Communications, Decision-Making, OODA, Doctrine, Planning			**15. NUMBER OF PAGES** 173
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Page 695 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 696 of 3957

Approved for public release; distribution is unlimited

DECEPTION: THEORY AND PRACTICE

James D. Monroe
Master Sergeant, United States Army
B.A., Thomas Edison State College, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2012

Author: James D. Monroe

Approved by: Dr. Hy Rothstein
Thesis Advisor

Dr. Kalev Sepp
Second Reader

Dr. John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

Page 698 of 3957

ABSTRACT

This thesis explores the history of U.S. Army deception and doctrine, and combines the insights gained with the various works on deception, cognitive psychology, communications, and decision-making in order to distill a concise handbook for deception practitioners. A longitudinal review of U.S. Army doctrine reveals a wide variation in the treatment of deception, from emphasized to ignored. This variation can be primarily explained by the U.S. preference for the cumulative destruction style of war and the perceived balance of power between the U.S. and its adversaries. This thesis strives to fill the current doctrinal gap by distilling the existing body of work to create a theory of deception in the military context. The theory presented provides a cogent structure, taxonomy, and lexicon; as well as, emphasis on how deception functions within the frameworks of communications and decision-making. Next, a synthesis of the practice of deception is presented, with a focus on deception planning and the essential elements of deception practice. Examples of U.S. use of deception from the Revolutionary War to Operation DESERT STORM are presented to provide illumination on the utility and use of deception. Finally, the thesis provides recommendations on how to organize for deception operations.

Page 699 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 700 of 3957

TABLE OF CONTENTS

I. INTRODUCTION....1
A. BACKGROUND....1
B. HYPOTHESES....3
C. SCOPE AND SIGNIFICANCE....3
D. METHODOLOGY....4

II. DECEPTION IN U.S. ARMY DOCTRINE....7
A. PRE-WORLD WAR II ERA....8
B. WORLD WAR II ERA....10
C. POST WORLD WAR II THROUGH VIETNAM....13
D. POST VIETNAM ERA THROUGH DESERT STORM....18
E. POST COLD WAR ERA....21
F. CONCLUSIONS OF DOCTRINE REVIEW....24

III. EXPLANATIONS FOR VARIATION OF DECEPTION EMPHASIS....25
A. THE AMERICAN WAY OF WAR....25
1. Styles of War....26
2. American Preference for Cumulative Destruction....29
3. Balance of Power....31
B. PROFESSIONAL OFFICER CLASS....34
C. OVER-CLASSIFICATION....35
D. MORALITY....36
E. CONCLUSION....37

IV. THEORY OF DECEPTION....39
A. WHAT IS DECEPTION....39
1. Deception Defined....40
2. Deception: Truth and Lies....41
B. TAXONOMY OF DECEPTION....43
1. Taxonomy of Method....43
2. Deception....44
3. Active Deception....45
a. Displays....45
b. Feints....47
c. Demonstrations....47
d. Disinformation....48
4. Cover....49
a. Camouflage....49
b. Denial....50
5. Alternate Deception Taxonomies....50
a. Commission and Omission....50
b. Level of Sophistication....51
c. Effect-Based....52
C. DECEPTION AND UNCERTAINTY....52

Page 701 of 3957

1. Uncertainty 52
2. A-Type Deception....53
3. M-Type Deception....54
D. THE WHY OF DECEPTION....54
1. Overview 54
2. Surprise....55
3. Freedom of Action....55
4. Save Lives and Resources....56
5. Mislead the Target 56
6. Relative Superiority 57
7. Security 58
8. Subversion 58
9. Mental Isolation 59
E. COMMUNICATIONS PROCESS OF DECEPTION....60
1. Overview of Communications....60
2. Indicators....61
3. Channels....62
4. Deception's Role in the Communications Process 63
F. DECEPTION AND TARGET DECISION-MAKING....63
1. Observe 65
2. Orient 66
a. Cultural Schemata *67*
b. Personal Schemata....*68*
c. Cognitive Biases and Heuristics....*69*
d. Results of Orientation *71*
3. Decide....71
4. Act....72
G. DECEPTION PROCESS 72
1. Bell and Whaley 72
2. See-Think-Do....74
3. Revised Deception Process 74
V. PRACTICE OF MILITARY DECEPTION 77
A. DECEPTION PLANNING PROCESS....79
1. Mission Analysis....79
a. Information Requirements *79*
2. Planning Guidance....82
3. Planning Methodology....83
a. DO....*83*
b. THINK....*84*
c. SEE *84*
4. Deception Means 85
a. Physical....*85*
b. Cyber Electromagnetic....*86*
c. Administrative *87*
5. Execution and Assessment 88

Page 702 of 3957

a. Execution *88*
b. Assessment *89*
6. Termination 90
B. PRINCIPLES OF DECEPTION 91
1. Know the Target and Exploit Existing Perceptions 93
a. Understand the Target *93*
b. Exploit Existing Perceptions *93*
c. Avoiding Windfalls *94*
2. Security is Paramount 95
3. Utilize Flexibility, Variety, and Conditioning 96
a. Flexibility *96*
b. Variety *96*
c. Conditioning *97*
4. Coordination and Control 98
a. Control *98*
b. Coordination *98*
5. Requirement for Target Action 99
6. Preparation and Timing 99
7. Beware Unintended Consequences 100
C. DECEPTION IN SUPPORT OF IRREGULAR OPERATIONS 101
1. Unconventional Warfare 101
2. Counterinsurgency/Foreign Internal Defense 103
3. Stability Operations / Humanitarian Assistance Operations 104
4. Counterterrorism 105
5. Cyberwarfare 106
D. MILITARY DECEPTION FAILURES 106
VI. HISTORIC U.S. ARMY USE OF DECEPTION 109
A. REVOLUTIONARY WAR – BATTLE OF TRENTON 109
B. CIVIL WAR 110
1. Peninsula Campaign 110
2. Capture of Atlanta 111
3. Athens, Alabama 112
C. PHILIPPINE INSURRECTION – RAID ON PALANAN 113
D. WORLD WAR I – SAINT MIHIEL 115
E. DECEPTION IN WORLD WAR II 117
1. Operation FORTITUDE SOUTH 117
2. 23rd Headquarters Special Troops 119
3. Operation WEDLOCK 120
F. KOREAN WAR – INCHON LANDING 122
G. VIETNAM WAR 124
1. MACVSOG 124
a. Sacred Sword Patriots League *124*
b. Deception in Support of Security *126*
2. MACV 127
H. OPERATION DESERT STORM 129

Page 703 of 3957

VII. CONCLUSIONS AND RECOMMENDATIONS....133
A. CONCLUSION....133
B. RECOMMENDATIONS....134
1. Doctrine....135
2. Leadership, Education, and Training....136
3. Personnel Selection....138
4. Facilities....139
C. FINAL NOTE....139
LIST OF REFERENCES....141
INITIAL DISTRIBUTION LIST....153

Page 704 of 3957

LIST OF FIGURES

Figure 1. Timeline of Deception-Related Doctrine and Deception Proponents from 1905–2011 8
Figure 2. Comparison of Balance of Power and Doctrinal Emphasis of Deception 32
Figure 3. Daniel and Herbig's "Deception's Subsidiary Concepts." (From:) 42
Figure 4. Interrelationship of Truth, Deception, and Lies 43
Figure 5. Taxonomy of Deception 44
Figure 6. Communications Cycle 61
Figure 7. Expanded OODA Process (From:) 65
Figure 8. Bell and Whaley's Deception Planning Loop (From:) 73
Figure 9. Example of Bell and Whaley's Deception Planning Process in Action (From:) 73
Figure 10. Revised Deception Process 76

Page 705 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 706 of 3957

LIST OF TABLES

Table 1. Characteristics of Cumulative Destruction and Systemic Disruption.....27
Table 2. Chisholm and Feehan's Eight Ways to Deceive.....51
Table 3. Examples of Target Responses to Deception.....57
Table 4. Examples of Channels.....63
Table 5. Sample Deception Planning Resources 81
Table 6. Notional Execution Matrix Based on Events of Operation DESERT STORM....88
Table 7. Potential Termination Triggers 91
Table 8. Deception Fundamentals, Principles, and Maxims.....92
Table 9. Deception Analysis of Battle of Trenton 110
Table 10. Deception Analysis of Peninsula Campaign.....111
Table 11. Deception Analysis of Atlanta 112
Table 12. Deception Analysis of Athens, Georgia.....113
Table 13. Deception Analysis of Raid on Palanan.....115
Table 14. Deception Analysis of Saint Mihiel.....116
Table 15. Deception Analysis of Operation FORTITUDE SOUTH 118
Table 16. Deception Analysis of Operation KODAK.....120
Table 17. Deception Analysis of Operation WEDLOCK 122
Table 18. Deception Analysis of Operation CHROMITE.....123
Table 19. Deception Analysis of SSPL 126
Table 20. Deception Analysis of MACVSOG Security.....127
Table 21. Deception Analysis of DIAMOND I.....128
Table 22. Deception Analysis of Ranger Assault 128
Table 23. Deception Analysis of Operation DESERT STORM 131
Table 24. Recommended Personnel for Formal Deception Education.....137

Page 707 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APD	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
ARVN	Army of the Republic of Vietnam
ATTP	Army, Tactics, Techniques, and Procedures
C&D	Cover and Deception
CCD	Camouflage, Concealment, and Decoys (Army)
CCD	Camouflage, Concealment, and Deception (Joint)
D&D	Denial and Deception
DOTLMPF	Doctrine, Organization, Training, Leadership, Materials, Personnel, and Facilities
EEFI	Essential Elements of Friendly Information
FM	Field Manual
HUMINT	Human Intelligence
ICD	Imitative Communication Deception
IDF	Israeli Defense Forces
JOPES	Joint Operations Planning and Execution System
JP	Joint Publication
JSC	Joint Security Control
MACV	Military Assistance Command – Vietnam
MACVSOG	Military Assistance Command – Vietnam Studies and Observation Group
MD	Military Deception
MDMP	Military Decision Making Process
MED	Manipulative Electronic Deception
MISO	Military Information Support Operations

NCOIC	Non-commissioned Officer in Charge
NKPA	North Korean People's Army
NVA	North Vietnamese Army
OIC	Officer in Charge
OODA	Observe-Orient-Decide-Act
SOP	Standard Operating Procedures
TC	Training Circular
UNIFIL	United Nations Interim Force in Lebanon
VC	Viet Cong

ACKNOWLEDGMENTS

I would like to thank the faculty and staff of the Defense Analysis Department for providing this amazing experience. I am humbled by the collective knowledge and experience in this department. I would also like to thank Dr. Hy Rothstein and Dr. Kalev Sepp for their invaluable mentorship and advice, without which I would not have been able to complete this thesis. Thanks also to Zooey Lober and the rest of the hard-working and patient personnel at the Dudley Knox Library Interlibrary Loan desk for their tireless efforts in finding my esoteric, and often quixotic, requests. Additionally, I thank the myriad organizations who responded to my plaintive information requests, especially the folks at the United States Army Military History Institute. To my fellow students, thanks for the prodding and cajoling to tackle this topic, and for the opportunity to interact and learn from you. Finally, I have to thank my lovely wife, Christy, whose patient support and faith, both in this endeavor and my career, have been invaluable.

Page 711 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 712 of 3957

I. INTRODUCTION

> *For where the lion's skin will not reach, you must patch it out with the fox's.*
>
> *– Lysander the Spartan*[1]

During the opening phases of the 2006 Israeli-Hezbollah War, Israeli Defense Forces (IDF) hammered the network of Hezbollah bunkers along the Lebanese border. Hezbollah had been building the bunker network for years, under the watchful eyes of IDF surveillance, Lebanese spies working for Israel, and the United Nations Interim Force in Lebanon (UNIFIL), patrolled the southern Lebanese border. What the IDF did not realize until far too late was the network of bunkers so diligently—and visibly—emplaced by Hezbollah were decoys; Hezbollah's true bunkers were scattered across the countryside and covered by layers of security and camouflage. The bunker deception was but one of several cunning stratagems used by Hezbollah to blunt the IDF's technological and information advantages, allowing Hezbollah to maintain combat effectiveness in the face of the Israeli assault. Deception had once more proven its worth.[2]

A. BACKGROUND

Stratagems are essential in war, as commanders seek to hide their real intentions, capabilities, and actions from the enemy, while cunningly showing false intentions capabilities and actions to lure the enemy into defeat. From the earliest battles of antiquity, commanders have used guile and misdirection for tactical, operational, and strategic effect. Hannibal at Cannae, the Greeks' use of the Trojan Horse, and Gideon's raid on the Midianites are but a few examples of successful deception in the ancient world. Operations OVERLORD and BARBAROSA during WWII, British pseudo-operations

---

[1] Plutarch, John Dryden and Arthur Hugh Clough, *Plutarch's Lives*, Modern Library paperback ed., Vol. 1 (New York: Modern Library, 2001), 588.

[2] David A. Acosta, "The Makara of Hizballah: Deception in the 2006 Summer War" (Master's thesis, Naval Postgraduate School), 43 – 45, accessed 15 January 2012, http://handle.dtic.mil/100.2/ADA469918.

Page 713 of 3957

during the Mau-Mau insurgency in Kenya, and Hezbollah's use of deception against Israel during the 2006 war demonstrate the continuing utility of deception in the modern era.

Even within the more limited scope of U.S. Army history, deception has played an important role. General Washington utilized numerous stratagems to great effect during the Revolutionary war, including deceiving the British about the status of his forces at Valley Forge to deter attack, and later about his intentions to attack New York, setting the stage for the final showdown at Yorktown. During the Civil War, Confederate General Magruder used decoy cannons made of nothing more than painted tree trunks to hold Union forces in check for months after the First Battle of Manassas. General Pershing deceived the Germans about his intentions in order to gain surprise for the assault on the St. Michel salient during World War I.[3] U.S. use of deception reached a plateau during World War II. After a slow start, the U.S. Army became adept at using deception and by 1947 Chief of Staff of the Army, General Eisenhower [in a 1947 memo to the Lauris Norstad, Director, Plans and Operations Division] stated:

> …no major operations should be undertaken without planning and executing appropriate deception measures. As time goes on… there is a danger that these two means [psychological warfare and cover and deception] may in the future not be considered adequately in our planning. I consider it essential that the War Department should continue to take those steps that are necessary to keep alive the arts of… cover and deception and that there should continue in being a nucleus of personnel capable in handling these arts in case an emergency arises. I desire therefore that the Director of Plans and Operations maintain the potential effectiveness of these arts in order that their benefits may become immediately available, as and when desired, in furtherance of national security.[4]

During Vietnam, the Military Assistance Command Vietnam—Studies and Observation Group [MACVSOG] made extensive use of deception in its operations against

[3] Richard Baker, "The Lost and found Art of Deception" (Paper presented at the Conference of Army Historians, Arlington, Virginia, 25 – 28 July 2011).

[4] Dwight D. Eisenhower, *The Papers of Dwight David Eisenhower: The Chief of Staff*, ed. Louis Galambos, Vol. VIII (Baltimore: Johns Hopkins Press, 1978), 1763.

North Vietnam. During Operation DESERT STORM, U.S. forces deceived Saddam's forces into believing the assault into Kuwait would come from the sea, and not from the now famous "left hook."

In spite of the demonstrated utility of deception in support U.S. military operations, the U.S. Army currently falls short on the requirement to provide practitioners of deception with a solid doctrinal foundation in the theory and practice of deception. Instead, the U.S. Army has for the most part of two decades done little more than pay lip service to the importance of deception, or in the case of camouflage and concealment, stripped the concepts of their deception lineage. The last dedicated deception manual was published in 1988, and is no longer available through official channels. Furthermore, the 1957 and 1967 editions of the deception field manual have effectively disappeared.[5] Current U.S. Army doctrine, discounting uses of the word "deception" as a buzzword, is limited to a 30-page section in the information operations field manual that completely ignores essential tenets of deception like perceptual and cognitive biases. There is a need for a concise distillation of theory and practice for the military practitioners of deception.

B. HYPOTHESES

The degree of emphasis of deception in U.S. Army doctrine is primarily related to the perceived balance of power between the United States and potential adversaries.

There are essential tenets of the theory and practice of deception that can be drawn from the existing bodies of work.

C. SCOPE AND SIGNIFICANCE

What the literature review shows is there is a definite lack of guidance on the theory and practice of deception within current U.S. Army doctrine, despite a continuing theme in the doctrine that deception is of utility to operations. On the civilian side, there is a diversity of ideas on the theory and practice of deception; however, these ideas are

[5] The author's quest to find these manuals has included contacting each service academy and war college, all the proponents for deception; as well as, the U.S. Army Military History Institute, and the National Archives. These requests were in addition to the tireless and patient work of the Dudley Knox Library Staff. The vanishing of *FM 31-40* is indicative of the U.S. Army's habit of purging "obsolete" doctrine; a habit that perhaps merits its own thesis on the value of institutional knowledge.

dispersed over a large body of work. What is lacking in the civilian literature is an equivalent to the Grand Unification Theory in Physics, one work that distills the breadth and depth of the deception field into a usable synthesis. While not being so presumptuous as to present a Grand Unification Theory of deception, this thesis will bridge the gap in U.S. Army doctrine by creating a petite military deception focused synthesis of the body of deception work. This work is not intended to be proscriptive or all-inclusive; rather, the goal of the work is to provide commanders and practitioners a framework of concepts and ideas which can be altered to fit their organizational and operational needs. Central to this thesis is a reunification of cover with deception, as cover and active deception are mutually supporting concepts. The creation of an unclassified deception handbook will fill a doctrinal void and hopefully increase the perceived utility of deception within the force.

D. METHODOLOGY

The purpose of this thesis is to explore the breadth of U.S. Army military deception history and doctrine, and combine the insights gained with the various works on deception theory and practice, cognitive psychology, communications, and decision-making in order to distill the theory and practice of deception into a concise handbook for deception practitioners. Rather than attempting to cover the entirety of deceptive practices, the scope of this thesis is deception as employed in support of military objectives.

In order to achieve this goal, the thesis first constructs a longitudinal review of U.S. Army doctrine focusing on the capstone operations manual series and deception related manuals in order to discern whether there is a pattern to U.S. Army doctrine's treatment of deception. The scope of this survey is from the 1905 *Field Service Regualtions* through the 2012 *ADP 3-0*. Next the thesis examines the reasons commonly given for why deception is marginalized within military affairs. This examination is conducted through the lenses of doctrine and practice.

Then the thesis shifts to a distillation of the existing body work on deception to create a theory of deception in the military context. Within the theory of deception

chapter the focus will be on providing a cogent structure, taxonomy, and lexicon for deception with an emphasis on how deception works. The structure provided by Bell and Whaley's general theory of deception will be used as the initial framework. To the framework is added an understanding of the role of perceptional and cognitive biases in deception; a fleshed out lexicon of deception related terms; and a broad set of categories for deception techniques. This requires taking the mélange of existing works on deception and rendering the concepts down to a cohesive synthesis.

After deception theory, the thesis presents a synthesis of the practice of deception. The practice of deception chapter first presents a planning process that builds upon the planning process presented in *JP 3-13.4: Military Deception*. Next, the chapter reviews the various maxims, principles, and considerations presented by deception theorists and practitioners to draw out the essential elements of deception practice. Additionally, the chapter examines the uses of deception in war illuminated with examples from history. The practice chapter ends with a discussion of deception failures in order to reinforce the necessity of proper planning and execution.

A chapter surveying U.S. military use of deception from the Revolutionary War to Operation DESERT STORM follows the practice chapter in order to provide additional illumination in the context of historic U.S. operations. This chapter serves a secondary purpose of priming the mind of the reader by demonstrating the U.S. military has a long and storied history of using deception. Finally, a conclusions chapter provides recommendations on how to organize for deception operations, with ideas on manning, training, integration in the staff, and special resource requirements.

THIS PAGE LEFT INTENTIONALLY BLANK

Page 718 of 3957

II. DECEPTION IN U.S. ARMY DOCTRINE

Deception is common sense soldiering.

– General Carl E. Vuono[6]

According to *FM 1, The Army*, "Doctrine is the concise expression of how Army forces contribute to campaigns, major operations, battles, and engagements."[7] Furthermore, doctrine creates a shared culture for the force; standardizes operations; and provides a common frame of reference.[8] Thus any attempt to understand the role of deception within the U.S. Army must begin with an examination of U.S. Army doctrine. The U.S. Army has two capstone manuals that serve as the doctrinal foundations of the force; currently, these manuals are: *FM 1: the Army* and *APD 3-0: Unified Land Operations*.[9] *FM 1* serves as a broad overview of the U.S. Army's "fundamental purpose, roles, responsibilities, and functions, as established by the Constitution, Congress, and the Department of Defense."[10] *APD 3-0* serves as the "overarching doctrinal guidance and direction for conducting operations."[11] In addition to these capstone documents, it is necessary to examine other doctrine publications directly related to the various aspects of deception. Each of these manuals in its various incarnations over time plays a vital role in setting the conditions for the role, or lack of a role, of deception in U.S. Army operations.

The adjectives best describing the U.S. Army's historical and present guidance on deception are haphazard and shallow. Within the operations field manuals are statements to "use deception" sprinkled about almost as an afterthought. Only rarely are any statements approaching the strength of General Eisenhower's about the essential

---

[6] Quoted in Center for Army Lessons Learned, *CALL Bulletin 3-88: Deception* (Fort Leavenworth, KS: Combined Arms Training Activity, 1988), 3.

[7] Headquarters, Department of the Army, *Field Manual 1: The Army, 2005* (Washington, DC: Department of the Army, 2005), 1-20.

[8] Headquarters, Department of the Army, *Field Manual 1: The Army, 2005*, 1-20 to 1-21.

[9] Each of these manuals has undergone name and nomenclature changes over their history.

[10] Headquarters, Department of the Army, *Field Manual 100-1: The Army* (Washington, DC: Department of the Army, 1994), v.

[11] Headquarters, Department of the Army, *Army Doctrine Publication 3-0: Unified Land Operations* (Washington, DC: Department of the Army, 2011), ii.

importance of deceptions in every operation. Discussion of how deception works is either missing or disregarded. For example, in *FM 3-13*, the section on exploiting target biases states that the target's biases can be "the most powerful weapon in the MD [military deception] planner's arsenal;" however the very next sentence obliterates the importance of the target's biases with "However, such information is not essential to preparing a viable MD plan."[12]

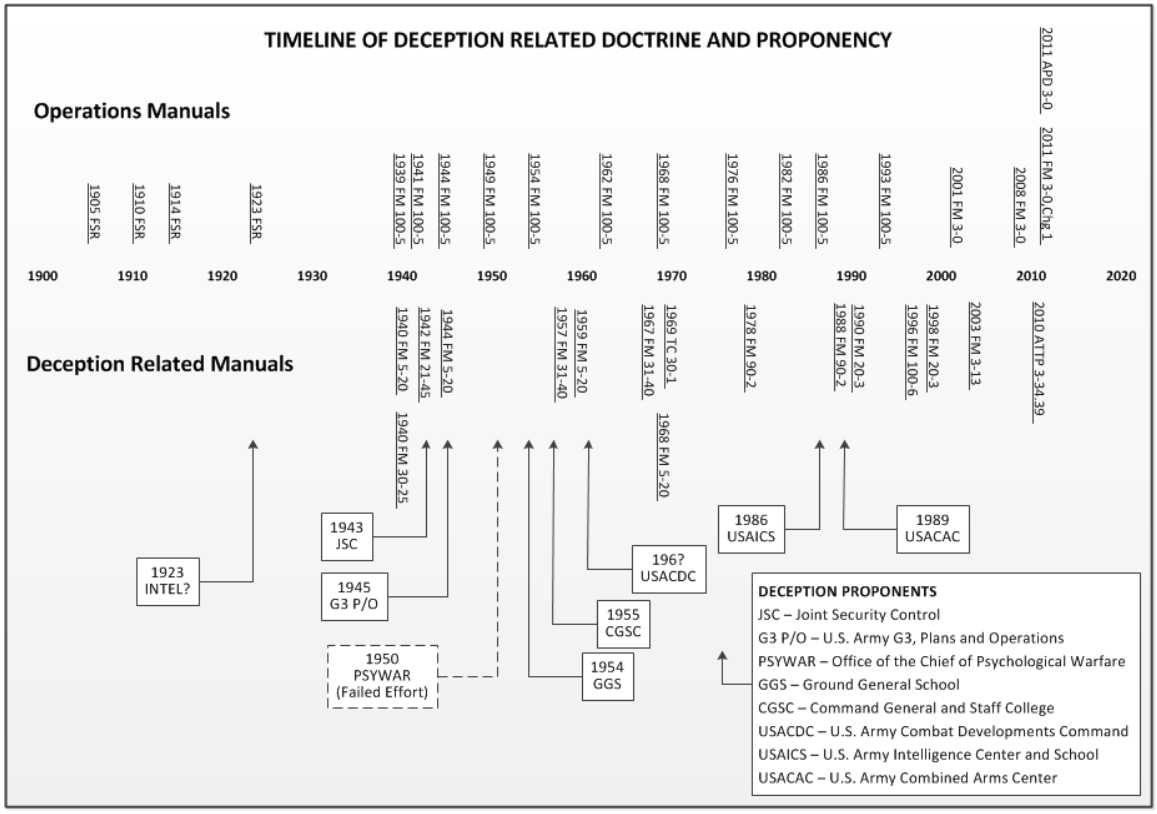


Figure 1. Timeline of Deception-Related Doctrine and Deception Proponents from 1905–2011

A. PRE-WORLD WAR II ERA

Discussion of the concept of deception in U.S. military doctrine prior to the World War II era was minimal, and when present often negative. The 1905 edition of the War Department's *Field Service Regulations* admonishes there will be no quarter

[12] Headquarters, Department of the Army, *Field Manual 3-13: Information Operations: Doctrine, Tactics, Techniques, and Procedures* (Department of the Army, 2003), 4-9.

Page 720 of 3957

expected for troops utilizing the enemy's uniform for "treacherous advantage," and advised commanders forced to use pieces of the enemy's uniform in extremis to maintain sufficient difference from the enemy's ensemble so as to avoid the charge of willful deception.[13] Where concealment is discussed, it is almost purely in association with force protection, with only one mention of concealing trench works in the defense to set the stage for an "ambuscade."[14] The 1910 edition eliminates much of the discussion on perfidy and wrongful deception, and increases the mentions of surprise and concealment. However, discussion of deceiving the enemy is limited to cryptic comments like: "If it is desirable to annoy or deceive the enemy, the supreme commander gives the necessary orders."[15] In the 1914 edition of *Field Service Regulations* the main discussion of surprise is in the context of an imperative to not be surprised.[16] While the term deception is not used in the manual, deceiving the enemy is given as a primary purpose for holding attacks.[17] Amusingly, the other major reference on the topic of deception occurs in the guidance on war correspondents.[18]

The 1923 edition breaks from the preceding editions, representing the hard learned lessons of World War I. The manual introduces the concept of counterinformation, that is, the measures designed to prevent the adversary from gaining information on friendly capabilities, dispositions, and plans. Counterinformation effectively constitutes the deception principle of hiding the real. Of particular note is the value placed on camouflage throughout the manual. In addition to efforts to deny information, counterinformation is supported by means designed to mislead or deceive

[13] War Department, *Field Service Regulations, United States Army. 1905, with Amendments to 1908* (Washington, DC: Government Printing Office, 1908), 200; This is possibly a reaction to the backlash against Colonel Funston's use of enemy uniforms during the Philippine Insurrection.

[14] War Department, *Field Service Regulations.1905*, 102.

[15] War Department, *Field Service Regulations, United States Army. 1910* (Washington, DC: Government Printing Office, 1910), 76.

[16] War Department, *Field Service Regulations, United States Army. 1914* (New York, NY: Government Printing Office, 1914), 80.

[17] War Department, *Field Service Regulations. 1914*, 84 – 85.

[18] War Department, *Field Service Regulations. 1914*, 168.

the enemy.[19] In a complete reversal from the 1914 manual, surprise is now presented as vital to all combat actions, with feints and demonstrations presented as ways of gaining surprise.[20] Furthermore, surprise and deception are considered essential to the successful execution certain operations, e.g., river crossings.[21] While still insignificant in the context of the entirety of the manual, the inclusion of deception concepts indicates some lessons learned during World War I, such as General Pershing's use of deception during the offensive against the Saint Mihiel salient, were taken to heart.[22]

B. WORLD WAR II ERA

The intriguing anomaly in U.S. military doctrine prior to and during the World War II era is the presence of the concept of deception. Though cursory, the inclusion of both the covering and deceiving aspects of deception within U.S. doctrine runs counter to the prevailing conventional wisdom that the U.S. military was a deception neophyte until the capability was nurtured under the tutelage of its British counterparts. Building on the 1923 *Field Service Regulations*, the 1939 operations manual, now *FM 100-5: Tentative Field Service Regulations: Operations*, establishes deception's role in support of surprise, stating: "The effect of surprise is dependent on… the effectiveness of the means employed to deceive the enemy of our own dispositions and intentions."[23] The cover aspect of deception remains incorporated in the section on counterinformation, or "…measures taken to prevent the enemy from gaining information relative to our dispositions, movements, and plans."[24] Additionally, active deception becomes more strongly tied to counterinformation, with the manual stating: "Counterinformation is supplemented by positive measures designed to deceive or mislead the enemy as to our dispositions and intentions;" however, while counterinformation is provided a page and a

[19] War Department, *Field Service Regulations, United States Army. 1923* (Washington, DC: Government Printing Office, 1924).

[20] War Department, *Field Service Regulations. 1923*, 77.

[21] War Department, *Field Service Regulations. 1923*, 118.

[22] See Chapter VI for further discussion of the Saint Mihiel deception operation.

[23] War Department, *Field Manual 100-5: Tentative Field Service Regulations of Operations, 1939* (Washington, DC: Government Printing Office, 1939), 28 – 29.

[24] War Department, *Field Manual 100-5: Tentative Field Service Regulations*, 41.

half, the "postive measures" are not described in any detail.[25] Interestingly, within the types of operations, deception—again without detail—is only mentioned in the section on guerrilla warfare, as if this is the only appropriate time. Here, the manual states:

> The *attack* [emphasis in original] on the enemy is made by surprise obtained by deception and ambush…. By feint and demonstration… by spreading false information, the attacker attempts to mislead the enemy….[26]

In the 1941 edition, now *FM 100-5: Field Service Regulations*, the term counterinformation is replaced by counterintelligence. The set of tasks bundled under the aegis of counterintelligence includes: counterespionage, cover, measures designed to deceive the enemy, counterpropaganda, and censorship.[27] Thus active deception completes the integration into counterintelligence started in preceding editions. The counterintelligence section includes three paragraphs on active deception, and includes a prompt designed to spur the egos of commanders: "A commander who is ingenious and resourceful in the use of tactical stratagems [*sic*] and ruses often will find methods of deceiving or misleading the enemy and of concealing his own intentions."[28] Of note is the inclusion of several examples of deception techniques: e.g., feints, demonstrations, fake concentrations, and dummies. However, the section also includes a combined warning and constraint that since deception creates the danger of misleading one's own forces: "Such measures may be adopted only by the theater commander or by his authority."[29] Throughout the manual, deception is integrated into discussions on the various types of operations; such as, the use of simulated activities by screening forces to facilitate a retrograde maneuver, and the use of feints during mountain operations.[30] Despite the incorporation of deception across the manual, there are two notable

---

[25] War Department, *Field Manual 100-5: Tentative Field Service Regulations*, 42.

[26] War Department, *Field Manual 100-5: Tentative Field Service Regulations, 1939*, 228 – 229.

[27] War Department, *Field Manual 100-5: Field Service Regulations of Operations, 1941* (Washington, DC: Government Printing Office, 1941), 57.

[28] War Department, *Field Manual 100-5: Field Service Regulations, 1941*, 58.

[29] War Department, *Field Manual 100-5: Field Service Regulations, 1941*, 58.

[30] For deception in support of the retrograde, see War Department, *Field Manual 100-5: Field Service Regulations, 1941*, 169. For deception in support of mountain operations, see page 220.

inconsistencies. First in a curious change from the 1939 manual, the section on partisan warfare, which replaces the 1939 section on guerrilla warfare, is devoid of deception. Second, in opposition to the overall tenor of deception as a useful tool, the manual seems to undercut the utility of deception in the offense stating:

> The degree of surprise attained is dependent in a large measure on the coordination and timing of the measures taken to deceive the enemy. Ruses, demonstrations, feints, and other measures for deception executed at the wrong time and place will be obvious to an alert enemy and will warn him of the impending attack. Superior mobility and speed of execution may be determining factors in achieving surprise.[31]

In addition to the operations manual, during this period there were several other manuals directed related to deception. *FM 30-25: Basic Field Manual of Military Intelligence Counterintelligence* expands the guidance of *FM 100-5* with sections on each of the aspects of counterintelligence. Though the section on tactical measures—feints, demonstrations, and ruses—is unfortunately a verbatim repeat of the section in *FM 100-5*, the counterintelligence manual is a de facto deception manual as it provides in depth detail on the cover aspects of concealment and denial through the manual's emphasis on depriving the enemy access to friendly information. In keeping with the constraint imposed by *FM 100-5*, while the manual encourages commanders to embrace most aspects of deception, false information—e.g., the deliberate loss of notional orders—is restricted to the discretion of the theater commander out of the risk that friendly plans will act on the assumption the enemy has been deceived.

FM 21-45: Basic Field Manual of Protective Measures, Individuals and Small Units, published in 1942, provides further guidance on concealment at the Soldier and unit levels; as well as, reinforcement of the vital necessity to protect military information. Notably, *FM 21-45* sets more stringent guidance for protecting information than current doctrine; for example, the manual states:

> Prior to going into combat, all distinguishing marks and insignia on vehicles, equipment, or persons will be removed or obliterated under an officer's supervision. You must be careful to remove divisional, regimental, or company insignia from your clothes and equipment. Search

[31] War Department, *Field Manual 100-5: Field Service Regulations, 1941*, 109.

> your pockets for letters, memoranda, orders, souvenirs, or keepsakes which might disclose your organization.[32]

Additionally, while cover at this time is coupled with deception, the War Department and later the U.S. Army have published a separate manual for camouflage since at least 1940. Despite being treated separately from cover and deception, camouflage was intrinsically linked to both concepts until the late 1960s. The 1940 edition of *FM 5-20: Engineer Field Manual, Camouflage* lists three methods of camouflage: hiding, blending and deceiving.[33] The 1944 edition expands upon the theme of camouflage and deception, devoting an entire chapter to the subject of deceiving camouflage.[34] Furthermore, the 1944 edition states:

> Camouflage uses concealment and deception to promote our offensive action, to surprise, to mislead the enemy, and to prevent him from inflicting damage upon us. Concealment includes hiding from view, making hard to see clearly, arranging obstructions to vision, deceiving and disguising, and deception involving sound.[35]

C. POST WORLD WAR II THROUGH VIETNAM

While the 1944 edition of *FM 100-5* is essentially the same as the 1941 edition, the 1949 edition of *FM 100-5* differs in two critical ways with regards to deception. First, this edition of the operations manual introduces a distinct set of principles of war, with surprise being one.[36] Second, though counterintelligence continues to include means to deceive the enemy, the separate paragraphs on deception present in the two previous editions are absent.[37] The separation of deception from counterintelligence possibly reflects the shift of deception proponency from the Joint Security Control to the Army

---

[32] War Department, *Field Manual 21-45: Basic Field Manual of Protective Measures, Individuals and Small Units* (Washington, DC: Government Printing Office, 1942), 137.

[33] War Department, *Field Manual 5-20: Engineer Field Manual of Camouflage, 1940* (Washington, DC: War Department, 1940), 3.

[34] War Department, *Field Manual 5-20: Camouflage Basic Principles, 1944* (Washington, DC: War Department, 1944).

[35] War Department, *Field Manual 5-20, 1944*, 4.

[36] Headquarters, Department of the Army, *Field Manual 100-5: Field Service Regulations—Operations, 1949* (Washington, DC: Department of the Army, 1949), 21 – 23.

[37] Headquarters, Department of the Army, *Field Manual 100-5, 1949*, 43 – 46.

G3, Plans and Operations Division. The lack of detail on the execution of deception is perhaps best explained by a training memorandum from the Office of the Chief of Army Field Forces to the commanders of the Armor, Infantry, and Artillery Centers. This declassified memorandum reveals the intent of the Army to keep the lessons learned from World War II well under wraps: "The security classification of this whole subject [strategic cover and deception] is and probably will remain TOP SECRET…."[38]

In 1950, Brigadier General McClure campaigned for the establishment of a psychological warfare division within the Department of Army Special Staff. This division was to have purview over psychological operations, cover and deception, and unconventional warfare; however, when the Office of the Chief of Psychological Warfare was established in 1951, cover and deception were not included in the scope of the office's operations.[39] In 1954, proponency for deception was assigned to the Ground General School, specifically to the Aggressor Center at Fort Riley, Kansas.[40] This decision was the General Staff's halfhearted response to a request from the Commander, Army Field Forces for a purpose built unit trained in deception along the lines of the 23rd Headquarters Special Troops in World War II.[41] The decision to place deception under the Aggressor Center given the Aggressor Center's role as a professional opposing force seems to demonstrate how quickly the Army drifted from General Eisenhower's admonishment.

The 1954 edition of *FM 100-5* represents another fundamental revision of the manual; as well as, both the apex of discussion of deception activities within the capstone document and the beginnings of deception's dismemberment. This iteration of *FM 100-5*

---

[38] Office of the Chief of Army Field Forces, *Strategic and Tactical Cover and Deception Training* (Fort Monroe, VA: Department of the Army, 1948).

[39] Alfred Paddock Jr, *US Army Special Warfare. Its Origins: Psychological and Unconventional Warfare, 1941 – 1952* (Washington, DC: National Defense University, 1982), accessed 12 February 2012, http://handle.dtic.mil/100.2/ADA118758, 89.

[40] Concepts and Force Design Group, *Tactical Cover and Deception: Final Report* (Alexandria, VA: U.S. Army Combat Developments Command, 1972), accessed 8 August 2011, https://www.dtic.mil/DOAC/document?document=ADB966185&collection=ac-tr&contentType=PDF&citationFormat=1f , 1-3.

[41] U.S. Department of the Army. General Staff, G-3, "Combat Deception," (1954), Photocopy from U.S. Army Military History Institute, Carlisle, PA.

separates active deception from counterintelligence into a distinct three page section on "combat deception" that includes subsections on the importance of military deception; the fundamentals of military deception; security considerations; planning; and means. The manual advises: "It is imperative that commanders constantly realize the importance of combat deception and that they train their troops and staff in the techniques and planning for combat deception."[42] Though the split of deception from counterintelligence elevates the status of deception within the manual, the split has the negative effect of separating deception from the security aspects of cover. Furthermore, while deception is still considered a tool of surprise, a new principle of war, economy of force, admonishes that deception—along with limited attacks, retrogrades, and the defense—is only to be used in non-critical areas in support of the concentration of forces at the decisive point.[43] This admonishment runs counter to deception's economy of force role, and could only serve to dissuade the use of deception.

In 1955, the Ground General School was discontinued and deception proponency was transferred along with the aggressor cadre to the Command and General Staff College.[44] In 1957, the U.S. Army published a field manual dedicated to deception, *FM 31-40*: *Tactical Cover and Deception;* however, this manual was classified 'confidential,' effectively placing it, and therefore detailed deception guidance, out of reach of much of the force. As a consequence of the manual's publication, the 1962 iteration of *FM 100-5* truncates the section on military deception to two paragraphs on the utility of deception that close with a reference to *FM 31-40*. At the same time, the cover aspects of counterintelligence and camouflage remain intact. Despite the removal of deception guidance to *FM 31-40*, this *FM 100-5* continues the trend of deception being an important part of operations: "Tactical cover and deception plans are an integral part of

[42] Headquarters, Department of the Army, *Field Manual 100-5: Field Service Regulations—Operations, 1954* (Washington, DC: Department of the Army, 1954), 37 – 39.

[43] Headquarters, Department of the Army, *Field Manual 100-5: 1954*, 47.

[44] Headquarters, Department of the Army, *General Orders no. 20* (Alexandria, VA: Department of the Army, 1955), www.armypubs.army.mil/epubs/pdf/go5520.pdf.. The aggressor cadre was a permanent opposing force designed to provide realism to Army training exercises. The aggressor cadre was equipped with numerous deception aids, including sonic platoons—elements outfitted with loudspeaker equipped vehicles and weapon simulation devices for conducting audio deceptions. See *FM 30-101 (1959)* for more information on the aggressor cadre.

all operations planning."[45] Furthermore, this edition of the operations manual includes tactical deception units as a type of combat support element—possibly a reference to the sonic deception units assigned to the aggressor cadre.[46] The 1968 version of *FM 100-5*, *Operations of Army Forces in the Field* repeats the short section on deception and a reference to *FM 31-40*. However, missing from this edition of *FM 100-5* is any reference to dedicated deception units as combat support elements; instead, tactical cover and deception is listed as a task of engineering units.[47] At some point in the early 1960s proponency for deception was transferred from Command and General Staff College to the U.S. Army Combat Developments Command.[48]

FM 31-40 was updated with changes in 1960 and 1963, and a still classified update to *FM 31-40* was published in 1967. [49] In 1969, the U.S. Army published *Training Circular 30-1: Tactical Cover and Deception* (*TC 30-1*), an unclassified document providing guidance on the training of cover and deception from the company to division level, with the stated intent of encouraging commanders to include cover and deception in their planning process.[50] In 1973 an update was drafted but not published. Currently none of the editions of *FM 31-40* are available for examination, though an idea of their contents can be drawn from *TC 30-1*. The circular provides a basic overview of the history of deception; definitions of key terms and concepts; general guidelines, responsibilities, and considerations for planning of deception operations; and example

[45] Headquarters, Department of the Army, *Field Manual 100-5: Field Service Regulations—Operations, 1962* (Washington, DC: Department of the Army, 1962), 50.

[46] Headquarters, Department of the Army, *Field Manual 30-101: Aggressor, the Maneuver Enemy, 1959* (Washington, DC: Department of the Army, 1959), 55 – 57.

[47] Headquarters, Department of the Army, *Field Manual 100-5: 1962*, 39.

[48] This shift occurred prior to the still classified 1965 U.S. Army Combat Development Command report titled "Army Requirements for Tactical Deception."

[49] The official changes are noted on the entry for the 1967 edition of *FM 31-40* on the Combined Arms Research Library website. http://comarms.ipac.dynixasp.com/ipac20/ipac.jsp?menu=search&aspect=subtab316&npp=25&ipp=20&spp=20&profile=carlcgsc&ri=2&source=~!comarms&index=BIB&term=334188&x=0&y=0&aspect=subtab316

[50] Headquarters, Department of the Army, *Training Circular No. 30-1: Tactical Cover and Deception* (Washington, DC: Department of the Army, 1969), 3.

applications of deception. Of particular note is the planning consideration of target reaction, which demands a thorough understanding of the target:

> Success of cover and deception is dependent on the ability of the deceiver to predict the probable enemy reaction. The staff charged with the deception planning must be able to think as the enemy does and not react as a friendly commander transplanted into the enemy situation. This is possible only as a result of a thorough understanding of the enemy, his culture, and military system. The enemy intelligence system must be evaluated because this system is the vehicle that carries the deception story to the enemy commander. Determination must be made regarding the enemy's characteristics, his habits that make him vulnerable to deception, and those aspects that present the least likely deception target. The probable enemy reaction depends on the commander. An uncertain commander may react to deception while a steadfast veteran commander may ignore all but exceptionally convincing efforts. Some commanders may be overanxious, others overcautious; if possible, we should know the characteristics of the enemy commander, to include the degree of freedom allowed subordinates, his reaction time to new situations, and how this fear of the unknown influences his actions. A single known characteristic of a commander is more important than the entire statistical record of his military career.[51]

The one major drawback of *TC 30-1* is that since *FM 31-40* was classified, the information in *TC 30-1* with regards to means, techniques and examples of application is unfortunately shallow.

Looking at the camouflage aspect of deception, the 1959 edition of *FM 5-20* represented the pinnacle of the linkage between camouflage and cover and deception. In the manual's discussion of the nuclear battlefield, the manual explicitly states the role of camouflage in both denying information and deceiving:

> The best means of reducing the chance of a unit becoming the target of nuclear attack is to deny the enemy information as to the unit location and strength, or to fool the enemy by deception. Habitual use of proper camouflage will greatly assist in denying this information to the enemy.[52]

---

[51] Headquarters, Department of the Army, *Training Circular No. 30-1*, 15.

[52] Headquarters, Department of the Army, *Field Manual 5-20: Camouflage Basic Principles and Field Camouflage, 1959* (Washington, DC: Department of the Army, 1959), 3.

Additionally, *FM 5-20* emphatically bound camouflage to deception via the very definition of camouflage: "Camouflage is a French word meaning disguise and is used to describe actions taken to mislead the enemy by misrepresenting the true identity of an installation, an activity, or an item of equipment."[53] Finally, the manual reinforced camouflage's linkage to cover and deception to the point of subordinating camouflage to deception: "Camouflage, as an element of military deception, permits us to approach unseen and to remain hidden within striking distance of the enemy."[54]

Between the 1959 edition of *FM 5-20* and its successor in 1968, the relationship between camouflage and deception was severed. In the 1968 edition of *FM 5-20*, the third method of camouflage was changed from "deceiving" to "disguising."[55] Though deception was still discussed in the manual, to include a chapter on decoys, the concept of camouflage as an element of deception was thoroughly expunged. The divorce of camouflage from deception was reciprocated on the deception side of doctrine. The 1969 *TC 30-1* listed *FM 5-20* as a reference; however, the 1978 *FM 90-2: Tactical Deception* did not.

D. POST VIETNAM ERA THROUGH DESERT STORM

The 1976 edition of *FM 100-5* is an anomaly within the operations series as the manual is fixated squarely on the operations of a numerically smaller force against numerically superior Soviet forces in Western Europe. Though the distinct section on deception present in previous editions is absent, deception remains thoroughly integrated in the manual. For example, the following guidance is given for the offense: "If a smaller force is to concentrate superior combat power at the point of decision… commanders must employ surprise and deception as well as the full mobility of the force."[56] Furthermore, one of the basic tasks of the covering force in the defense is to deceive the

---

[53] Headquarters, Department of the Army, *Field Manual 5-20: 1959*, 3.

[54] Headquarters, Department of the Army, *Field Manual 5-20: 1959*, 4.

[55] Headquarters, Department of the Army, *Field Manual 5-20: Camouflage, 1968* (Washington, DC: Department of the Army, 1968), 20.

[56] Headquarters, Department of the Army, *Field Manual 100-5: Operations, 1976* (Washington, DC: Department of the Army, 1976), 3-6 to 3-7.

enemy, and deny information on friendly force dispositions.[57] In the section on desert warfare, the manual states, "using deception is a primary means of obtaining success."[58] However, despite the relatively complete integration of deception into operations, details on how to execute deception activities are again absent. Oddly, no mention is made of a deception manual within the body of the manual, though *FM 90-2* is listed in the references.[59]

The 1982 and 1986 editions of *FM 100-5* introduce the concept of Airland Battle, a fundamental revision of how the U.S. Army conducts operations. The Airland Battle approach places the principle of maneuver in primacy and embraces Liddell Hart's indirect approach.[60] As a result, deception is integrated into the 1982 and 1986 editions of *FM 100-5* to an unprecedented—and unrepeated—degree. Deception is included in the list of major functional areas alongside maneuver, intelligence, and fires.[61] In addition, deception is listed as a reason for offensive action, and discussed in depth in the sections on defense and retrograde operations.[62] Furthermore, echoing General Eisenhower's admonishment, the 1986 edition of *FM 100-5* states: "An integral part of any plan of campaign or major operation is the deception plan…. Deception is a vital part of tactical operations as well."[63] The dedicated section on deception, though smaller than the one in the 1954 edition, is still robust and includes examples of deception integration; as well as, some planning guidance.[64] The section on electronic warfare includes mention of manipulative electronic deception [MED] and imitative communications deception [ICD]

---

[57] Headquarters, Department of the Army, *Field Manual 100-5: 1976*, 5-10.

[58] Headquarters, Department of the Army, *Field Manual 100-5: 1976*, 14-10

[59] The reference to *FM 90-2* is bizarre given *FM 90-2* was not published until two years after this edition of *FM 100-5*. *FM 31-40* (1967) was the current deception manual at the time of publication.

[60] Headquarters, Department of the Army, *Field Manual 100-5: Operations, 1982* (Washington, DC: Department of the Army, 1982), 9-1.

[61] Headquarters, Department of the Army, *Field Manual 100-5: Operations, 1986* (Washington, DC: Department of the Army, 1986), 40.

[62] For offensive operations see: Headquarters, Department of the Army, *Field Manual 100-5: 1986*, 94; for defensive operations see: Headquarters, Department of the Army, *Field Manual 100-5: 1982*, 11 – 12; for retrograde operations see: Headquarters, Department of the Army, *Field Manual 100-5: 1986*, 158.

[63] Headquarters, Department of the Army, *Field Manual 100-5: 1986*, 53.

[64] Headquarters, Department of the Army, *Field Manual 100-5: 1986*, 53.

as electronic warfare activities that support the overall deception plan.[65] In a striking departure from previous operations manuals, the 1982 edition removes deception from the discussion of surprise as a principle of war, instead moving deception to the principle of security.[66]

In 1978, the U.S. Army retrieved the dedicated military deception manual from classified purgatory and published the unclassified *FM 90-2*: *Tactical Deception.* As the title implies, the focus of *FM 90-2* is with only the tactical fight: "…tactical deception here refers to short-term actions of corps or lower units within the battle area."[67] Though this "How to Fight" manual is rather simplistic, its release marked the beginning of a military deception renaissance within the U.S. Army. Of note however, the 1978 field manual severs the connection between deception and the term cover, though it maintains camouflage and concealment as aspects of visual deception. Despite these limitations, *FM 90-2* provides a workable foundation of deception practice, principles, and planning considerations.

In 1986 proponency for deception was transferred to the U.S. Army Intelligence Center and School at Fort Huachuca. Shortly afterwards, *FM 90-2* was updated as *FM 90-2: Battlefield Deception.* The 1988 iteration of *FM 90-2* is an intellectually weighty tome, delving into the cognitive underpinnings of deception as well as providing detailed guidance on the planning and execution of deception at both the tactical and operational levels of war. This manual was designed to address what the U.S. Army considered to be a shortfall in deception integration:

> Today, commanders use little deception in planning, directing, and conducting combat operations. As a result, many deception-related skills that have served our Army well in the past have been forgotten, and where remembered, have not been made part of our war-fighting capabilities Armywide.[68]

---

[65] Headquarters, Department of the Army, *Field Manual 100-5: 1982*, 7-19.

[66] Headquarters, Department of the Army, *Field Manual 100-5: 1982*, B-4.

[67] Headquarters, Department of the Army, *Field Manual 90-2: Battlefield Deception (HTF)* (Washington, DC: Department of the Army, 1978), 1-1.

[68] Headquarters, Department of the Army, *Field Manual 90-2: Battlefield Deception* (Washington, DC: Department of the Army, 1988), 1-0.

Without having access to the editions of *FM 31-40* for comparison, the 1988 edition of *FM 90-2* represents the strongest presentation of deception theory and practice within U.S. Army doctrine. Shortly after the publication of this edition, deception proponency was shifted once more, to the U.S. Combined Arms Center, where it remains.

E. POST COLD WAR ERA

Despite the successful use of deception in Operation DESERT STORM, the 1993 edition of *FM 100-5* almost appears to be a repudiation of the prior editions with regards to deception, and marks the beginning of deception's descent into a doctrinal abyss. Among the principles of war, deception is absent from security, and relegated to a mere factor of surprise; furthermore, economy of force demands force allocations for tasks such as deception be measures so as to not detract from the ability to mass at the decisive point.[69] Deception is not listed as a combat function; rather, deception is relegated to a single mention as one of the tasks contributing to mobility and survivability.[70] Finally, the robust section on deception in the 1986 edition is replaced by a two paragraph recitation of the definition of deception and guidance to see *FM 90-2* for further information. Though the term deception continues to appear throughout the manual, the overall marginalization of the concept of deception from the previous manuals is striking. A possible explanation for the marginalization of deception lies in the shift of the strategic equation with the fall of the Soviet Union. The collapse of the Soviet Union left the United States without a peer competitor, and thus without the need for indirect approaches to compensate for numerical inferiority and vulnerable lines of communication.[71]

The marginalization of deception continued outside the operations manual. In 1997, the U.S. Army's Combined Arms Center rescinded *FM 90-2* without replacement.

---

[69] Headquarters, Department of the Army, *Field Manual 100-5: Operations, 1993* (Washington, DC: Department of the Army, 1993), 2-5.

[70] Headquarters, Department of the Army, *Field Manual 100-5, 1993*, 2-14.

[71] See Chapter III for further discussion of the relationship between deception integration and perceived balance of power.

The stated reason was that the manual "no longer represents valid Army doctrine."[72] In 1998, an unofficial military deception planner's guide was published with a SECRET classification, again putting the tenets of deception outside the reach of a majority of the force. Additionally, since this was an unofficial document, it is given no reference in subsequent editions of *FM 100-5*. With the rescinding of *FM 90-2*, deception was subsumed by the emerging concept of information operations and incorporated into the 1996 *FM 100-6: Information Operations* as little more than a buzzword. Absent from *FM 100-6* is any guidance on the planning and execution of deception operations; as well as, any mention of the cognitive and theoretical foundations discussed in *FM 90-2*. *FM 3-13*: *Information Operations* replaced *FM 100-6* in 2003. Though *FM 3-13* provides more discussion on the integration, planning, and execution of deception than FM 100-6, the level is still far below *FM 90-2*. Furthermore, *FM 3-13* has fallen out of favor itself and is no longer in synch with *ADP 3-0*, limiting the manual's appeal.

In the 2001 iteration of the operations manual, now *FM 3-0, Operations*, deception continues its path into doctrinal oblivion. In keeping with the model of *FM 100-6*, deception is relegated to being an element of information operations, and an aspect of information superiority. While deception returns to the discussion of the principle of security, deception is absent from the principle of surprise.[73] The separate section on deception is limited to a single paragraph which restates the definition of military deception; gone is the guidance to refer to a deception field manual because the 1988 version of *FM 90-2* was phased out without replacement. As with the 1993 *FM 100-5*, the term deception is present, but the concept is not.

The 2008 edition of *FM 3-0* sees deception, now categorized as an information task, again limited to a single paragraph with a reference to *FM 3-13: Information Operations* and the joint forces publication on military deception, *JP 3-13.4: Military*

[72] Memorandum signed by Colonel Clinton J. Ancker III, Director, Corps and Division Doctrine, dated 30 September 1996 as cited in Bradley K. Nelson, "Battlefield Deception: Abandoned Imperative of the 21st Century" (Monograph, U.S. Army Command and General Staff College, 1997), 28, accessed 2 January 2012, http://handle.dtic.mil/100.2/ADA339425.

[73] Headquarters, Department of the Army, *Field Manual 3-0: Operations, 2001* (Washington, DC: Department of the Army, 2001), 4-14.

Deception. For the first time since 1914, the concepts of feints and demonstrations—in fact, the very words—do not appear within the operations manual. The early 2011 change to *FM 3-0* gives deception three paragraphs as an element of inform and influence activities, though there is a note stating: "military deception will migrate to another functional area in future editions of *FM 3-0*."[74] Interestingly, this edition does not reference the still current *FM 3-13* for deception guidance, rather it points to *JP 3-13.4*, the joint force publication. *ADP 3-0: Unified Land Operations* superseded *FM 3-0* as part of the Army's "Doctrine 2015" program. *APD 3-0*, weighing in at a concise 32 pages, does not mention deception at all, and relegates all inform and influence operations to three uses of the term without elaboration or mention of external references.

The 1990 edition of *FM 5-20*, renamed *FM 20-3: Camouflage*, further reduces the relationship of camouflage to deception by removing the chapter on decoys and stating that camouflage and deception are part of a set of interrelated tactical measures supporting survivability.[75] In 1998, *FM 20-3: Camouflage, Concealment and Decoys* introduces the term Camouflage, Concealment, and Decoys [CCD]. It is important to note the level of the disjunction between deception and cover at this point. While at the Army level the acronym CCD means the aforementioned Camouflage, Cover, and Decoys; at the joint level CCD means Camouflage, Concealment, and Deception [the Army refers to the joint version of CCD as JCCD]. Further, whereas the 1990 edition includes deception in the interrelated tasks supporting survivability, the 1998 edition removes deception. While essentially ignoring the connection between deception and camouflage, *FM 20-3* does ironically state in a standalone paragraph in its introduction:

> Deception helps mask the real intent of primary combat operations and aids in achieving surprise. Deception countermeasures can delay effective enemy reaction by disguising information about friendly intentions, capabilities, objectives, and locations of vulnerable units and facilities.[76]

---

[74] Headquarters, Department of the Army, *Field Manual 3-0: Operations, Change 1* (Washington, DC: Department of the Army, 2011), 6-19.

[75] Headquarters, Department of the Army, *Field Manual 20-3: Camouflage, 1993* (Washington, DC: Department of the Army, 1990), 1-1.

[76] Headquarters, Department of the Army, *Field Manual 20-3: Camouflage, Concealment, and Decoys, 1999* (Washington, DC: Department of the Army, 1999), 6.

The 2010 iteration of the Army's camouflage doctrine, *ATTP 3-34.39: Camouflage, Concealment, and Decoys* represents a complete reversal of earliest editions of camouflage field manuals, calling deception a component of CCD. However, the publication offers no discussion or guidance on deception.[77]

F. CONCLUSIONS OF DOCTRINE REVIEW

A review of the U.S. Army capstone document for operations from 1905 to present shows the emergence and growth of deception as an operational concept. However, the level of emphasis is cyclic, with peaks occurring during and immediately after World War II, and during the late 1970s through 1980s. Conversely deception integration is at its weakest prior to World War I, and since the end of the Cold War. Furthermore, the only time all the aspects of deception were unified under one concept was during the World War II era when the aspects were bundled under the aegis of counterintelligence. Since that time, deception was slowly and methodically dismembered and marginalized to the point that camouflage is no longer considered a form of deception and the term "cover" has completely lost its connection to deception within U.S. Army doctrine.[78]

---

[77] Headquarters, Department of the Army, *Army Tactics, Techniques, and Procedures 3-34.39: Camouflage, Concealment, and Decoys/Marine Corps Reference Publication 3-17.6A* (Washington, DC: Department of the Army, 2010), iv.

[78] Headquarters, Department of the Army, *Field Manual 1-02: Operational Terms and Graphics* (Washington, DC: Department of the Army, 2004), 1-49; (Army) 1. Protection from the effects of fires. (FM 6-0) 2. A form of security operation whose primary task is to protect the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of and direct fire against the main body. Unlike a screening or guard force, the covering force is a self-contained force capable of operating independently of the main body.

III. EXPLANATIONS FOR VARIATION OF DECEPTION EMPHASIS

As can be seen from the longitudinal survey of deception within U.S. Army doctrine, deception is consistently mentioned; however, the degree of emphasis and level of guidance varies significantly over time. The variance in deception emphasis has driven deception authors to propose numerous explanations as to why the U.S. Army does not treat deception with a greater level of emphasis given deception's demonstrated utility. The reason given the most weight is the idea that America's desired style of warfare, firmly grounded in cumulative destruction and influenced heavily by Clausewitz, leaves little consideration for indirect methods like deception.[79] The second reason, espoused by Herbert Goldhamer, is the rise of a professional officer class separated officers from the political practice of deception.[80] A third reason cited is the over-classification of deception post-WWII has had the unintended consequence of removing deception from consideration by the force. Fourth, various authors have pointed to the perception within Western culture that deception is immoral as reducing the desire to embrace deception's worth. While none of these explanations completely explain the diminished role of deception in U.S. Army doctrine, the American style of war best explains the fluctuations.

A. THE AMERICAN WAY OF WAR

The most frequent explanation of why the U.S. Army has not consistently placed the degree of emphasis on deception commensurate of deception's utility is that the style of war preferred by the United States does not emphasize indirect approaches, including deception. In order to assess this explanation it is necessary to first analyze the styles of war to see if there is a variation of deception emphasis between the styles, then examine

---

[79] Russell Weigley, *The American Way of War: A History of United States Military Strategy and Policy*, Indiana University Press paperback ed. (Bloomington IN: Indiana University Press, 1977), 584.

[80] Herbert Goldhamer, *Reality and Belief in Military Affairs: A First Draft (June 1977)* (Santa Monica, CA: The Rand Corporation, 1979), accessed 25 August 2011, http://www.rand.org/content/dam/rand/pubs/reports/2005/R2448.pdf.

whether the United States has a preference for one style of war, and finally, what reasons might drive any United States preference for a particular style.[81]

1. Styles of War

Essential to understanding the role, or lack of a role, of deception in the U.S. Army is an understanding the two warfighting styles employed by the U.S. Army. On one end of the spectrum is cumulative destruction, which includes what Hans Delbrück and Russell Weigley refer to as the strategy of annihilation, and what Basil Liddell Hart and Edward Luttwak call attrition. On the other end of the spectrum is systemic disruption, which includes Delbrück and Weigley's strategy of attrition; as well as, the indirect approach by Liddell Hart, and relational maneuver by Luttwak.[82] Cumulative destruction seeks to destroy the enemy's capacity for war by decisive defeat of the enemy's military forces, and exemplified by the battles of Cannae, Austerlitz, and the trenches of World War I, especially the German strategy at the Battle of Verdun. Because successful application of the cumulative destruction approach is rooted in the ability of a force to effectively inflict greater net damage on the enemy force, the approach is dependent on an overall force superiority. Even if an inferior force can achieve a series of tactical victories, the additive effect of the losses results in strategic defeat.[83] For example, General Lee's tactical victories over General Grant in the 1864 campaign came with unsustainable manpower losses for the Confederate force, resulting in the final strategic defeat and surrender at Appomattox.

Systemic disruption seeks to achieve victory through attacks against the enemy's weaknesses, (e.g., popular will, production capacity, communications, and command and

---

[81] Author's note: the discussion of styles of war within this thesis is solely in the context of emphasis on deception; any evaluation of the superiority of one style of war over the other is beyond the scope of this work.

[82] The terms cumulative destruction and systemic disruption are used because the various authors have used the term attrition with diametrically opposed meanings. Delbrück and Weigley equate attrition with the strategy of exhaustion; see Delbrück's *The History of the Art of War*. On the other hand, Luttwak, Erfurth, and Boyd use attrition with the meaning *Vernichtungsfeldzug* [annihilation through a series of battles]; see Luttwak's "Notes on Low-Intensity Warfare." In a similar vein, there is a risk of unintentional conflation of relational-maneuver with the maneuver principle of war.

[83] Edward Luttwak and Steven Canby, *MINDSET: National Styles in Warfare and the Operational Level of Planning, Conduct and Analysis* (Pontiac, MA: C&L Associates, 1980).

control) which leave the enemy paralyzed and unable to react effectively. The exemplars for systemic disruption are the German blitzkrieg, most forms of guerrilla warfare, and the AirLand Battle concept. Because the systemic disruption approach places strength against weakness, the potential effect is not dependent on overall force superiority. An inferior force has the potential for strategic victory over a superior force; therefore inferior forces must lean towards a systemic disruption approach in order to have a chance at prevailing.[84] Guerrilla campaigns and insurgencies by necessity spend most of their time tilted heavily toward systemic disruption, as a toe-to-toe fight with government forces from a position of inferiority invites defeat. For example, during the Tet Offensive, the Viet Cong attempted to shift to a cumulative destruction posture resulting in the destruction of the Viet Cong as an effective fighting force.

	Cumulative Destruction	**Systemic Disruption**
Target	Strength against Strength	Strength against Weakness
Endstate	Incapacitation through attrition of resources (e.g., manpower, equipment, supplies); *Materialschlacht* (battle of material)	Incapacitation through strategic paralysis
Focus of Efforts	Tactical level, with objectives in terms of terrain	Operational level, with objectives in terms of shattering the enemy
Outcome	Predictable, based on "overall superiority of net attrition capacity"[85]	Unpredictable, based on ability to perceive and affect enemy weaknesses
Orientation	Interior focus on processes to achieve maximum efficiency of tasks	External focus to identify enemy weaknesses and limitations
Force Design	Systems and formations designed for all-around capabilities – infrequent, revolutionary changes to capabilities	Systems and formations designed for specific enemy forces – frequent, evolutionary changes to capabilities

Table 1. Characteristics of Cumulative Destruction and Systemic Disruption

[84]Luttwak and Canby, *MINDSET: National Styles in Warfare*, 6.

[85] Luttwak and Canby, *MINDSET: National Styles in Warfare*, 3.

[86] Luttwak and Canby, *MINDSET: National Styles in Warfare*, 1 – 29; William Lind, "The Case for Maneuver Doctrine," in *The Defense Reform Debate*, eds. Asa Clark, Peter Chiarelli, Jeffrey McKitrick, and James Reed (Baltimore: The John Hopkins University Press, 1984), 88 – 100.

Cumulative destruction and systemic disruption as described above actually represent a false dichotomy for the sake of analysis. In practical application, pure expressions of either approach do not exist. Rather, all warfighting can be envisioned as existing on a spectrum between cumulative destruction and systemic disruption, exhibiting aspects of each style.[87] The degree to which a commander's style tips towards cumulative destruction or systemic disruption influences the degree to which deception is practiced. Luttwak suggests that forces leaning towards the cumulative destruction style tend to be more focused on internal processes and organization than on the enemy since victory is achieved by the most effective and efficient application of superior firepower. Because of this inward perspective, there is less effort given to understanding the enemy to the degree needed for effective deception. Conversely, systemic disruption oriented forces are more focused on the external since victory is achieved through the identification and exploitation of enemy weaknesses.[88] Deception is considered to be one of the three interrelated principles of systemic disruption, along with avoidance of the enemy's main strength and dominance of momentum.[89] As a result of the centrality of deception to systemic disruption, the deception plan is elevated "…to full equality with the battle plan; certainly deception planning cannot remain a mere afterthought."[90] Thus, as a force leans towards cumulative destruction, the emphasis of deception decreases, and conversely, as the force leans towards systemic disruption, the emphasis of deception increases.

Clausewitz's *On War* and Jomini's *The Art of War* are considered the pillars of the cumulative destruction mode of warfighting. Sun Tzu's *The Art of War* and Basil Liddell Hart's *Strategy* are representative of the systemic disruption model. Colonel John Boyd's "Patterns of Conflict" provides a thorough comparison between the two styles, though Boyd's preference for systemic disruption colors the discussion. Additionally,

---

[87] Luttwak and Canby, *MINDSET: National Styles in Warfare*, 10; Huba Wass de Czege, "Army Doctrinal Refore," in *The Defense Reform Debate*, eds. Asa Clark, Peter Chiarelli, Jeffrey McKitrick, and James Reed (Baltimore: The John Hopkins University Press, 1984), 103.

[88] Edward Luttwak, "Notes on Low-Intensity Warfare," *Parameters* 8, no. 4 (1983), accessed 14 July 2011, http://www.carlisle.army.mil/usawc/Parameters/Articles/1983/1983%20luttwak.pdf, 13.

[89] Luttwak and Canby, *MINDSET: National Styles in Warfare*, 20 – 21.

[90] Luttwak and Canby, *MINDSET: National Styles in Warfare*, 17.

Michael Handel's *Masters of War* offers side-by-side comparison and analysis of Clausewitz, Jomini, and Sun Tzu; as well as, Machiavelli and Mao Tse-tung.

2. American Preference for Cumulative Destruction

As Lysander suggested, when the skin of the lion—force—will not suffice, then the skin of the fox—guile—must be used to cover the gap. The inherent implication to this advice is when the skin of the lion is sufficient, the fox is not needed. Several authors mention the evolution of Napoleon's warfighting as the exemplar for this relationship. As Napoleon's armies grew in power and capability, Napoleon transitioned from a reliance on cunning and misdirection to a reliance on force.[91] Weigley, in his classic, *The American Way of War*, states as his premise that America fought a war of systemic disruption during the Revolutionary War because the nascent nation was too weak to fight a war of cumulative destruction; however, after the Revolution as the nation grew and strengthened, the strategy of cumulative destruction became the preferred America strategy.[92] Even during the Revolutionary War there was resistance to the systemic disruption approach employed by General Washington, as exemplified by John Adams in a letter to Abigal Adams: "I am sick of Fabian systems in all quarters. The officers drink, A [*sic*] long and moderate war. My toast is, A [*sic*] short and violent war."[93] John Adams' desires are frequently reflected in U.S. Army doctrine. For example, *FM 100-5* (1939) states:

> The *ultimate objective* [emphasis in original] of all military operations is the destruction of the enemy's armed forces in battle…. Concentration of *superior forces* [emphasis in original], both on the ground and in the air, at the decisive place and time, creates the conditions most essential to decisive victory and constitutes the best evidence of superior leadership.[94]

---

[91] J. Bowyer Bell, "Toward a Theory of Deception," *International Journal of Intelligence and Counterintelligence,"* 16, no. 2 (2003), 251;

[92] Weigley, *The American Way of War*, xxii.

[93] John Adams, Abigail Adams and Charles Adams, *Familiar Letters of John Adams, and His Wife Abigail Adams during the Revolution. with a Memoir of Mrs. Adams* (New York: Hurd and Houghton, 1876), 305.

[94] War Department, *Tentative Field Service Regulations of Operations, 1939*, 27.

Additionally, *FM 100-5* (1993) states the American people's desire for short, decisive war:

> The American people expect decisive victory and abhor unnecessary casualties. They prefer quick resolution of conflicts and reserve the right to reconsider their support should any of these conditions not be met.[95]

These attitudes are the essence of cumulative destruction, and help demonstrate the U.S. Army's preference for that style of war.

Since the United States tends towards the cumulative destruction side of the spectrum, U.S. Army doctrine tends to embrace Clausewitz's positions on the execution of war. As a result, Clausewitz's disdain may have an impact on deception's place in doctrine. Clausewitz writing about craft and cunning stated: "The fact remains that those qualities do not figure prominently in the history of war. Rarely do they stand out amid the welter of events and circumstances."[96] As for the act of deception, Clausewitz argues:

> To prepare a sham action with sufficient thoroughness to impress an enemy requires a considerable expenditure of time and effort, and the costs increase with scale of the deception. Normally, they call for more than can be spared, and consequently so-called strategic feints rarely have the desired effect.[97]

Goldhamer suggests this blatant disregard for the historic record as the "bias of a professional soldier for whom the conflict of force with force and the destruction of the enemy on the battlefield were the principle instruments in the art of war."[98] Handel suggests that Clausewitz and Jomini's diminishing of deception and trickery in war was a result of the period in which they fought.[99] Handel further points out that Clausewitz's method of war relied on a concentration of forces at the decisive point, and that deceptive feints and demonstrations reduced a commander's ability to mass his forces.[100]

---

[95] Headquarters, Department of the Army, *Field Manual 100-5, 1993*, 1-3.

[96] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret, 3rd ed. (New York: Alfred A. Knopf, Inc., 1993), 238.

[97] Clausewitz, *On War*, 239

[98] Goldhamer, *Reality and Belief in Military Affairs*, 100.

[99] Michael I. Handel, *Masters of War : Classical Strategic Thought*, 3rd rev. and expanded ed. (London; Portland, OR: Frank Cass, 2001), 216.

Regardless of the reasoning at the time behind Clausewitz's diminishment of the utility of deception, his work continues to influence the development of U.S. military doctrine.

3. Balance of Power

If one accepts that the U.S. Army tends to favor a cumulative destruction style, why has U.S. Army doctrine on occasion increased its emphasis on deception? The answer may lay in the comments of Weigley and others: perceived and actual balances of power influence the proportions of cumulative destruction and systemic disruption within a force's particular warfighting style. If there is a significant imbalance between opponents, the stronger force can rely on its strength to overcome the opposition. J. Bowyer Bell states:

> Power and capacity, as in real life, can make deception unnecessary. Napoleon, as the power of his armies increased, relied more on force and less on cunning and misdirection. In an invasion of a small country, the larger aggressor need only dispatch overwhelming power: how could Grenada repulse the forces of the United States…. American military strategy has often been based on deploying maximum power and technological capability without recourse to duplicity—"more" is more and force needs no enhancing…"[101]

Because a superior force does not need to rely as heavily on aspects of systemic disruption like deception, while conversely an inferior force must shift weight towards a systemic disruption approach, there is a trend whereby the level of emphasize on deception within U.S. Army doctrine waxes and wanes as the perceived and actual balance of power shifts (Figure 2).

---

[100] Handel, *Masters of War*, 225.

[101] Bell, "Toward a Theory of Deception," 251; A similar opinion is stated in *Secret Soldiers*: "An army possessing overwhelming numbers of troops or material would not have to resort to wiles." Philip Gerard, *Secret Soldiers* (New York: Penguin Group, 2002), 5.

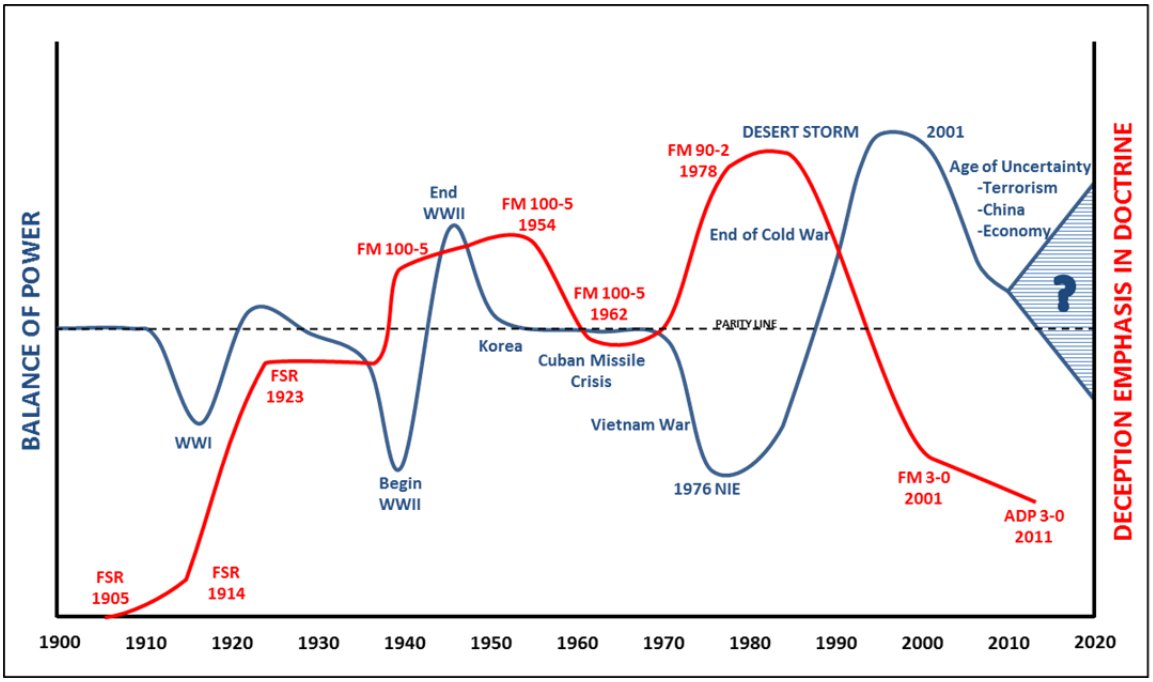


Figure 2. Comparison of Balance of Power and Doctrinal Emphasis of Deception

During World War I, the German military was seen initially as a superior competitor, thus during World War I deception—especially the covering aspects of camouflage and operations security—increased in importance. This increase is reflected by the inclusion of sections on counterinformation and surprise in the 1923 *Field Service Regulations*. Similarly, during World War II the Axis was seen as an existential threat, and deception reached a crescendo. Post-World War II, the United States operated from a position of parity during the Cold War, and over time deception receded from the operations manuals.[102]

The 1970s represented a tectonic shift in the perceived balance of power. First, the failures of Vietnam, the Mayaguez incident, and the failed attempt to rescue the hostages in Iran caused a crisis of faith within the U.S. Army leading to the development

[102] The emergence of the Special Forces and the rest of the special operations community can be viewed as the U.S. attempt to keep the conventional forces focused on cumulative destruction while still leveraging the value of systemic disruption.

of the Airland Battle doctrine.[103] Second, the 1976 National Intelligence Estimate on Soviet military capability included a second assessment which painted the Soviet military as superior to the United States military in both nuclear and conventional forces:

> *Within the ten year period of the National Estimate the Soviets may well expect to achieve a degree of military superiority which would permit a dramatically more aggressive pursuit of their hegemonial [sic] objectives*, [italics in original] including direct military challenges to Western vital interests, in the belief that such superior military force can pressure the West to acquiesce or, if not; can be used to win a military contest at any level.[104]

Additionally, the National Intelligence Estimate addendum reassessed Soviet intentions, painting a picture that the Soviet Union was a far greater and imminent threat than previously recognized. This radical re-estimation of Soviet capabilities and intentions shifted the perceived balance of power, placing the U.S. in an inferior position. As a result, U.S. Army doctrine at the time increased emphasis on systemic disruption and deception. The 1976 edition of *FM 100-5* fixates almost totally on operations in Western Europe against a superior force. This manual also marks the reemergence of deception emphasis to a degree not seen for decades. Furthermore, the era marks a renaissance of deception throughout the U.S. Army culminating with the central use of deception during Operation DESERT STORM. The 1982 and 1986 editions of *FM 100-5* see the U.S. Army doctrine at the apex of systemic disruption.

With the collapse of the Soviet Union in 1991, the United States was left without a peer competitor. As a result, the balance of power shifted decisively in the favor of the United States, alleviating the perceived need to emphasize systemic disruption. In the absence of an overpowering threat, U.S. military doctrine returned to the comforts of the cumulative destruction style of war, and deception emphasis ebbed to the point that the current capstone operations manual, *APD 3-0*, does not mention deception at all.

---

[103] William Lind, "Defense Reform: A Reappraisal," in *The Defense Reform Debate*, eds. Asa Clark, Peter Chiarelli, Jeffrey McKitrick, and James Reed (Baltimore: The John Hopkins University Press, 1984), 328.

[104] Team "B", *Soviet Strategic Objectives: An Alternative View* (Washington, DC: Director of Central Intelligence, 1976), accessed 16 April 2012, http://www.foia.cia.gov/docs/DOC_0000278531/DOC_0000278531.pdf, 47.

B. PROFESSIONAL OFFICER CLASS

Goldhamer suggests an interesting alternate hypothesis: the rise of the professional officer class led to the marginalization of deception in war. The professional officer class became specialists in the art of the direct approach as described by Clausewitz, and developed a professional pride in using physical force to overcome an adversary. The sense of worth as a professional officer was based in the ability to defeat the enemy in a stand up fight.[105] Gerald in *Secret Soldiers* provides anecdotal evidence supporting Goldhamer's assertion stating:

> Not all soldiers are fond of practicing deception. Some American combat commanders in World War II instinctively resisted using deception, preferring to charge straight ahead like the old-style cavalrymen they were…. Others… simply preferred conventional battle as a route to honor and glory.[106]

Additionally, the political agnosticism of the professional officer class also impacted deception, as it separated military action from foreign political involvements—foreign political involvements are seen by Goldhamer as more conducive to manipulation and deception.[107] The divorce of the senior officer class from diplomacy meant a degradation of peacetime concerns about national strategy; as well as:

> …those manipulative and deceptive measures that might strengthen in peacetime the nation's position vis-a-vis a potential enemy by misleading him and weakening his present and future powers of resistance. Such measures require close coordination of military and political leadership, a cooperation less likely to occur given the professional soldier's distance from the foreign office and for the most part, the political leader's and parliamentarian's divorce from strategic and grand strategic concerns."[108]

Goldhamer's argument is undermined somewhat by the championing of cover and deception by General Eisenhower during and after World War II; however, the idea of the U.S. Army as a profession of arms is a recurrent theme that may serve to reinforce direct approaches.

---

[105] Goldhamer, *Reality and Belief in Military Affairs*, 103.

[106] Gerald, *Secret Soldiers*, 7

[107] Goldhamer, *Reality and Belief in Military Affairs*, 103.

[108] Goldhamer, *Reality and Belief in Military Affairs*, 104.

C. OVER-CLASSIFICATION

A third potential explanation for the dearth of deception in U.S. Army doctrine is the over-classification of deception. While security is essential for the execution of deception operations, classification of the very concept can be immensely detrimental to the inculcation of the utility of deception to the force. If future leaders are not exposed to deception during their formative years as junior officers, how can they be expected to appreciate deception's utility later? The negative impact of classification can be seen in a 1948 memorandum from the Office of the Chief of Army Field Forces to the commanders of the Armored, Artillery, and Infantry Centers on the subject of training cover and deception. The cursory introduction to strategic cover and deception was restricted to confidential level with no questions authorized and contained the comment: "The security classification of this whole subject [strategic cover and deception] is and probably will remain TOP SECRET [emphasis in original]…" leaving one to wonder the utility of the training.[109] Tactical cover and deception was subjected to similar classification. Classification of the first two editions of *FM 31-40: Tactical Cover and Deception* effectively removed deception from the playing field. The 1954 edition of *FM 100-5* contained several pages on the planning and execution of tactical cover and deception; however, this was cut to a couple of paragraphs in the 1962 edition.

In addition to the classification of doctrine, the classification of the actual deception operations negatively impacted the institutional memory of the force. The mission of 23rd Headquarters Special Troops, a purpose built deception unit in World War II, was not declassified until 1996.[110] With the information on operations compartmentalized behind walls of classification, the memory of deception resting in the minds of the practitioners could not be effectively passed on to future generations of leaders. Thus as the personnel with firsthand knowledge of deception operations retired from the force, the institutional knowledge retired with them.[111] The double impact of the

---

[109] Office of the Chief of Army Field Forces, *Strategic and Tactical Cover and Deception Training*, 9.

[110] National Army Security Agency Association, "The 23rd Headquarters Special Troops (World War II)" accessed 1 January 2012, http://www.nasaa-home.org/23rdhqs.htm.

[111] Bell, "Toward a Theory of Deception," 251.

Page 747 of 3957

classification of both deception doctrine and historic examples of deception placed an extremely high barrier against access of deception resources by junior leaders, inhibiting the development of new institutional memories on the use of deception. The lack of exposure at the junior levels translating into a feeling at higher levels of command that deception is unnecessary—after all, it was not needed at the lower levels.

D. MORALITY

A fourth potential explanation touched on by Jon Latimer, John Bell, and Barton Whaley is that deception is immoral. Honesty has long been considered a virtue within American life as expressed by maxims such as "Honesty is the best policy," and the apocryphal tale of George Washington and the cherry tree. The idea of the American military as moral paragons is also frequently present in official and unofficial military guidance and writings. For example, General Dempsey [in his paper "America's Military- a Profession of Arms"] recently stated:

> The Profession of Arms demands its members live by the values described in the "City on the Hill" metaphor. We must provide an example to the world that cannot be diminished by hardships and challenges. This example is based upon the words and intent of the US Constitution that each of us takes a personal oath to support and defend. Our oath demands each of us display moral courage and always do what is right, regardless of the cost. We are all volunteers in our willingness to serve and to place others' needs above our own. As shared values, our calling cards are Duty, Honor, Courage, Integrity, and Selfless Service. Commitment to the rule of law is integral to our values which provide the moral and ethical fabric of our profession.[112]

Deception in particular has been viewed as dishonorable, an idea exemplified by the some of the responses over Colonel Funston's use of deception to achieve victory over the insurgents during the Philippine Insurrection; rather than lauded, Funston was vilified for winning by deceit.[113] On the floor of the Senate, Senator Patterson of

---

[112] Martin Dempsey, "America's Military—a Profession of Arm" (Washington, DC: Joint Chiefs of Staff, 2012), accessed 24 February 2012, http://www.jcs.mil/content/files/2012-02/022312120752_Americas_Military_POA.pdf, 3.

[113] J. Bowyer Bell and Barton Whaley, *Cheating and Deception* (New Brunswick, NJ Transaction Publishers, 1991), 45.

Colorado accused Funston of violating the rules of civilized warfare.[114] Colonel Funston was also the subject of a sermon decrying the use of underhand methods which lower the standard of honor.[115] However, while it may be that deception is viewed as immoral, little in U.S. Army doctrine conveys this view. The 1905 edition of *Field Service Regulations* stands almost alone in its level of condemnation of illegal acts of deception.[116] Furthermore, a survey of the use of deception by the U.S. Army across the span of its history shows that even if deception is viewed by the organization as immoral the view is not a serious impediment to the execution of deception. Rather, the attitude of Ulisse Guadagnini seems to hold more sway: "Moral considerations have validity only in civilian life and should not interfere with preparations for war."[117]

E. CONCLUSION

The primary explanation for the undervaluing of deception in U.S. Army doctrine is the emphasis on the cumulative destruction style of war; however, the other explanations play their part in further reducing the level of emphasis. Taken together, the composite effect of the explanations leads to the creation of an organizational bias against deception. Daniel and Herbig state that organizational bias presents itself in two ways. First, there is a "bureaucratic imperative that organizations trained for particular tasks will seek to perform them." Second, due to availability bias, people will think and act in ways familiar to them.[118] Allison and Zelikow in *Essence of Decision* present a model for organizational behavior that suggests the behavior is linked more to standard operating procedures and established doctrine than to deliberate choices. Formalized doctrine

---

[114] "Gen. Funston's Action," *The Washington Post (1877 – 1922)* March 28, 1902, ProQuest (144350948).

[115] "Funston Subject of Sermon," *New York Times (1857 – 1922)* April 15, 1901, ProQuest (96118056).

[116] While acts of perfidy are frequently cited in doctrine as illegal, the 1905 Field Service Regulations described illegal acts of deception using terms like treacherous, fiendishness, and infamy. War Department, *Field Service Regulations, 1905*, 214.

[117] Quoted in Waldemar Erfurth, *Surprise*, trans. Stefan T. Possony and Daniel Vilfroy (Harrisburg, PA: Military Service Publishing Company, 1943), 51.

[118] Donald C. Daniel and Katherine L. Herbig, "Propositions on Military Deception," in *Strategic Military Deception*, eds. Donald C. Daniel and Katherine L. Herbig (New York: Pergamon Press, 1982), 14.

serves to constrain behavior.[119] Thus the degree of emphasis on deception in doctrine translates to the degree of deception operations in practice.

Another area where the organizational bias has impacted deception is the lack of a stable proponency. Since 1923, deception has shifted proponency numerous times, and has never been in the position of being the primary focus of whatever command held purview. Additionally, some aspects of deception have been separated under difference proponents, such as camouflage under the U.S. Army Engineer School. The lack of a stable proponency with deception as its central focus further undermines the integration of deception into U.S. Army doctrine three important ways. First, the frequent changes of deception proponency impede continuity of knowledge. Second, since deception is never the primary focus for a proponent, deception is always at risk of marginalization in favor of the primary focus. Third, some efforts implemented are abandoned when the proponency changes. For example, while deception was under the U.S. Army Intelligence Center and School, the tables of organization for corps and divisions were modified to add deception cells. After deception proponency shifted to the U.S. Army Combined Arms Center, the deception cells were dropped in order to support the emerging requirement for unmanned aerial vehicles.[120]

[119] Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. (New York: Addison Wesley Longman, Inc, 1999), 143 – 145.

[120] Nelson, "Battlefield Deception," 29 – 30.

IV. THEORY OF DECEPTION

> *Every means is permitted which deceives the enemy and induces him to take wrong steps. The lion's bravery and the fox's cleverness must combine to wrest victory from the enemy.*
>
> *– General Waldemar Erfurth*[121]

A. WHAT IS DECEPTION

Despite deception's long and storied place in the history of war, J. Bowyer Bell and Barton Whaley assert in, *Cheating and Deception*, that their theory was the first attempt to create a "general theory of cheating."[122] Bell and Whaley's theory of deception is elegant in its simplicity. The theory categorizes all deceptions into two interdependent sets: showing the false and hiding the real. These categories are further subdivided into six categories. Hiding the real is divided into the categories of masking, repackaging, and dazzling, while showing the fake is divided into the categories of mimicking, inventing, and decoying. Each category has myriad characteristics that can be drawn from for the deception plan. The categories of deception and the chosen characteristics are used in ruses to create one of five effects: unnoticed, benign, desirable, unappealing, and dangerous. The purpose of the ruse is to create a perception in the target that causes the target to generate an illusion the target interprets as reality, causing the target to act in the desired manner to achieve the deception goal and thus the strategic goal.[123] While Bell and Whaley's theory provides a neat and tidy structure for the taxonomy of deception, one weakness of the theory is that it does not delve in the cognitive psychology allowing deception to occur.

Michael Dewar offers a different theory of deception in *The Art of Deception in Warfare*. Dewar's theory is a less structured discussion than Bell and Whaley's theory; nevertheless, the theory provides important insights into the inner workings of deception. Dewar provides an overview of deception means, principles, and techniques. Of

---

[121] Erfurth, *Surprise*, 198.

[122] Bell and Whaley, *Cheating and Deception*, 45.

[123] Bell and Whaley, *Cheating and Deception*, 45 – 74.

Page 751 of 3957

particular note are his comments on the prevalence of preconceived ideas on the battlefield, and the role of doctrinal and technical innovation in achieving surprise.[124]

1. Deception Defined

According to *Random House Webster's*, deception is "something that deceives or is intended to deceive; fraud; artifice."[125] While this is a sufficient definition for casual uses, this definition is not sufficient for deception in the context of military operations. Daniel and Herbig in their work "Propositions on Military Deception" define deception as: "the deliberate misrepresentation of reality done to gain a competitive advantage."[126] One problem with Daniel and Herbig's conceptualization of deception is their fixation on deception as being based in falsehood or lies. This concept of deception ignores the ideas of deception by omission and deception by selective truth. Furthermore, the definition makes no mention of the target of the deception. In the definition's defense, the concept of gaining a competitive advantage is important. Deception in military operations is not undertaken for deception's sake; deception is undertaken to achieve some goal.

The definition of deception used in U.S. Army doctrine since at least 1969 is a better starting point for a working definition of deception: "Activity designed to mislead an enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interest." [127] While the current U.S. Army definition is a good starting point, this definition too is not quite sufficient. The first deficiency with the current doctrinal definition is that "induce" is an imprecise term for what deception does: manipulating the enemy's decision-making process. Second, the best deceptions rely on a foundation of truth to reinforce and support the falsehoods, an idea the definition seems

---

[124] Michael Dewar, *The Art of Military Deception in Warfare*, 1st ed. (Newton Abbot, UK: David & Charles, 1989), 9 – 20.

[125] *Random House Webster's Unabridged Dictionary*, 2nd ed., revised and updated ed. (New York: Random House Reference, 2001), 516.

[126] Daniel and Herbig, *Propositions on Military Deception*, 3.

[127] Headquarters, Department of the Army, *Training Circular no. 30-1: Tactical Cover and Deception*, 5; An almost identical definition is given in the 1957 *Special National Security Estimate: Soviet Capabilities for Deception* by the Central Intelligence Agency: Director of Central Intelligence, *Soviet Capabilities for Deception* (Washington, DC: Central Intelligence Agency, 1957), accessed 30 January 2012. http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&res_dat=xri:dnsa&rft_dat=xri:dnsa:article:CSE00201

to ignore with the modifiers used to describe the evidence. Finally, the term enemy is unnecessarily constraining, as deception can be applied against any target. A strength of the doctrinal definition is its acknowledgement of the role of intent in human deception. While biological deceptions exhibited in the plant and animal kingdoms can be unintentional, human deception requires intent.[128]

Taking in account the shortcomings of the existing definitions of deception, a modified definition of deception can be crafted:

> Deception is the deliberate misleading of a target into taking actions prejudicial to the target's interests by manipulating the target's decision-making processes through the communication of true, manipulated, distorted, and/or falsified information.

This revised definition of deception requires some elaboration. Deliberate misleading does not obligate the practitioner to a formal planning process; while formal planning is preferable, rapid ad-hoc planning by a nimble practitioner can in extremis achieve the objective in time constrained or fluid situations, though with increased risk of failure. Successful deception is more than creating a perception; successful deception is about the target taking action. Furthermore, the goal of a deception can be the target taking no action at all, e.g., the failure of a regime's security apparatus to breach a special reconnaissance element's cover or the German armored divisions remaining in place at Pas de Calais during the opening phases of Operation OVERLORD. The interaction between the practitioner and the target occurs in the framework of communication. Finally, the perceptions used by the target in its decision-making process rely heavily on the indicators created by the practitioner.

2. Deception: Truth and Lies

Many definitions of deception conflate deception with lies; however, this conflation is incorrect as deceptions and lies are not synonymous. In order to discuss the difference between a lie and deception it is first necessary to establish an adequate

[128] For a discussion on biological deceptions see: Scott Gerwehr and Russell W. Glenn, *Unweaving the Web: Deception and Adaptation in Future Urban Operations* (Santa Monica, CA: Rand, 2002), 78. For a discussion on the requirement for intent in human deception see: Roderick M. Chisholm and Thomas D. Feehan, "The Intent to Deceive," *The Journal of Philosophy* 74, no. 3 (March, 1977), 143 – 159.

definition of each. One definition defines a lie as occurring when a person asserts to a second person a proposition that the first person knows to either be false or not true with the intent of causing the second person to have a justified belief in the proposition.[129] Since a deception can contain truth—an actual training exercise used as part of a deception is still a true event—it is immediately apparent that deception and lies are not equal; however, this still leaves the proposition that lies are a subset of deception.[130] For example, Daniel and Herbig's model of deception has lies and the act of lying subsumed by deception (Figure 3). The definition of deception used here requires injury to the target or advantage for the practitioner; this leaves lies undertaken without the intent of injury or advantage [white lies] to exist outside the sphere of deception. Thus, while the sets of lies and deception overlap, neither subsumes the other (Figure 4). While lies are used in deception, not all deceptions are lies. Judicious use of the truth can be far more supportive of deception than outright falsehood.

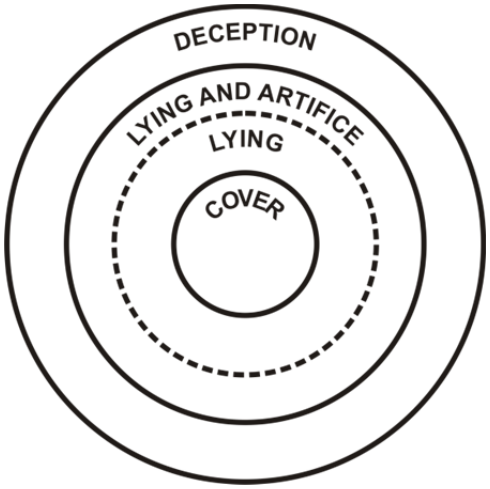


Figure 3. Daniel and Herbig's "Deception's Subsidiary Concepts." (From: [131])

[129] Chisholm and Feehan, *The Intent to Deceive*, 152; This work presents an in-depth parsing of what it means to lie and what it means to intend to deceive.

[130] Chisholm and Feehan provide another illuminating example attributed to Immanuel Kant: "For there are types of intended deception that cannot properly be said to be cases of lying. Kant's example will do: 'I may, for instance, wish people to think that I am off on a journey, and so I pack my luggage; people draw the conclusion I want them to draw . . .' But although I thus succeed in deceiving them, Kant insists, 'I have not lied to them, for I have not stated that I am expressing my opinion.'" Chisholm and Feehan, *The Intent to Deceive*, 149.

[131] Daniel and Herbig, *Propositions on Military Deception*, 4.

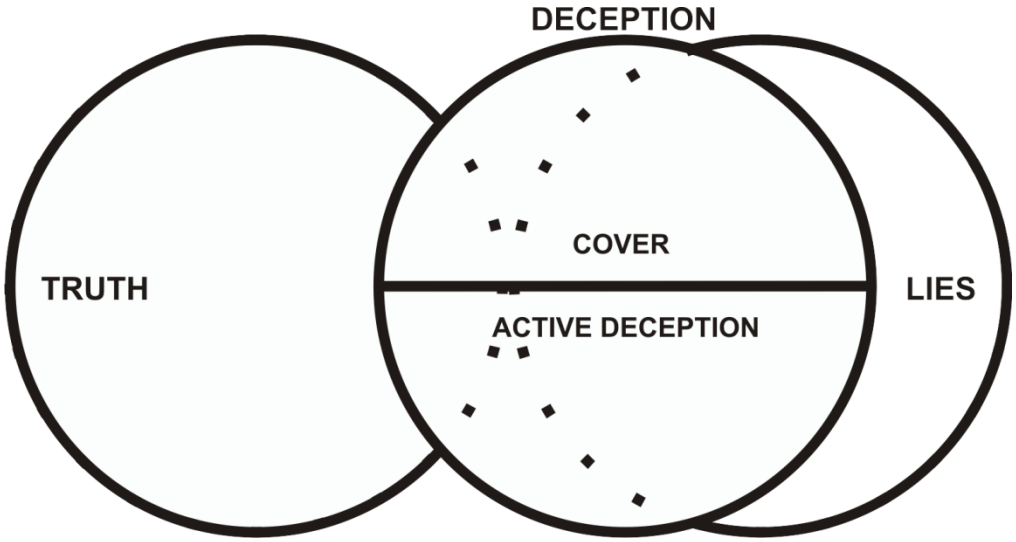


Figure 4. Interrelationship of Truth, Deception, and Lies

B. TAXONOMY OF DECEPTION

1. Taxonomy of Method

Taxonomies are systems of categorizing items in a set into subordinate sets based on a defined system of characteristics. The most recognizable example for taxonomies is the system of classifying living things into kingdoms, phyla, classes, orders, families, genera, and species. Within the field of deception, there are several suggested taxonomies for deception, four of which are: method, sophistication, effect, and commission-omission. Taxonomy by method focuses the mode of the deception, such as a display. Taxonomy by sophistication categorizes deceptions by the degree to which the deception adapts or does not adapt to changing circumstances. Taxonomy by effect focuses on what the deception does, e.g., dazzling. Finally, taxonomy by commission-omission breaks down deceptions based on whether the deception causes the target to acquire a false belief or contributes to the target continuing a false belief. For this purposes of this work, taxonomy by method is used as it closely matches existing U.S. Army doctrinal concepts of deception (Figure 5). Brief descriptions of the alternate taxonomies are provided at the end of this section.

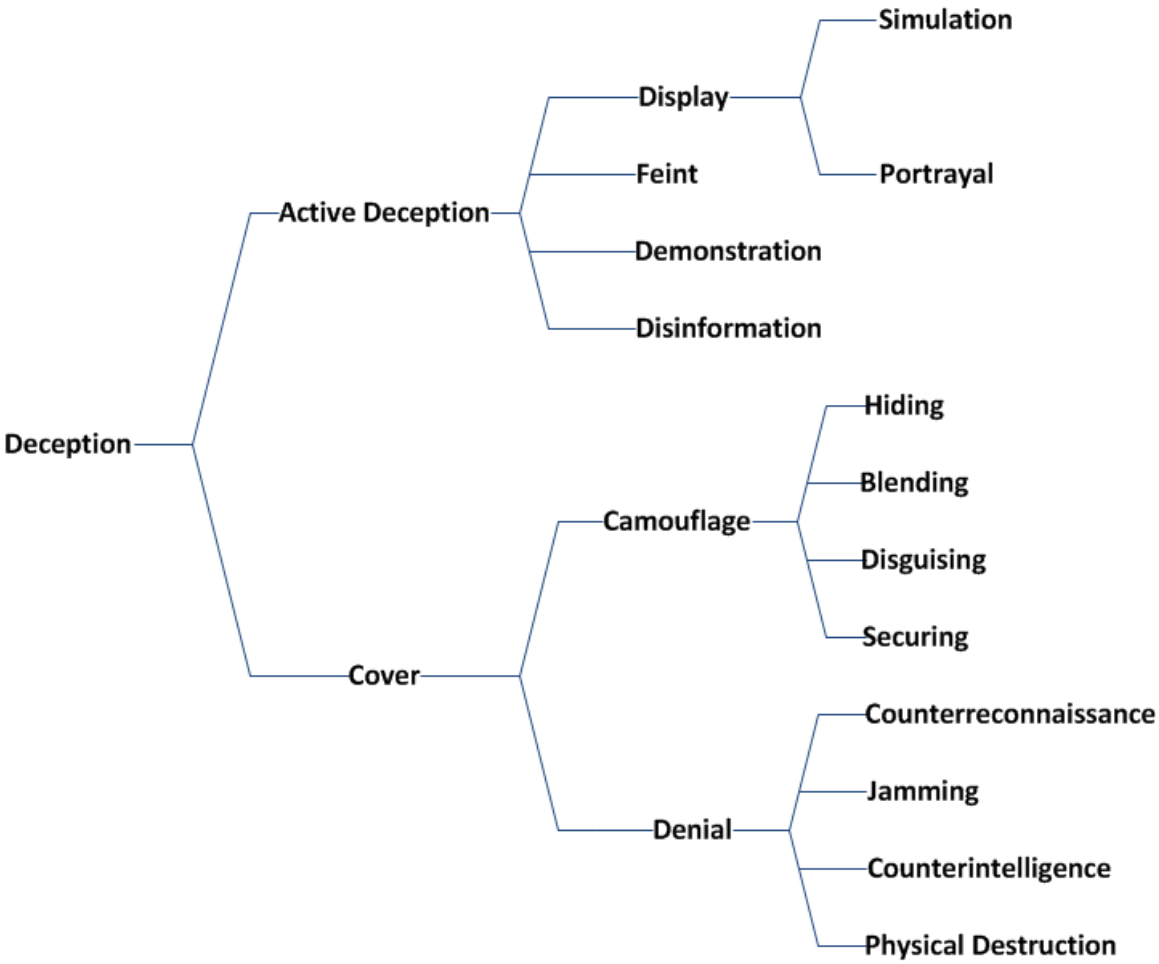


Figure 5. Taxonomy of Deception

2. Deception

Deception is the set of actions designed to deliberate mislead a target into actions or inactions prejudicial to the target's interests by manipulating the target's decision-making processes through the communication of true, manipulated, distorted, or falsified information. Deception is subdivided into two broad categories: active deception and cover. Active deception consists of those actions designed to convey deceptive indicators to the target. Cover, as used here, is the set of actions designed to prevent the target access to the indicators necessary for constructing a correct perception of the situation

and environment, and thus necessary for proper decision-making.[132] Though some of the actions included in the category of cover are not usually considered to be part of deception in U.S. Army doctrine, the obfuscation of indicators is an intrinsic part of deceiving a target.[133]

3. Active Deception

Active deception is comprised of actions which convey deceptive information to the target, also referred to as simulation or showing the false. The set of active deception includes those modified versions of the actions traditionally associated with military deception. Active deception is divided into four broad categories: displays, feints, demonstrations, and disinformation.

a. Displays

Displays are static depictions of activities, forces, or equipment for the purpose of deceiving the target's collection apparatus.[134] Though the formal Army definition of a display limits the type of target collection to visual, displays can also occur in all physical senses; as well, as in the electromagnetic spectrum. Displays are divided into two categories: simulation and portrayal. Simulations use decoys and other devices

---

[132] This usage of cover is consistent with historic Army and DOD usage, and in numerous civilian works. See: Headquarters, Department of the Army, *Field Manual 1-02*, 1-48 to 1-49; Concepts and Force Design Group, *Tactical Cover and Deception: Final Report*, 1-4; Daniel and Herbig, *Propositions on Military Deception*, 4; Robert Goldsmith and Ralph Gerenz, *Techniques for Detecting Cover and Deception*, (Billerica, MA: Betac Corporation, 1983), accessed 16 May 2012, http://handle.dtic.mil/100.2/ADP002896, 145.

Cynthia Grabo provides an alternative definition for cover which is more constrained: "Cover (here meaning the "cover plan'' or "cover story'') is a form of military deception which should be distinguished from active military deception, although it may often be used in conjunction with it. Cover will be used when it may be presumed that the military buildup itself cannot be concealed from the adversary, and its purpose therefore is to offer some seemingly plausible explanation (other than planned aggression) for the observable military activity." Cynthia Grabo, *Anticipating Surprise: Analysis for Strategic Warning*, ed. Jan Goldman (Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, 2002), accessed 14 May 2012, www.ni-u.edu/ni_press/pdf/Anticipating_Surprise_Analysis.pdf, 125.

[133] Bell and Whaley, *Cheating and Deception*, 49; Roy Godson and James J. Wirtz, "Strategic Denial and Deception," in *Strategic Denial and Deception: The Twenty-First Century Challenge*, eds. Roy Godson and James J. Wirtz (Piscataway, NJ: Transaction Publishers, 2002), 1 – 2.

[134] Adapted from official Army definition: "In military deception, a static portrayal of an activity, force, or equipment intended to deceive the adversary's visual observation." Headquarters, Department of the Army, *Field Manual 1-02*, 1-83.

Page 757 of 3957

to create a dummy force or capability. Decoys are models or dummies used to replicate actual equipment, buildings, and personnel.[135] Magruder's Quaker guns were decoys used to create the perception that the Confederate lines were more heavily fortified than they were in reality. MACVSOG's ruse of an active resistance movement in North Vietnam contained major elements of simulation and portrayal.[136]

Portrayals use actual forces to present either the image of a unit which either does not exist, or that the unit is of a different type than it actually is.[137] An infantry company presenting itself as an infantry battalion or brigade is a form of portrayal. Pseudo-operations and "false flag" operations are specialized forms of portrayals where the unit being portrayed is either a third party or an element of the target's forces. Colonel Funston's ruse during the Philippines Insurrection involved his force portraying the insurgent force in order to gain access to the insurgent camp.[138] British forces in Kenya used pseudo-operations to masquerade as Mau-Mau elements for the purposes of intelligence collection.[139] Soviet forces engaged in "false flag" operations during the suppression of resistance movements in Lithuania by posing as the Lithuanian resistance while attacking the population in an effort to separate the resistance from the population.[140] Portrayals also encompass the cyberwar concepts of the honeypot and social engineering.[141]

---

[135] Headquarters, Department of the Army, *Training Circular No. 30-1*, 5.

[136] See Chapter V for more information on MACVSOG deception operations.

[137] Headquarters, Department of the Army, *Training Circular No. 30-1*, 10.

[138] See Chapter V for additional details on Colonel Funston's operation.

[139] Kitson, Frank, *Gangs and Counter-gangs*, (London: Barry and Rockliff, 1960).

[140] John Prados, *Presidents' Secret Wars*, revised and updated ed. (Chicago: Elephant Paperbacks, 1996), 38.

[141] A honeypot is an enticing computer or server designed to draw attacks by adversarial forces. Honeypots may also be classified as a form of feint here since they must survive contact with the target without revealing their true nature. The purpose of the honeypot is typically to gain intelligence about the adversarial forces' capabilities, identities, and location.

b. Feints

Feints are operations designed to deceive the target into reacting as if the feint is an actual decisive operation.[142] Feints differ from demonstrations in that some manner of contact with the target is sought. The degree of contact varies significantly. Feints are used for several purposes; for example, to distract the target from the actual decisive action, facilitating relative superiority at the point of decision; luring the target into exposing artillery positions; or to trick the target into prematurely committing the reserve. *Field Service Regulations* (1914) describes a stronger variant of the feint: holding attack. In addition to distracting the enemy from the main effort, the holding attack seeks to fix the enemy in time and space.[143] Also, the covering force concept in *FM 100-5* (1976) has an element of feint, though its primary mission is not deception.[144] In addition to traditional offensive and defensive operations, feints also encompass lures designed to draw the target into an unequal fight, e.g., the bait and ambush tactics of guerrilla and insurgent forces.

c. Demonstrations

Demonstrations are deceptive shows of force where actual engagement with the target is not sought.[145] Because contact is not sought with the target, the forces used for a demonstration can be considerably smaller than those used for a feint. While the traditional U.S. Army doctrinal definition of demonstrations implies demonstrations occur in the vicinity of the enemy lines, almost as a less aggressive form of a feint, this is

---

[142] Adapted from the DOD and Army definitions of feint: "In military deception, an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action. (Army) A form of attack used to deceive the enemy as to the location or time of the actual decisive operation. Forces conducting a feint seek direct fire contact with the enemy but avoid decisive engagement." Headquarters, Department of the Army, *Field Manual 1-02: Operational Terms and Graphics*, 1-76.

[143] War Department, *Field Service Regulations*, 1914, 84 – 85.

[144] Headquarters, Department of the Army, *Field Manual 100-5*, 1976, p5-10 to 5-13.

[145] Adapted from the DOD, NATO, and Army definitions of demonstration: "An attack or show of force on a front where a decision is not sought, made with the aim of deceiving the enemy. 2. (DOD only) In military deception, a show of force in an area where a decision is not sought; made to deceive an adversary. It is similar to a feint but no actual contact with the adversary is intended. (Army) 1. A form of attack designed to deceive the enemy as to the location or time of the decisive operation by a display of force. Forces conducting a demonstration do not seek contact with the enemy." Headquarters, Department of the Army, *Field Manual 1-02: Operational Terms and Graphics*, p1-57 to 1-58.

not the case. Demonstrations include training events and exercises well away from the target. For example, a demonstration of increased airborne training in the United States can be used to create the perception of a pending airborne assault.

d. Disinformation[146]

Disinformation is the exposure to target collection assets of false, modified, or selectively true information with the intent to deceive.[147] Disinformation has no set form or design; any communication from a presidential proclamation to a scrap of paper left in a waste basket can be used to convey disinformation. The British DOUBLE CROSS system during World War II is considered the exemplar for disinformation, with British intelligence using its control of the German HUMINT networks in Britain and North Africa to great advantage.[148] Disinformation also includes the flooding of the information environment with notional information for the purposes of overloading the target's systems.[149] Deceptions of this type are similar to the jamming denial type, but different in that disinformation flooding contains deceptive indicators intended to mislead the target; whereas, the jamming of a radio net with static does not. Using multiple radio networks to obscure the actual location of a unit is an example of this form of disinformation, as is swamping a regime's police hotline with false reports in order to overwhelm the response system.

---

[146] Disinformation is used here because most deception literature uses the term "ruse" to mean any manner of deception. Disinformation differs from misinformation in that disinformation requires intent to deceive; whereas, misinformation does not require intent to deceive, though the intent may be present.

[147] Adapted from the DOD definition; Headquarters, Department of the Army, *Field Manual 1-02*, 1-82. Also see Barton Whaley, *Stratagem: Deception and Surprise in War* (Cambridge, MA, Center for International Studies Massachusetts Institute of Technology, 1969), accessed 16 February 2012, http://www.vietnam.ttu.edu/virtualarchive/items.php?item=2171516001, 17.

[148] See David Mure's *Master of Deception* and Ben MacIntyre's *Agent Zigzag* for further information on the British DOUBLE CROSS system.

[149] Barton Whaley, *Stratagem: Deception and Surprise in War* (Norwood, MA: Artech House, 2007), 9.

4. Cover

Cover is the set of actions taken to protect the actual mission by preventing the deception target from receiving the indicators of real actions, capabilities, or intentions.[150] Whereas active deception seeks to provide misleading information to the deception target, cover seeks to obfuscate by masking indicators and closing channels. There are two categories of cover: camouflage and denial.

a. Camouflage

Camouflage seeks to prevent indicators from being detected by the target's collection assets. Within camouflage, there are four broad methods: hiding, blending, disguising, and securing. In hiding the item is concealed by a physical barrier; such as, a bunker, cave, forest canopy, or netting. The physical barrier itself may be visible, blended into the background, or disguised. In blending, the item is concealed by means that merge the item with the background. This can be accomplished in the field through the application of camouflage paint or natural materials. In disguising, the item is concealed by making it look like something innocuous, such as a bunker disguised as a farmhouse.[151] In securing, indicators are reduced via the use of operations security, information security, and emissions control. While not traditionally considered aspects of camouflage, securing functions serve the same purpose—suppression of friendly indicators. The concepts of camouflage are applicable across the spectrum of operations. A special operations team operating out of a safe house is hidden within the safe house, which in turn is blended into the surrounding neighborhood. A HUMINT team attached to a maneuver element is blended in with the element. An intelligence officer conducting special reconnaissance while posing as a tourist is disguised. Through proper document disposal procedures, information is secured.

---

[150] Headquarters, Department of the Army, *Training Circular No. 30-1*, 5; see Note 130 for more information on this definition of cover versus the competing definition.

[151] Headquarters, Department of the Army, *Field Manual 5-20, 1968*, 17 – 20.

b. Denial

Whereas camouflage focuses on masking indicators, denial attacks the channels indictors travel on to the target. Denial seeks to degrade target collection channels so that the adversary is either not able to receive indicators, or is herded onto a smaller set of channels. Forcing the target to depend on a smaller set of channels reduces the ability of the target to validate intelligence using multiple sources, reducing the effort necessary in telling the deception story. Additionally, if the target can be herded onto channels controlled by friendly forces, deception indicators can be fed directly into the target's intelligence cycle, as was the case with the British DOUBLE CROSS operation in WWII. Denial methods include counterreconnaissance, jamming, counterintelligence, and physical destruction of collection tools. While these methods are not normally considered aspects of deception by U.S. Army doctrine, they are forms of cover to be considered during any deception planning and execution.

5. Alternate Deception Taxonomies

In addition to the method-based taxonomy of deception, there are other taxonomies for deception. Three alternate taxonomies are: commission and omission; level of sophistication; and effect-based. These taxonomies are useful for expanding the ways to think of deception.

a. Commission and Omission

Chisholm and Feehan in "Intent to Deceive" delineate eight types of deception divided into two categories. Deceptions by commission are typified by the deceiver contributing causally to the belief of the target. Deceptions by omission are typified by the deceiver facilitating the target's maintenance of an existing belief.

Page 762 of 3957

Deception by Commission 1- Deceiver contributes causally to target acquiring belief in the proposition 2- Deceiver contributes causally to target continuing to believe in the proposition 3- Deceiver contributes causally to target stopping belief in the negation of the proposition 4- Deceiver contributes causally to target not acquiring belief in the negation of the proposition
Deception by Omission 5- Deceiver allows target to acquire belief in the proposition 6- Deceiver allows target to continue belief in the proposition 7- Deceiver allows target to cease belief in the negation of the proposition 8- Deceiver allows target to continue without the belief in the negation of the proposition

Table 2. Chisholm and Feehan's Eight Ways to Deceive.[152]

b. Level of Sophistication

Gerwehr and Glenn in *Unweaving the Web: Deception and Adaptation in Future Urban Operations* present a way to categorize deceptions based on the level of sophistication used in the deception. Sophistication is determined by the degree to which the deception takes in count the variables of a situation, e.g., environmental factors, target capabilities, target preconceptions, and the context of the situation. There are four levels of sophistication, ranging from least to most sophisticated: static, dynamic, adaptive, and preemptive. Static deceptions are the least sophisticated of deceptions and "…are in place regardless of state, activity, or the histories of either the deceiver or target."[153] The Army Combat Uniform is an example of static camouflage. "Dynamic deceptions are those that activate under specific circumstances. The ruse itself and the trigger do not change over time, nor do they vary much by circumstance or adversary."[154] A howitzer battery having established procedures to erect camouflage netting upon occupying a firing position is an example of a dynamic deception. "Adaptive deceptions are triggered like dynamic deceptions, but either the trigger or the ruse itself can be modified with experience. This category covers deception improved through trial and error."[155] Wearing cloths of local design in order to blend into crowd during a special reconnaissance mission is an

[152] Chisholm and Feehan, *The Intent to Deceive*, 143 – 159.

[153] Gerwehr and Glenn, *Unweaving the Web*, 33.

[154] Gerwehr and Glenn, *Unweaving the Web*, 33.

[155] Gerwehr and Glenn, *Unweaving the Web*, 34.

example of adaptive camouflage. Premeditative deceptions display the greatest level of sophistication. "Premeditative deceptions are designed and implemented based on experience, knowledge of friendly capabilities and vulnerabilities, and, moreover, observations about the target's sensors and search strategies."[156] Complex deceptions, such as Operation FORTITUDE, are at the premeditative level of sophistication.

c. Effect-Based

Bell and Whaley in *Cheating and Deception* present an effect-based taxonomy of deception that categorizes deception by what the deception does. This taxonomy has two broad subdivisions: hiding and showing. Hiding deceptions seek to obscure indicators, and consist of masking, repackaging, and dazzling. Masking deceptions hide by blending the object into the background, as in camouflage. Repackaging deceptions hide the real by making the object appear as something innocuous, e.g., a bunker made to look like a food stand. Finally, dazzling seeks to confound the target about certain aspects of an object, such as using multiple radio transmitters to confuse the target of a unit's true location. Showing deceptions seek to present misleading indicators to the target and consist of mimicking, inventing, and decoying. Mimicking deceptions recreate the characteristics of an object for advantage, such as using a company of soldiers to replicate a division. Inventing deceptions mislead via creation of new objects, as in notional documents. Decoying misleads by presenting alternate options as the actual option, such as the First U.S. Army Group being used to mislead German leadership as to the actual target of Operation OVERLOAD.[157]

C. DECEPTION AND UNCERTAINTY

1. Uncertainty

Uncertainty is an unavoidable aspect of military operations. Despite the desires of every commander, a perfect understanding of the situation is impossible.[158] Among the

[156] Gerwehr and Glenn, *Unweaving the Web*, 35.

[157] Bell and Whaley, *Cheating and Deception*, 49 – 61.

[158] Indeed, the belief that a perfect understanding is even possible sets the stage for deception, whether self-inflicted or enemy induced.

Page 764 of 3957

phenomena creating uncertainty are inadequacy of collection channels, infiltration of noise corruption, and the fundamental inability to read the opponent's mind. The compounded result of these phenomena is an obscuration of the situation, as if a metaphorical fog had settled over the field. As Whaley states:

> It ["the fog of war"] refers to the chaos of information inherent in the fast-breaking crisis of battle--the confusing muddle of delayed and mislaid messages, garbled and misunderstood orders, fragmentary and misinformed intelligence, pridefully exaggerated claims of successes and cringingly suppressed reports of blunders. In other words, "the fog of war" is the state of uncertainty resulting from the inability of a military information system to either accurately or speedily monitor the events of battle. The battle maps and situation reports become jangled representations of fiction and fact. The Commander neither knows what he knows nor can be certain of what he doesn't know. Crucial decisions about deployment, tactics, and strategy are made with the most fragmentary information.[159]

Deception and uncertainty enjoy a complex relationship. The fog of war created by uncertainty provides the necessary environment for deception. If the enemy possessed perfect situational awareness deception would be almost impossible. Deception in turn can be used to either thicken the fog of war—increasing the target's uncertainty—or deception can be used to present a false parting of the fog—decreasing the target's uncertainty—by revealing vista of the deceiver's making. Deception used to increase uncertainty is often referred to as ambiguity increasing, or A-Type, deception. Deception used to create a false reduction of uncertainty is often referred to as misleading, or M-Type, deception.[160]

2. A-Type Deception

A-type deceptions seek to increase the ambiguity of a situation so that the target becomes "…unsure as to what to believe."[161] Ambiguity can be increased through the use of covering deception to obscure the real situation, through the use of active

[159] Whaley, *Stratagem* (1969), 257 – 258.

[160] Daniel and Herbig, *Propositions on Military Deception*, 5-7; Additionally, *FM 90-2, 1988* calls M-type "misdirection." Headquarters, Department of the Army, *Field Manual 90-2, 1988*, 1-9.

[161] Daniel and Herbig, *Propositions on Military Deception*, 5.

deception to present a number of reasonable alternatives to the real, or a mixture of both aspects. A-type deceptions can be attempted solely through the use of covering aspects, such as a unit camouflaging itself in a wood line. One of the goals of A-type deceptions is to cause the target to delay decision-making in the hopes of further information, thereby allowing the deceiver to seize or retain initiative. Another goal is to cause the target to spread their forces in an effort to cover every potential outcome, thus affording the deceiver the opportunity to achieve relative superiority at the point of decision.[162]

3. M-Type Deception

M-type deceptions "…reduce ambiguity by building up the attractiveness of one wrong alternative."[163] All M-type deceptions utilize covering deception to obscure the true situation, while using active deception to present the false situation. One goal of M-type deceptions is for the target to concentrate resources against the deception, allowing the deceiver opportunity to successfully conduct the true plan.[164] For example, the ambush of the Japanese fleet at Midway was facilitated by deceptive radio traffic which created the perception that Admiral Halsey's fleet was still in the vicinity of the Solomon Islands.[165]

D. THE WHY OF DECEPTION

1. Overview

As discussed previously, deception is not undertaken for the sake of deception; deception is conducted to drive the behavior of the target to achieve some benefit for the practitioner or some deleterious effect for the target. Four reasons are typically given for the use of deception: to achieve surprise, to gain freedom of action, to save lives, and to

---

[162] Daniel and Herbig, *Propositions on Military Deception*, 5 – 6.

[163] Daniel and Herbig, *Propositions on Military Deception*, 6.

[164] Daniel and Herbig, *Propositions on Military Deception*, 6.

[165] Katherine Herbig, "American Strategic Deception in the Pacific: 1942-44," *Strategic and Operational Deception in the Second World War*, ed. Michael Handel (New York, Routledge,1987), 262 – 263.

mislead the enemy.[166] In addition to these reasons, there are four other reasons for attempting deception: to secure relative superiority at the point of decision, security, subversion, and mental isolation.

2. Surprise

Surprise is the most common reason cited for the use of deception. Surprise in the military context is defined as: "[striking] the enemy at a time or place or in a manner for which he is unprepared."[167] There can be no question of the role of surprise in war; of 122 battles surveyed in Whaley's classic study, the casualty ratio in battles without surprise was one-to-one; however, the casualty ratio where surprise was achieved was one-to-five in favor of the initiator.[168] Deception is the handmaiden of surprise as the secrecy necessary for surprise to succeed "…cannot be obtained by 'saying nothing.' Secrecy requires the systematic confusion and deception of the enemy."[169]

3. Freedom of Action

Deception can enhance freedom of action by decreasing the chance of enemy interference. Disguising movements of personnel, materials, and equipment as something innocuous can facilitate staging for future operations. Deceptions designed to prevent the target from interdicting lines of communication support freedom of action. Deception can also be used to assist the movement of key leaders. For example, President Roosevelt's secret meeting with Prime Minister Churchill to hammer out the Atlantic Charter in the fall of 1941 was facilitated by a portrayal depicting the president as being on a fishing trip off Cape Cod.[170]

---

[166] Jock Haswell, *The Tangled Web: The Art of Tactical and Strategic Deception* (Buckinghamshire, UK: John Goodchild Publishers, 1985), 23.

[167] Headquarters, Department of the Army, *Field Manual 3-0: Operations, Change 1*, A-3.

[168] Whaley, *Stratagem* (2007), 102 – 103.

[169] Erfurth, *Surprise*, no. 1, 33.

[170] James F. Dunnigan and Albert A. Nofi, *Victory and Deceit: Dirty Tricks at War* (New York: William Morrow and Company, Inc., 1995), 203 – 205.

Page 767 of 3957

4. Save Lives and Resources

Deception can be used to save lives and resources in three ways. First, through the achievement of surprise, gaining of freedom of action, and securing of relative superiority, deception can reduce the amount of fighting necessary to reach a decision, thus reducing casualties and material costs. Second, deception can be used to elicit surrender, thereby avoiding conflict all together. Nathan Bedford Forrest used a ruse involving a notional secret weapon to successfully elicit the surrender of four Union blockhouses during the Civil War.[171] Finally, deception can be used in the retrograde to decrease the risk to the withdrawing troops. During the Korean War, 7th Division used the fact that the Chinese forces in the vicinity of Pork Chop Hill were conditioned to seeing armored personnel carriers resupplying U.S. forces on the crest of the hill. When the decision was made to withdraw the forces, rather than risk a night withdrawal, the forces were withdrawn using armored personnel carriers mimicking a supply run.[172]

5. Mislead the Target

"Deception is by itself an asymmetric approach to warfighting: tricking the opponent into misapplying strengths and revealing weaknesses."[173] A 1948 Department of Army memorandum on strategic and tactical cover and deception training provided ten specific examples of desired outcomes for deception operations (Table 3). These outcomes were divided into positive reactions—the target takes an action to its detriment--and negative reactions—the target fails to take an action to its detriment.

How deception can be used to mislead the target into not exploiting a weakness is illustrated by an example from the Vietnam War. A brigade commander was ordered to detach two battalions to support another operation, and the brigade commander realized that to do so would offer the Viet Cong an opportunity to exploit the reduction in forces

---

[171] The Editors of the Army Times, *The Tangled Web: True Stories of Deception in Modern Warfare* (Washington, DC: R. B. Luce, 1963), 3.

[172] U.S. Army Command and General Staff College, *Reference Book 31-40: Techniques for Deception* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 1976), p6-9 to 6-10.

[173] Scott Gerwehr and Russell W. Glenn, *The Art of Darkness: Deception and Urban Operations* (Santa Monica, CA: RAND, 1999), 10.

in his area of operations. In order to support the requirement while preventing the Viet Cong from seizing the advantage, the brigade commander directed support personnel to portray the advance parties of another division while spreading the rumor that the portrayed division would be assuming control of the area of operations. The combination of the portrayal and the ruse caused the Viet Cong to go to ground, denying them the opportunity to exploit the brigade's temporary loss of maneuver forces.[174]

Positive reactions by target to deception
1- Movement of reserves and their premature commitment to erroneous positions 2- Engagement by enemy in activities which exhaust his resources and/or prohibits their use elsewhere (i.e., extensive defensive preparations) 3- Dispersal or over-extension of enemy forces 4- Diversion of enemy thrusts 5- Disclosure of enemy positions
Negative reactions by target to deception
1- Failure to move reserves to meet intended offensives 2- Failure to exploit our weaknesses 3- Failure of counterattack 4- Failure to disengage 5- Failure to locate and act against true positions of artillery, reserves, dumps, etc.

Table 3. Examples of Target Responses to Deception.[175]

6. Relative Superiority

Relative superiority is the "condition that exists when an attacking force… gains a decisive advantage over a larger or well-defended force."[176] Deception, along with surprise and maneuver is an essential tool for gaining relative superiority.[177] Demonstrations and feints that draw away the defender's reserves from the point of decision assist in the achievement of relative superiority. The aspects of Operation FORTITUDE that caused the German command to retain forces in Pas de Calais even after the Normandy landing assisting in the Allies gaining and maintaining relative superiority

[174] U.S. Army Command and General Staff College, *Reference Book 31-40*, 6-12.

[175] Office of the Chief of Army Field Forces, *Strategic and Tactical Cover and Deception*, 13.

[176] William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare Theory & Practice* (Novato, CA: Presidio Press, 1995), 4.

[177] Headquarters, Department of the Army, *Field Manual 100-5: 1976*, 3-6 to 3-7.

Page 769 of 3957

at the Normandy beachhead. Use of deception to bait a superior force into an ambush is time honored technique used by inferior forces to gain relative superiority.

7. Security

Deception can be a vital asset for maintenance of security. "Real secrecy can only be achieved if, in addition to the correct information which the enemy receives, he is also provided with incorrect information. Confusion is the only effective method of maintaining secrecy."[178] This is especially true for irregular warfare and intelligence operations. Deception in support of security typically relies heavily on camouflage and denial. In addition to the cover aspects, ruses in the form of cover stories and notional documents are used frequently. Status for cover and status for action are terms for the cover stories developed to protect intelligence operatives and facilitate their missions. MACVSOG utilized a set of cover stories for the overall organization, subordinate elements, and even missions in an effort to obscure its activities.[179] The cover for status of MACVSOG stated the organization was simply a special staff section focused on the comprehensive study of counterinsurgency operations, with no implementation authority.[180]

8. Subversion

Subversion is defined as: "Action designed to undermine the military, economic, psychological, or political strength or morale" of a targeted organization.[181] Deception can be used in a subversion role, by exploiting internal cleavages within the targeted organization in order to foment mistrust and discord. In addition to mistrust and discord,

---

[178] General Alfred Krauss as quoted in: Erfurth, *Surprise*, 6.

[179] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Appendix H Security, Cover & Deception* (Washington, DC: Joint Chiefs of Staff, 1970), accessed 2 September 2011. http://www.dod.gov/pubs/foi/International_security_affairs/vietnam_and_southeast_asiaDocuments/520-18.pdf.

[180] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Appendix H Security, Cover & Deception*, H-10.

[181] This definition is modified from the official definition by substituting targeted organization for regime in order to allow for targeting of non-state actors. Headquarters, Department of the Army, *Field Manual 1-02*, 1-178.

subversive deception can be used to introduce friction into the target's decision cycle and actions; thereby, reducing the overall effectiveness of the target.[182] Subversion by deception may be particularly effective when used against organizations sensitive to internal threats; such as, networked terrorist groups and authoritarian regimes. MACVSOG's use of poison pen letters to increase distrust within the North Vietnamese leadership is an example of deception to achieve subversion.[183]

9. Mental Isolation

Deception Mental isolation occurs when the target is unable to perceive or make sense of the situation.[184] The ultimate goal of mental isolation is to reduce the target to passivity or paralysis as the target is unable to appreciate or cope with the practitioner's actions.[185] Deception in support of mental isolation seeks to create an impenetrable fog of war through camouflage and denial, while increasing uncertainty and ambiguity by the presentation of conflicting information through what channels the target retains access to.[186] The effective mental isolation and subsequent paralysis of a target can negate the target's fighting power and thus ability to resist.[187] During the Six-Day War, Israeli Military Intelligence attempted a form of mental isolation against Arab forces. Operation FOG OF BATTLE "misled top enemy commanders, drew them into traps, diverted their forces in the wrong directions, spread confusion and chaos within upper level enemy headquarters, and speeded up the process of demoralization and disintegration of the channels of command."[188]

---

[182] Friction is defined as "the accumulation of chance errors, unexpected difficulties, and the confusion of battle." Headquarters, Department of the Army, *Field Manual 100-5, 1986*, 16.

[183] Richard H. Shultz, *The Secret War Against Hanoi : Kennedy and Johnson's Use of Spies, Saboteurs, and Covert Warriors in North Vietnam* (New York: HarperCollins, 1999), 136.

[184] John Boyd, "The Strategic Game of ? and ?" (Presentation, John Boyd Compendium, 1987), accessed 19 February 2012, http://www.danford.net/boyd/strategic.pdf, 36.

[185] Boyd, *The Strategic Game of ? and ?*, 47.

[186] Mao Tse-tung, "On the Protracted War " in *Selected Works of Mao Tse-Tung*, Vol. 2 (Peking: Foreign Language Press, 1965), 166.

[187] Basil Henry Liddell Hart Sir, *Strategy*, 2d rev ed. (New York: Meridian, 1991), 212.

[188] Leo Heiman, "War in the Middle East: An Israeli Perspective," *Military Review* 47, no. 9 (1967), 60.

E. COMMUNICATIONS PROCESS OF DECEPTION

1. Overview of Communications

In order to understand deception, it is necessary to look at the context in which deception is practiced. Of importance to the understanding of deception are the communications environment and the target's decision-making process. Roberta Wohlstetter's *Pearl Harbor: Warning and Decision* provides insight to the role of noise within the communications process. Wohlstetter defines noise as competing or contradictory signals that are useless for understanding a situation.[189] William Reese's "Deception within a Communications Theory Framework" presents an overview of communications theory that is critical to understanding the process by which information is transmitted from the practitioner to the target. Reese includes in his work the roles of channels and indicators; as well as, the ways by which errors enter the process.[190] Whaley and Bell's collaboration *Cheating and Deception*; as well as, Bell's "Toward a Theory of Deception" discuss how deception works through communication.

Deception occurs within the framework of communication (Figure 6). An actor is constantly emitting indicators of his actions, capabilities, and intentions into the environment, and is likewise constantly receiving indicators from other actors. Indicators travel from one actor to another via channels. Some indicators are not perceived by the target due to the lack of a viable channel to convey the information. Other indicators are corrupted by errors of encoding, transmission, or decoding. The corruption of indicators is a form of noise. The indicators an actor receives from other actors in the environment constitute another form of noise. The limited set of indicators that do reach the target are what the target relies on to form the perceptions of the practitioner for use in the target's decision-making process. Because the target does not have access to all the indicators of the practitioner, the target never has a complete picture of the actor's intentions, capabilities, and actions.

---

[189] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), 3.

[190] William Reese, "Deception within a Communications Theory Framework," in *Strategic Military Deception*, eds. Donald C. Daniel and Katherine L. Herbig (Elmsford, NY: Pergamon Press Inc, 1982), 99 – 114.

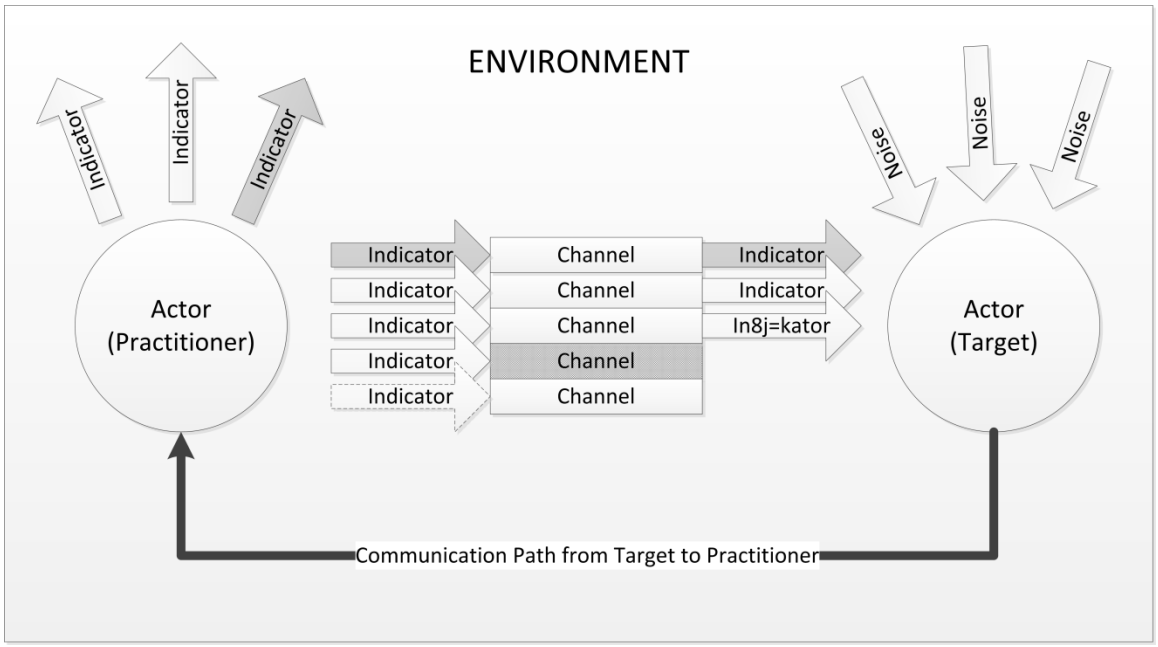


Figure 6. Communications Cycle

As Figure 6 shows, deception works within the communications process. The practitioner is constantly emitting indicators of his actions into the environment. Some indicators are not seen by the target as there is no channel to convey the indicator to the target. The white indicators represent indicators of the practitioner's true capabilities and intentions. The grey indicators represent deceptive indicators. The dashed line indicator represents an indicator obscured through cover means. The In8j=kator indicator represents an indicator corrupted by errors in encoding, transmission, or decoding. The cross-hatched channel is a channel closed through denial means. Finally, the noise arrows represent indicators from other actors or the environment that interfere with the target's perception of the practitioner's indicators. The process depicted is one-half of the complete communications process. There is a mirror process running from the target to the practitioner as indicated by the black arrow.

2. Indicators

Indicators are individual snippets of information about the capabilities, intentions, and actions of an actor created through the actor's interaction with the environment. Indicators can take myriad forms and include exercises and training events; personnel and

equipment movements; updates on social network sites and other communications activity; and solicitations for contracts.[191] These pieces of information can be real or deceptive. The purpose of deceptive indicators is to provide the target with the information required for the target to draw the conclusion that the deception story is reality.

Indicators, whether real or notional, are subject to errors in encoding, transmission, and decoding. Errors in encoding occur at the origin of the indicator and may result from typographical or syntax errors, improper execution of guidance, and translation errors. For example, a notional identification document with an outdated stamp is an error in encoding. Errors in transmission alter the indicator as it transits a channel from the transmitter to the receiver and can occur due to noise causing corruption, interaction with the channel causing changes to the indicator, or the failure of the channel to pick up the indicator. Technical faults in the target's reconnaissance plane resulting in indicators of troop movements not being observed is an example of an error in transmission. Errors in decoding enter the indicator as it is being processed by the receiver, and can include mistakes in interpretation and failures in perception. An imagery analyst mistaking a tank for a truck is an error in decoding.[192]

3. Channels

Channels are "the specific ways in which information about a given subject reaches an audience."[193] For deception, the most commonly used channel is the intelligence collection capabilities of the target. Intelligence channels consist of the suite of intelligence collection capabilities, e.g., human, signals, open source, and imagery. Examples of intelligence channels range from the double agents used by Britain in World War II as part of the Double Cross system to notional radio traffic.[194] In addition to

[191] To reinforce the variety of indicators, one—possibly apocryphal—indicator of crisis planning at the White House is said to be late night pizza deliveries.

[192] Reese, *Deception within a Communications Theory Framework*, 99 – 114.

[193] Godson and Wirtz, *Strategic Denial and Deception*, 19.

[194] Abram Shulsky, "Elements of Strategic Denial and Deception," in *Strategic Denial and Deception: The Twenty-First Century Challenge*, eds. Roy Godson and James J. Wirtz (Piscataway, NJ: Transaction Publishers, 2002), 19 – 26.

intelligence collection channels, there are many other channels for indicators to reach the target (Table 4). One of the goals of cover is to reduce the number of channels available to adversarial intelligence collection, as restricting channels makes the intelligence collection more dependent on the remaining channels, and reduces the likelihood of indicators of the actual plan reaching the target. Channels can be preexisting or created in support of the deception plan. The use of a corpse by British intelligence during WWII to convey notional plans to German intelligence is an example of a created channel.

Intelligence	Human, Signal, Imagery, Measures, Electronic
Traditional Media	Newspapers, Radio, Television, Handbills, Leaflets, Loudspeakers
Internet	Social Media Sites, Commercial Email, Notional Sites
Military Communications	Radio, Official Email, Orders, Radar
Diplomacy	Negotiations, Communiques, Official statements
Other	Word-of-mouth, Surveys, Telephone

Table 4. Examples of Channels

4. Deception's Role in the Communications Process

In addition to deception operating within the communications framework, deception affects the communications process itself on a number of levels. Indicators can be camouflaged to prevent the target from recognizing the indicators. Alternatively, indicators can be reduced through various security measures. Channels can be closed off via denial capabilities. For indicators that cannot be hidden from the target by cover tools, simulations and portrayals can be used to drown the indicator in a sea of noise.

F. DECEPTION AND TARGET DECISION-MAKING

To understand how deception affects the target, it is imperative to understand how decisions are made. Decision-making is not a rigid process of whereby two individuals can see the same indicator, reach the same conclusion, and act the same way; rather, decision-making is subject to numerous schemata—cultural, personal, and cognitive—the

composite of which is unique to every individual. Colonel John Boyd's "Organic Design for Command and Control" introduces a framework for the decision-making process, the Observe-Orient-Decide-Act (OODA) loop.[195] The OODA places decision-making in an iterative process where perceptions are created by the synthesis of new information and existing perceptions through the schematic lenses. From the revised perceptions, decisions are made, driving actions and inaction. While Boyd includes the lenses in his decision-making framework, he does not go into depth discussing how culture, personal experiences, and genetic heritage impact decisions.

Richard Heuer's *Psychology of Intelligence Analysis*, though intended as a tool for intelligence analysts contains a trove of information for the deception practitioner. Of particular use is Heuer's discussion of cognitive biases. Cognitive biases are defined by Heuer as "mental errors caused by our simplified information processing strategies… a cognitive bias does not result from any emotional or intellectual disposition towards a certain judgment, but rather from subconscious mental procedures for processing information."[196] Heuer categories the cognitive biases by their effect on intelligence analysis: "evaluation of evidence, perception of cause and effect, estimation of probabilities, and retrospective evaluation of intelligence reports."[197]

Michael Bennett and Edward Waltz's *Counterdeception Principles and Applications for National Security* expands the discussion of biases by adding three additional categories: personal, cultural, and organizational. Personal biases "are the result of personality traits and the firsthand experiences that affect a person's world view throughout the course of their life."[198] Cultural biases are "the result of interpreting and judging phenomena in terms particular to one's own culture and is influenced by the knowledge, beliefs, customs, morals, and habits, and cognitive styles that are acquired as

---

[195] John Boyd, "Organic Design for Command and Control," (Working Paper, 1987), accessed 19 February 2012, http://www.danford.net/boyd/organic.pdf.

[196] Richards J. Heuer Jr., *Psychology of Intelligence Analysis* (Reston, Virginia: Pherson Associates, LLC, 2007), 111.

[197] Heuer, *Psychology of Intelligence Analysis*, 112.

[198] Michael Bennett and Edward Waltz, *Counterdeception Principles and Applications for National Security* (Norwood, MA: Artech House, Inc., 2007), 73.

a member of one's specific social environment."[199] Organizational biases are "the result of the goals, mores, policies, and traditions that characterize the specific organization in which the individual works."[200] Bennett and Waltz's expansion of biases increases the number of potential levers a deception practitioner has to influence the deception target.

In order to explore how deception affects the target, an expanded version of the OODA process is used to represent the target's decision-making process. The OODA process consists of four interconnected phases: observe, orient, decide, and act (Figure 7)

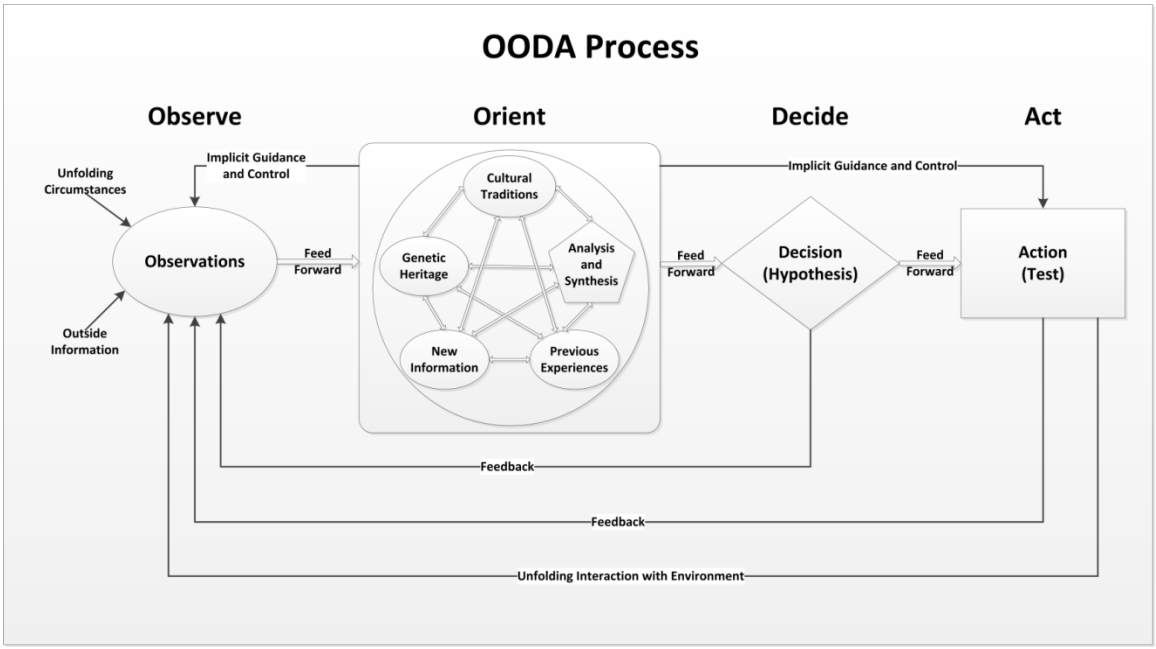


Figure 7. Expanded OODA Process (From: [201])

1. Observe

During the observe phase, the target interacts with the environment, actively and passively collecting indicators in an effort to gain an understanding of the situation. Despite the wishes of every actor, it is impossible to collect a perfect picture of the situation as some indicators are missed and others corrupted by transmission and coding

199 Bennett and Waltz, *Counterdeception Principles*, 72.

200 Bennett and Waltz, *Counterdeception Principles*, 74.

201 Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York, NY: Back Bay Books, 2002), 344.

errors. The inability to perceive the total picture is the "fog of war." Additionally, the target's existing perceptions of the environment and situation affect which indicators the target observes.[202] As Thomas Kuhn states: "What a man sees depends both upon what he looks at and also upon what his previous visual-conceptual experience has taught him to see."[203] It is during the observation phase the deception practitioner interacts with the target. Through camouflage, indicators of friendly activity are obscured from target collection. Furthermore, through denial, target collection channels are closed off, preventing the collection of unobscured indicators—both friendly and other actor. Finally, through active deception, manipulated or manufactured indicators are presented for collection, which taken together tell the deception story. Through these means, the fundamental effects of deception in the observe phase are to either thicken the fog of war by increasing ambiguity or uncertainty by obscuring indicators, or to part the fog of war by seeming to decrease ambiguity or uncertainty through the presentation of indicators revealing a misleading picture of the situation. It is necessary to understand the collection capabilities of the target in order to increase probability of reception of the manipulated indicators; as well as, to prioritize camouflage and denial activities towards protecting vulnerable indicators. Equally important is an understanding of what the target expects to see from the practitioner; in other words, the practitioner needs to develop a detailed understanding of self through the lens of the target.

2. Orient

After the observe phase, the target transitions to the orient phase. During the orient phase, the target processes the collected indicators through a series of schemata and synthesizes the result with the target's existing perceptions to create revised perceptions of the environment and situation. Schemata are defined as: "…the dynamic, cognitive knowledge structures regarding specific concepts, entities, and events used by

---

[202] Heuer, *Psychology of Intelligence Analysis*, 8 – 10.

[203] Thomas Kuhn, *The Structure of Scientific Revolutions*, 3rd ed. (Chicago: University of Chicago Press, 1996), 113; This is an important point; an engineer, infantryman, and helicopter pilot looking at a wooded glen will *see* different things. The engineer may see the glen in terms of soil substrate suitability for a road; the infantryman may see the glen in terms of cover, concealment, and avenues of approach; while the pilot sees in terms of potential landing zones.

Page 778 of 3957

individuals to encode and represent incoming information efficiently."[204] These schemata create biases in the way the target perceives and processes information. Schemata can be categorized as cultural, personal, and genetic. Cultural schemata include the collective experiences, legacies, biases, and heuristics developed by organized groups. Personal schemata include personal experiences and the resultant biases and heuristics. Genetic schemata include the cognitive biases and heuristics developed through conflict based natural selection. Schemata and the resultant biases can both aid and hinder deception efforts.

a. Cultural Schemata

Cultural schemata are the collective set of knowledge, beliefs, experiences, values, and norms for a distinct aggregate of people with similar characteristics, e.g., state, ethnic group, region, religion, and organization. A target can be influenced by several different sets of cultural schemata, for example, a Sunni Muslim Iraqi Kurd is influenced by the schemata for his Sunni Islam, Iraqi, and Kurdish aspects. While members of a particular culture are not perfectly uniform in their cultural schemata, understanding the culture of the target is vital to the success of deception. Culture can be a source of trappings for a deception to increase its legitimacy, for example, the Sacred Sword Patriots League deception in Vietnam was based in a Vietnamese legend of a divine sword given to a prince to drive out the occupying Chinese.[205] Additionally cultural biases can impact the credibility given to different channels. For example, in a country without a tradition of free press, there may be less credibility given to traditional media channels. Likewise, in societies with a strong oral tradition; such as Arab societies, word of mouth channels may have higher credibility than in societies without a strong oral tradition. Understanding the degree to which a culture values certain channels can help in deciding which channels to priorities for exploitation or denial.

---

[204] Hazel Markus, "Self-Schemata and Processing Information about the Self," *Journal of Personality and Social Psychology* 35, no. 2 (1977), 63 – 78. as cited in Stanley G. Harris, "Organizational Culture and Individual Sensemaking: A Schema-Based Perspective," *Organization Science* 5, no. 3 (August, 1994), 310.

[205] Shultz, *The Secret War Against Hanoi*, 139 – 140.

Much like the social groups, organizations possess a distinct set of schemata that influence information processing. These schemata in turn generate organizational biases. An example of an organizational bias with applicability to deception operations occurred in the Burma Campaign of World War II. The Japanese command in Burma did not trust its intelligence analysts. British efforts to deceive the Japanese commander failed because of this bias against the intelligence analysts, the deception indictors presented by the British never impacted the Japanese commander's decisions.[206] A second example of organizational schemata impacting deception, this time to negative results, occurred as part of British plans to invade Italian controlled Abyssinia [Ethiopia]. The British plan called for an attack into northern Ethiopia, and a deception to make it appear the attack would come from the south. The British successfully deceived the Italians into believing the attack would come from the South; however, the British failed to account for the Italian Army's desire to avoid combat. Rather than reinforcing the southern approaches to repulse the perceived British offensive, the Italians withdrew northward, towards the actual British offensive.[207] [This episode led to Dudley Clarke's admonishment to plan deception in terms of the target's actions, and not the target's perceptions]

b. Personal Schemata

Whereas the cultural schemata are the result of the social environment, personal schemata are the result of the one's experiences, motivations, and emotions. Four variables impacting the degree to which an experience might affect an individual's worldview: whether the experience was first hand; how early the event occurred in the individual's lift; how important the consequences of the event were to the individual or his nation; and whether the individual has a sufficient range of experience to develop alternative perceptions.[208]

---

[206] Dewar, *The Art of Military Deception in Warfare*, 10.

[207] Dudley Clarke, 6 September 1972, "Some Personal Reflections on the Practice of Deception in the Mediterranean Theatre from 1941 to 1945," memorandum included in David Mure, *Master of Deception: Tangled Webs in London and the Middle East* (London: William Kimber & Co. Limited, 1980), 273.

[208] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), 239.

Within the context of deception, personal create exploitable vulnerabilities. For example, the paranoia of Stalin about internal security threats created a vulnerability which German intelligence exploited by creating a set of notional dossiers detailing Soviet officers' interactions with German intelligence officers. In a brilliant move, the dossiers were not created from scratch; rather Abwher used dossiers from an actual episode of German-Soviet military cooperation in 1927 as the basis for the notional dossiers. By modifying existing documents, Abwher managed to expediently create dossiers with an air of believability—the best deceptions are built on truth. While it cannot be proven the deception led to the subsequent purge by Stalin of not only the officers in the dossiers, but over 20,000 personnel, including a majority of senior leaders, the timing would seem to indicate a connection. The decimation of the Soviet armed forces during the 1937–1939 purge significantly reduced the effectiveness of the Soviet armed forces prior to Operation BARBAROSSA.[209]

c. Cognitive Biases and Heuristics

Cognitive biases and heuristics are what the OODA loop considers to be genetic heritage; that is cognitive biases and heuristics have developed through natural selection. There are many cognitive biases and heuristics; the ones most pertinent to deception are: small numbers, anchoring, confirmation, Rubicon, and availability.

Small numbers bias, also known as representativeness, is the tendency to overestimate the reliability of a small sample to be representative of the total set. Furthermore, this bias creates overconfidence in observed patterns and early trends. Taken together, this means that the perceptions of individuals are created by a smaller set of information than is thought.[210] Deception benefits from the small number bias by lessening the number of indicators needed to generate the required perception. However, the small numbers bias also increases the difficulty of shifting initial perceptions.

---

[209] Edward Epstein, *Deception: The Invisible War between the KGB and the CIA* (New York, NY: Random House Value Publishing, 1991), 140 – 143.

[210] Amos Tversky and Daniel Kahneman, "Belief in the Law of Small Numbers," *Psychology Bulletin* 76, no. 2 (1971), 105 – 110.

Page 781 of 3957

Anchoring heuristic also impacts how an individual adjusts an existing perception based on new information. There is a tendency for the starting perception to act as friction on any adjustments so that the adjusted perception may be closer to the starting position than appropriate.[211] Anchoring's importance to deception is twofold. First, anchoring reinforces the maxim that deceptions should use the target's existing perceptions. Second, anchoring indicates a need to ensure when deception is in support of a specific plan that the deceptive indicators are transmitted before indicators of the actual plan begin transmission.

Confirmation bias exhibits itself in the tendency of individuals to interpret new information in ways supportive to the individual's established perceptions.[212] Confirmation bias is one reason why deceptions that exploit existing target perceptions are preferable to deceptions that seek to change target perceptions. Additionally, confirmation bias is another reason to seek to implement deception prior to the target forming its initial perceptions. If the initial perceptions are formed relying on deceptive indicators, then confirmation bias will generally work to support the deception.

Rubicon bias is the tendency of individuals to place greater confidence in a decision once the decision is made. Prior to making a decision, an individual tends to evaluate the benefits, costs, and risks of the various options in reasonably deliberative manner—subject to the lenses of personal experience and other biases and heuristics. However, once a decision is made, the individual tends to view that decision as being the best possible decision.[213] Along with confirmation bias, the Rubicon bias suggests that deceptions should seek to leverage existing perceptions; rather than seeking to create new perceptions.

The availability heuristic expresses itself in the tendency of a person to evaluate the likelihood of an event based on "…the ease with which they can imagine

---

[211] Heuer, *Psychology of Intelligence Analysis*, 150 – 151

[212] Thomas Gilovich, *How We Know What Isn't So* (New York: The Free Press, 1991), 33.

[213] Dominic Johnson and Dominic Tierney, "Crossing the Rubicon: The Perils of Committing to a Decision" (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2011).

relevant instances of the event and the number or frequency of such events that they can easily remember."[214] In addition to recall, the availability heuristic also depends on the ability of a person to imagine an event. The availability heuristic impacts deception on several levels. First, since successful deceptions are often related to significant events, the availability heuristic can cause the perception of deception where none exists. Next, since the availability heuristic relies on recall and imagination, deception can be used to reduce or increase the perceived probability of an event. Finally, since the availability heuristic utilizes the probable, deception can be used to protect the unexpected by providing plausible explanations; for example, protecting human agents by attributing collected information to signals intelligence assets.

d. Results of Orientation

The results of the orient phase are revised perceptions of the situation and environment that are fed into the decide phase. Gaps in information identified during the analysis and synthesis can result in new requirements for the observe phase. Additionally, the revised perceptions impact how the expectancy bias affects the collection of new information. Successful deception corrupts the outputs of the orientation phase causing the target to perceive the situation as the deceiver intends.

3. Decide

Once the indicators are synthesized and analyzed, and the target's revised perception of the situation is created, the process transitions to the decide phase. During the decide phase, the target uses his perception to develop his courses of action. This phase marks the transition of the target from a deliberative mind-set to an implementation mind-set.[215] In addition to the decide phase feeding forward into the act phase, feedback from the decision phase feeds back into the observe phase as new information requirements.

---

[214] Bennett and Waltz, *Counterdeception Principles*, 102.

[215] Johnson and Tierney, "Crossing the Rubicon," 1.

4. Act

Finally, the chosen courses of action are implemented. These activities create indicators via interaction with the environment. It is at this point a successful deception plan reaches fruition though the target's implementation of the decided actions or inactions based on the manipulated perception. If the deception story is accepted and acted upon, there should be evidence in the indicators created by the target's activities. While indicators of successful deception are important, equally as important are indicators of deception failure; the deception practitioner should seek to collect indicators looking for feedback that the deception did not work.

G. DECEPTION PROCESS

1. Bell and Whaley

Bell and Whaley present the deception process as a deception planning loop that begins with the development of a desired deception goal in support of the strategic goal. The first half of the loop is the decision sector where the potential stratagem, illusion, channel, ruse, and characteristics are considered. The second half of the loop, the perception sector, executes the characteristics to drive the ruse through the selected channel in order to generate the intended illusion to activate the chosen stratagem to achieve the deception goal[216] (Figure 8). Bell and Whaley's process is demonstrated using their example from *Cheating and Deception* in figure 9. Bell and Whaley's deception planning process is thorough, but falls short of its potential. One key shortcoming is that the process ends with what the target thinks, rather than what the target does. This runs the risk of the target thinking what the deceiver desires, but not acting in the desired way.

[216] Bell and Whaley, *Cheating and Deception*, 71.

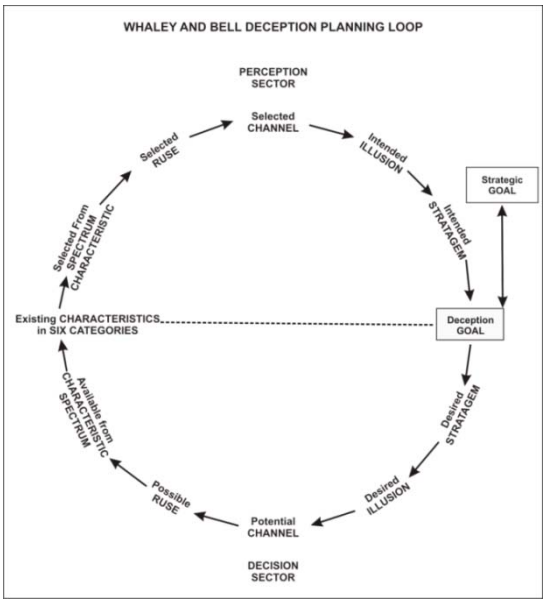


Figure 8. Bell and Whaley's Deception Planning Loop (From: [217])

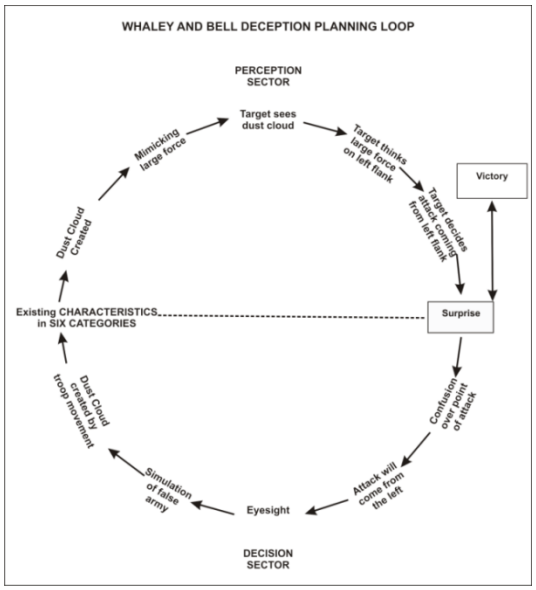


Figure 9. Example of Bell and Whaley's Deception Planning Process in Action (From: [218])

[217] Bell and Whaley, *Cheating and Deception*, 71.

[218] Bell and Whaley, *Cheating and Deception*, 70 – 72.

2. See-Think-Do

An alternate deception process is articulated in *Joint Publication 3-31.4: Military Deception*. *JP 3-13.4* utilizes a three step deception process: See-Think-Do. In the See-Think-Do model, the deception practitioner first decides what action or inaction the target must do in order to support the overall plan. This behavior becomes the deception objective. Next, the practitioner considers what the target must think in order to cause the deception goal. Finally, the practitioner formulates what the target must see in order to create the necessary perceptions to drive the target's thoughts. The set of indicators the target needs to see becomes the deception story.[219] While this process offers a direct, to the point, tool for deception planning, the model oversimplifies the complexities of target decision-making.

3. Revised Deception Process

Merging Bell and Whaley's deception planning loop together with the See-Think-Do process in the context of the communication and decision-making frameworks provides a potentially fuller understanding of the deception process (Figure 10) The process starts with the identification of a strategic, operational, or tactical objective, e.g., establish a beachhead on the mainland of Europe. From this objective a deception objective is derived, e.g., German forces reinforce Pas de Calais, leaving Normandy thinly defended. Potential deception objectives must be feasible, that is, the target must be capable of performing the action or inaction, and the action or inaction must be reasonable. Once the deception goal is determined, the next step is to evaluate what the target must think in order to drive the desired action, e.g., Pas de Calais is the Allied objective. This phase corresponds to the orient and decide stages of the OODA process. Critical to the determination of what the target needs to think is the knowledge of what the target already thinks; as well as, what cultural, organizational, and personal schemata influence the target's decision-making. In the case of the example, knowing the Germans already viewed Pas de Calais as the likely landing zone greatly aided the deception

[219] Joint Staff, *JP 3-13.4: Military Deception*, (Washington, DC: Department of Defense, 2006), pIV-1 to IV-2.

Page 786 of 3957

process. Likewise, had this phase revealed the Germans viewed Normandy as the most probable target the entire deception, and in deed the entire plan, would have to be reevaluated.

After the desired perception is decided, then the set of indicators necessary to create the perception must be designed, e.g., feints in the form of bombing and reconnaissance flights over Pas de Calais; disinformation through DOUBLE CROSS system; and simulated Allied forces staging across the English Channel from Pas de Calais. This set of indicators is what will paint the deception picture for the target to see. Again it is vital to understand what the target already perceives, as the existing perception not only drives how new indicators are interpreted through filters like the expectancy and confirmation biases, but also what the target sees the indicators as. Additionally, the channels available for the target to receive indicators must be identified, and of those channels which will be denied the target. Finally, based on the analysis of the available channels, and the indicators needed for the deception story, a prioritized set of indicators of the actual plan lays out what must be hidden from the target. In the example, many of the indicators of the Normandy Invasion did not contradict the Pas de Calais deception, and thus did not need to be covered; such as, the airborne training operations, and the general build up of materials and personnel. This allowed cover efforts to focus on protecting critical indicators like the Mulberry harbors. Once the deception plan is implemented, collection of enemy indicators is essential. These indicators help the deceiver to determine if the deception succeeded or more importantly if it failed.

Page 787 of 3957

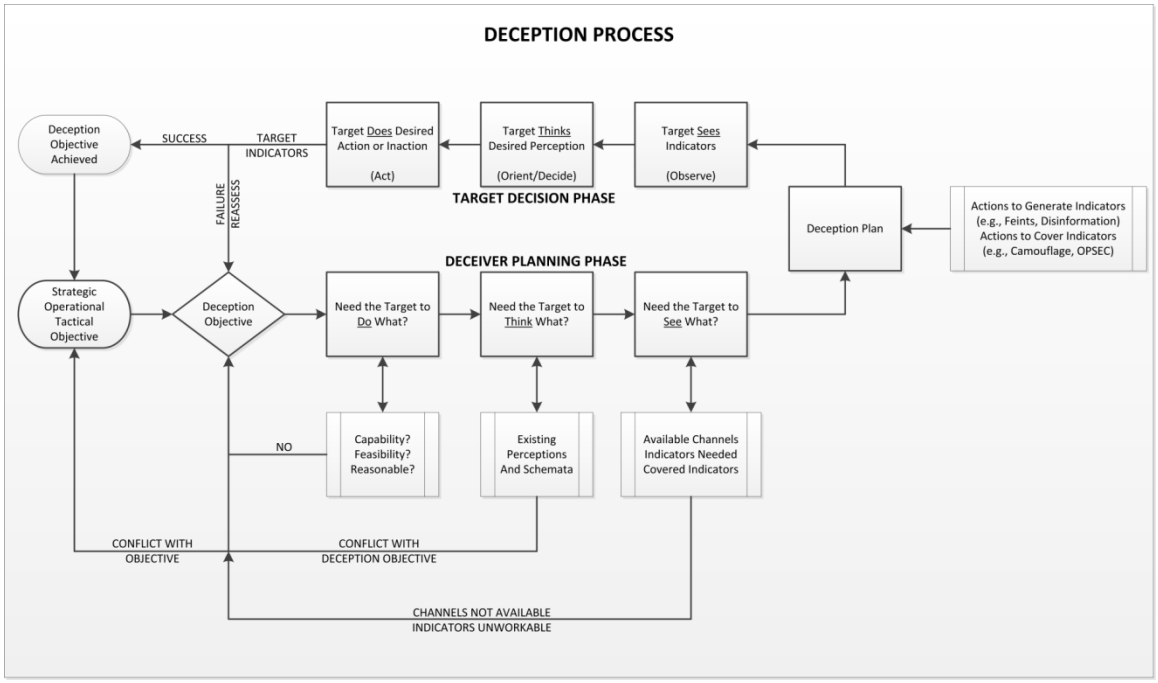


Figure 10. Revised Deception Process

V. PRACTICE OF MILITARY DECEPTION

> *I feel that deception and cover plans or operations are fully justified and that the employment of cover and deception should . . . be an accepted and organized procedure for any campaign.*
>
> *– General George S. Patton*[220]

FM 90-2: Battlefield Deception provides a five-step deception planning process. Step one—situation analysis—focuses on friendly and enemy situations, target analysis, and a stated desired situation. Step two—deception objective formulation—consists of determining the five w's of the deception objective: what action/inaction is necessary to achieve the desired situation; who must perform the action/inaction; when and where must they act; and who must be affected. Step three—desired perception—develops an idea of what the enemy must think to make him act in the desired manner, and what perceptions must be created in order to persuade the enemy to think in the desired way. Step four—deception story—generates the information that when conveyed to the target paints the perception picture for the target. Step five—deception plan—focuses on producing the overall plan for how to convey the necessary information to the enemy, as well as the recommending the intelligence requirements to look for indicators that the plan is working or not.[221]

FM 3-13: Information Operations provides a five-step deception planning process designed to nest within the Army's military decision making process [MDMP]. The steps to the process as outlined in *FM 3-13* are: receipt of the mission; mission analysis; course of action development; course of action analysis, comparison, and approval; and orders production. Though the names are different than the steps in *FM 90-2*, the processes within the steps are very similar. In addition to the planning process, *FM 3-13* provides guidance on the preparation, execution, and assessment of the deception plan. Interestingly, the initial iteration of the information operations field manual, *FM 100-6*, published in 1996, did not contain a discrete deception planning process.

---

[220] Quoted in Center for Army Lessons Learned, *CALL Bulletin 3-88*, 7.

[221] Headquarters, Department of the Army, *Field Manual 90-2: Battlefield Deception*, 4-4 to 4-15.

JP 3-13.4: Military Deception, provides a six-step deception planning process based on the Joint Operation Planning and Execution System [JOPES]. The six steps are: deception mission analysis; deception planning guidance; staff deception estimate; commander's deception estimate; deception plan development; and deception plan review and approval.[222] The content of these steps is similar to the steps in *FM 90-2* and *FM 3-13*, with the addition of the SEE—THINK—DO methodology.

In addition to the preceding examples of doctrinal deception planning, there is a vast body of official and unofficial research addressing the planning and practice of deception. Exemplars of the official research include the CIA Deception Research Program's *Deception Failures, Non-Failures and Why* and *Deception Maxims: Facts and Folklore*; the U.S. Army Research Institute for the Behavioral and Social Sciences' *Doing Deception: Attacking the Enemy's Decision Processes*; and Hans von Greiffenberg's *Deception and Cover Plans Project #29*, which analyzes German deceptions during World War II. Representative of the unofficial research is Benjamin Higginbotham's "On Deceiving Terrorists," which looks at using deception against non-state actors.

Finally, there are a number of historic accounts of deception planning and execution to draw from, with much of the work covering the World War II era. For example, Roger Hesketh's *Fortitude* represents the official history of the London Control Section's pinnacle operation. Similarly, the *Official History of the 23rd Headquarters Special Troops* details the unit's creation and conduct of tactical deception in the European Theater of Operations. David Mure's *Master of Deception* covers Dudley Clarke's A-Force in North Africa, and includes a memo from Clarke outlining his thoughts and observations on deception. Anthony Cave Brown's *Bodyguard of Lies* is a massive tome covering nearly the totality of Allied deception, espionage, and clandestine operations in the European Theater of Operations. The critical value of these works is their discussion of deception in real world application—outside the realm of theory.

---

[222] Joint Staff, *JP 3-13.4*, IV-3.

Page 790 of 3957

A. DECEPTION PLANNING PROCESS

The 2012 edition of JP 3-13.4 utilizes a six-step process for planning deception: deception mission analysis, deception planning guidance, staff deception estimate, commander's deception estimate, deception plan development, and deception plan review and approval.[223] This planning process will serve as the framework for the discussion of deception planning, with modifications derived from other works.[224]

1. Mission Analysis

The current U.S. military guidance on planning military deception has the military deception process overlaid on either MDMP or JOPES planning processes. This is not sufficient. Aspects of military deception planning must occur before the beginning of formal planning, and ideally the introspective analysis of friendly forces should be a continuous process even prior to receipt of a mission. For example, development of profiles of potential target leaders must be integrated with ongoing intelligence preparations, so that when the planning process begins this vital groundwork is already in place. Additionally, a firm understanding of friendly force indicators is necessary in order to plan on how to cover critical indicators; as well as, determining what indicators are necessary to create the perception of particular activities, e.g., the indicators created by pre-deployment preparations. These friendly force indicators should be collected and analyzed during routine garrison operations, field training, and actual missions.

a. Information Requirements

Information requirements for deception operations are complex, but not overwhelming. "In developing such [deception] plans the commander must visualize and understand the enemy viewpoint…."[225] As *TC 30-1* states:

---

[223] Joint Staff, *JP 3-13.4*, IV-4 to IV-14.

[224] This discussion is not meant to prescribe the way to plan and execute deception operations; rather, this section is meant as a discussion of the broad concepts associated with planning and execution.

[225] Headquarters, Department of the Army, *FM 100-5: 1962*, 50.

> Success of cover and deception is dependent on the ability of the deceiver to predict the probable enemy reaction. The staff charged with the deception planning must be able to think as the enemy does and not react as a friendly commander transplanted into the enemy situation. This is possible only as a result of a thorough understanding of the enemy, his culture, and military system. The enemy intelligence system must be evaluated because this system is the vehicle that carries the deception story to the enemy commander. Determination must be made regarding the enemy's characteristics, his habits that make him vulnerable to deception, and those aspects that present the least likely deception target. …if possible, we should know the characteristics of the enemy commander, to include the degree of freedom allowed subordinates, his reaction time to new situations, and how this fear of the unknown influences his actions. A single known characteristic of a commander is more important than the entire statistical record of his military career.[226]

Note, while *TC 30-1* talks in terms of the "enemy commander," it is important to realize when targeting non-hierarchal organizations such as networked non-state actors, the target may not be a "commander;" rather, the target may be someone like a low level leader, key financier, or technician. Additionally, the target may not be an "enemy" at all. As stated previously, enemies, adversaries, neutral parties, and even friendly parties are viable targets of deception, though the risk versus benefit calculations when looking to deceive neutral and friendly parties must be examined closely.

The practitioner must also have knowledge of the channels available for both real and deceptive indicators to reach the target; as well as, what channels are available for the collection of feedback in order to assess the deception operation's effectiveness. The deception practitioner should take every effort reasonable within the constraints of time and resources to develop a full understanding to the target. Fortunately, there are several products generated by others which are useful in the practitioner's analysis (Table 5).

[226] Headquarters, Department of the Army, *Training Circular No. 30-1*, 15

Page 792 of 3957

Element	Product
Intelligence	Intelligence Estimate Intelligence Summaries Intelligence Preparation of the Battlefield Network Link Analysis Counterintelligence Threat Analysis [CITA] High Value Individual Target Packets
Civil Military	ASCOPE Analysis CMO Estimate
Military Information Support	Target Audience Analysis Worksheets [TAAW] MISO Estimate
OPSEC	Critical Information OPSEC Indicators
Chaplain	Religious Assessment
Interagency	Country Studies Key Leader Profiles
Commercial Databases	Open Source Information

Table 5. Sample Deception Planning Resources

Not only must the practitioner understand multiple targets' personal characteristics, organization, and culture, the practitioner must also know his own organization in order to have a firm grasp of the indicators the organization generates, specifically the indicators comprising critical information. Critical information is the set of indicators that if pieced together could reveal the friendly force plans, capabilities, and intentions. The list of critical information should normally be produced by the OPSEC officer. A thorough knowledge of friendly forces is required as well for effective portrayals and simulations. One of the critical tasks for the 23rd Headquarters Special Troops was the reconnaissance of friendly formations. The signals units collected "…an unequalled library of combat [Standard Operating Procedures], [Signal Operating Instructions], and radio peculiarities." Likewise, the 603rd Combat Engineers studied unit "atmospherics" and collected samples of unit patches, command post signs, and bumper markings to facilitate the impersonation of any unit in the 12th Army Group.[227]

The degree to which a practitioner needs to understand his own unit means this requirement cannot wait for a specific mission. Ideally, the practitioner's estimate of the

[227] *Official History of the 23rd Headquarters Special Troops* (Photocopy from National Archives), 9.

Page 793 of 3957

friendly forces should be a continuous process, carried out in garrison, training, and actual operations. For this, military deception planning must also be continually nested with operations security planning. Understanding the myriad indicators an element on the move generates, prior to the start of formal mission planning, allows the military deception planner to implement early in the process the necessary cover plans to mask real indicators and the necessary deception plans to show the required false indicators. Waiting until the beginning of the formal planning process to start will result in delays that could allow the indicators of the real plan to be received by the target before the military deception plan is even implemented.

All the information is compiled into a deception estimate. Drawing from various sources, suggested elements of the deception estimate include:

- Potential target decision makers, to include biographical data and psychological profiles
- Existing preconceptions about friendly plans, capabilities, and intentions
- Target organization for systems of decision-making, information flow, and command and control; as well as, organization structure
- Target intelligence capabilities in order to identify channels
- Target potential plans, capabilities, and intentions
- Friendly force plans, capabilities, and intentions to identifying indicators
- Friendly force critical information
- Friendly force characteristics; such as, unit designations, leaders, insignia[228]

2. Planning Guidance

Deception planning guidance from the commander should focus on the deception goal: what the commander wants the target to do, or not to do. Identification of the deception goal must be accomplished as early as possible in the planning process so that the deception plan has sufficient preparation and execution time to allow the target opportunity to take the desired action prior to the execution of the actual plan.[229]

---

[228] Headquarters, Department of the Army, *Training Circular No. 30-1*; Joint Staff, *JP 3-13.4*; *Official History of the 23rd Headquarters Special Troops.*

[229] Headquarters, Department of the Army, *Training Circular No. 30-1*, 13.

Part of the planning guidance is an analysis of the risks and benefits for the various aspects of deception. Deception should be considered for all operations, and cover aspects always implemented, as FM 100-5 (1954) states: "…deception is a continuing action carried out by all echelons of command in activities such as cover and concealment, individual combat, use of dummy positions and installations, and decoys."[230]

There are situations where active deception may not be appropriate, or where deception should focus on supporting operations security and force protection instead of offensive operations. *Reference Book 31-40* recommends the following questions be considered in order to determine whether active deception should be implemented:

- Is the… situation such that the [target] is susceptible to deception?
- Is there a logical opportunity for deception?
- Are there resources, to include time, available to support the deception?
- Is the [target] likely to react in the desired manner in this situation?[231]

The final decision on when and how to implement deception rests with the commander.

3. Planning Methodology

a. DO

With the deception objective identified, the next step is the development of the deception story. The story should be developed using the SEE—THINK—DO methodology.[232] Backwards planning with this methodology starts with the DO step. This step takes the deception objective and couples it with a specific target. The result is phrased in terms of what the specified target does or does not do—this correlates to the act phase of the OODA decision-making process discussed in Chapter IV. For example, a deception objective might be: "Republican Guard commander keeps his forces in vicinity of Kuwait City." The deception objective must be evaluated in terms of capability, reasonability, and feasibility. If these criteria are not met then the deception objective or

[230] Headquarters, Department of the Army, *FM 100-5: 1954*, 38.

[231] U.S. Army Command and General Staff College, *Reference Book 31-40*, 1-2.

[232] Joint Staff, *JP 3-13.4*, IV-1to IV-2.

target needs to be reassessed. For example, the target of the deception may not have to authority to order the desired action; in this case, the target should be shifted to the individual with the appropriate authority.

b. THINK

The next step of planning the deception story is THINK. During this step, the deception practitioner must determine what perception the target needs to develop in order to cause the desired action. THINK encompasses the orient and decide phases of the OODA decision-making process. A firm understanding of the target's existing perceptions, organizational decision-making processes, and schemata is vital to the success of this phase of planning, as each of these influence the target's decision-making process (Figure 7, Chapter IV). Continuing the previous example, if the Republican Guard commander is a coward then he may need to think U.S. forces do not intend to attack Kuwait City; whereas, if he is not a coward, then he may need to think U.S. forces intend to attack Kuwait City.

c. SEE

The final step in the SEE—THINK—DO methodology is SEE. During this step, the practitioner determines what indicators the target needs to receive in order to develop the desired perception. SEE is the observe phase of the OODA decision-making process. The deception practitioner must know what channels are available for the target to collect indicators. The available channels serve as a limit on the range of deception techniques used to create the desired indicators—it is a waste of resources to craft an indicator the target cannot see. Finishing the previous example, after assessing that the Republican Guard commander is not a coward, it is determined that the channels available are best suited for demonstrations of amphibious training, simulations and portrayals of force build up along the border of Kuwait, and disinformation activities. Paralleling the development of what the target needs to see is the determination of what the target cannot be allowed to see. The indicators which might reveal the actual operation become the focus for covering deceptions to either obscure these indicators via camouflaging actions or by denying the channels capable of conveying the real

Page 796 of 3957

indicators. The set of desired indicators are then woven together to create the deception story. The deception story is the: "scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception."[233]

4. Deception Means

From the list of desired indicators developed during the SEE phase, a series of deception events is developed. Deception events are "deception means executed at a specific time and location in support of a deception operation."[234] The desired indicators are generated by the execution of the deception events. Deception means are the "methods, resources, and techniques that can be used to convey information to the deception target."[235] The number of deception means is effectively limitless and is only constrained by the imagination and resources of the practitioner. Deception means are subdivided into three broad categories: physical, cyber electromagnetic, and administration.

a. Physical

Physical means are those which activate the senses, principally the senses of hearing, vision, and smell. A static display of decoy tanks is an example of a physical deception means, as are smoke screens. Physical deception means include morphological deceptions that alter the physical characteristics of an object; such as, camouflage paint schemes or the frames used to disguise tanks as trucks during World War II.[236]

Physical means also utilize actions and behavior to convey or hide information from the target.[237] Demonstrations and feints are common forms of actions as physical means. Behavior can be used to create the perception of a pattern in order to condition the target to expect this pattern to continue; for example establishing a routine

---

[233] Joint Staff, *JP 3-13.4*, GL-3.

[234] Headquarters, Department of the Army, *Field Manual 1-02*, 1-52.

[235] Headquarters, Department of the Army, *Field Manual 1-02*, 1-52.

[236] Gerwehr and Glenn, *Unweaving the Web*, 39 – 40.

[237] Gerwehr and Glenn, *Unweaving the Web*, 39-40

supply convoy for the purposes of setting an ambush. Alternatively, behavior can be used to prevent the target from perceiving a pattern, such as using night movements to conceal a build up of forces before an assault.

Physical means also include sonic deceptions, as in artillery simulators and loudspeaker systems. It is important to note that not all sonic deceptions need to employ mimicry. One method of sonic deception employed by the 4th Infantry Division in Vietnam was the use of artillery fires to mask the sounds associated with infantry units occupying night positions.[238] Prior to the use of the fires, infantry units risked compromising their location due to the sounds associated with preparing and fortifying the positions. In an urban environment, or other environments not permissive to artillery fires, the sounds of operations on the ground could be masked using helicopter flights or loudspeaker operations in the areas surrounding the activity.

b. Cyber Electromagnetic

Cyber electromagnetic means utilize cyberspace and the electromagnetic spectrum [other than visual] in order to communicate deceptive indicators.[239] Deception activities within cyberspace include the transmission of notional documents as disinformation, portrayals in the form of honeypot systems to bait targets into the cyberspace equivalent of ambushes, and the use of camouflaging programs such as an onion router or proxy server to provide cover for cyberspace activities. Furthermore, overt hacking can be used as a feint in order to distract a systems administrator from other cyber warfare activities.

Deceptions within the electromagnetic spectrum are categorized into three types: manipulative, simulative, and imitative. Manipulative electromagnetic deceptions eliminate existing or convey misleading indicators, as in transmitting misleading information on a network known to be compromised. Simulative electromagnetic

---

[238] Office of the Adjutant General, *Lessons Learned, Headquarters, 4th Infantry Division Artillery* (Washington, DC: Department of the Army, 1969). http://handle.dtic.mil/100.2/AD0505964, http://handle.dtic.mil/100.2/AD0505964.

[239] Cyber electromagnetic means replaces the traditional category of technical means in order to include capabilities that did not exist when the technical means category was created.

Page 798 of 3957

deceptions replicate existing or create notional capabilities, such as using radio operators to create the emissions of a notional unit. Imitative electromagnetic deceptions introduce emissions into the target's own systems; for example, transmitting false GPS coordinates to the target's navigation system.[240]

Targets who make use of electronically disseminated policies and orders offer a rich resource for exploitation. These documents reveal a perfect template of what right looks like, and if they include copies of official signatures provide a valuable source of added credibility. Electronically disseminated notional documents can be used to increase friction within the target organization by forcing verification of every electronically disseminated documents, or by forcing the target organization to drop this method of information distribution altogether.

c. Administrative

Administrative means include organizational methods to convey misleading or hide real indicators. Examples of administrative means include operations security and information security to deny indicators; as well as, Human Intelligence officers' use of agents as channels in support of a ruse. Administrative means also include the creation of misleading documents; such as, doctored photographs, notional orders, or fake identification.

One method for developing notional documents is to use existing documents as the base. This expedites the work, and helps to ensure that the notional document looks like a real document. The exemplar for use of existing documents is the German use of decade-old dossiers on Soviet officers as the basis for deceptive dossiers implicating these officers in anti-Stalin activities.[241]

---

[240] For the types of electromagnetic deceptions see: Headquarters, Department of the Army, *Field Manual 3-13: Information Operations: Doctrine, Tactics, Techniques, and Procedures*, 4-7; For spoofing GPS transponders see: Erica Noane, "Hijacking Satellite Navigation," Massachusetts Institute of Technology, http://www.technologyreview.com/computing/21452/ (accessed February 25, 2012).

[241] Epstein, *Deception: The Invisible War*, 140 – 143.

Page 799 of 3957

5. Execution and Assessment

a. Execution

The deception events needed to generate the desired indicators are incorporated into a time-phased execution matrix in order to create and maintain the desired perception (Table 6). The deception execution matrix should be constructed and centrally controlled by the command exercising control of the overall plan. Additionally, the deception execution matrix must be nested within the overall mission's execution matrix; however, the deception execution matrix must be kept separate to ensure security.

Task #	Date-Time	Objective	Action	Unit	Termination	Remarks
1	Not later than 0001 5 Jan 1991	Demonstrate preparations for amphibious operations	Conduct amphibious assault training event	2nd Marine Expeditionary Force	Not earlier than 28 February 1991	Coordinate for press coverage of training
2	Not later than 0001 5 Jan 1991	Iraqi forces focus defensive preparations against attack from Southeast	Conduct training operations against replicas of Iraqi fortifications	1st Cavalry Division 2nd Armored Division 2nd Marine Expeditionary Force	Not earlier than 28 February 1991	Coordinate for press coverage of training
3	Not earlier than 0001 17 Jan 1991	Cover movement of XVIII Corps in preparation for 'Hail Mary'	Camouflage movement of XVIII Corps elements through radio silence	XVIII Corps	On order	
3	Not earlier than 0001 17 Jan 1991	Cover movement of XVIII Corps in preparation for 'Hail Mary'	Conduct radio traffic mimicking XVIII Corps elements in assembly area	XX Signal Battalion	On order	
4	Not earlier than 0001 13 Feb 1991	Iraqi forces remain in defensive positions	Conduct feints and probing attacks against Iraqi lines in tri-border area	1st Cavalry Division VII Corps Artillery	On order	
5	Not earlier than H-3	Draw Iraqi attention to Kuwaiti coast	Conduct simulation of amphibious operations	Seal Team Mimke	Not later than H+1	

Table 6. Notional Execution Matrix Based on Events of Operation DESERT STORM[242]

Emphasis on attention to detail during execution is critical to crafting a believable story. In an after action review of Operation ELEPHANT during World War II, a member of the 23rd Headquarters Special Troops lambasted the "bad theatre" of the operation. The mission was to portray the 2nd Armor Division so that the actual division

[242] Daniel Breitenbach, "Operation Desert Deception: Operational Deception in the Ground Campaign," (Paper, Naval War College, 1991), accessed 24 May 2012, http://handle.dtic.mil/100.2/ADA253245. The date-time information in the table is notional for the purposes of presenting a complete matrix.

Page 800 of 3957

could move to the front lines unmolested. Personnel were instructed to inflate the decoy tanks and then go to sleep with no thought of portraying the activities normally seen in a tank unit. Also, the personnel of the 23rd did not wear the patches of the 2nd Armor Division units, nor were the decoys painted with the appropriate bumper numbers. These shortcomings, taken with the blatant disregard of the 2nd Armor Division for operations security during its move, resulted in a very weak ruse.[243] It is paramount that attention to details be observed during deception operations, as a weak deception execution can result in the target recognizing the deception and exploiting it in turn.

b. Assessment

One problem with accessing deception effectiveness is that some assessments would have to rely on counterfactual information. A comment from *Secret Soldiers* sums up this dilemma: "How many American and British fighting men didn't die because, instead of striking the Allied line at a vulnerable point, the Germans discovered a regiment of dummy tanks concealed—but not too well—in the Normandy woods and pulled back instead? How many Old Hickories survived the push across the Rhine because the Germans were preparing to meet the attack thirty miles away, where the Special Troops were sending up their racket on heaters [loud speakers] and radios and massing their decoys with the help of stagecraft and impersonation?"[244]

This is not to say measures of effectiveness are not necessary; rather, measures of effectiveness should be tied to observable indicators that will reveal whether the target is acting on the deception. For example, in the case of a feint, a measure of effectiveness might be the target moving his reserves to support his lines at the point of the feint. In the case of deception for subversion, a measure of effectiveness might be reports of red-on-red violence, defections, or an increase in absenteeism with in the targeted organization. Measures of effectiveness are turned into intelligence requirements for collection.

---

[243] Gerard, *Secret Soldiers*, 153 – 156.

[244] Gerard, *Secret Soldiers*, 334.

Collecting for deception requires a witting actor on the unit's intelligence staff. This actor serves several functions. First, the individual helps to ensure any information requirements for the deception plan are included in the unit's overall collection plan. Second, as information comes into the intelligence section for processing, the witting actor looks for indicators that show the target is accepting or rejecting the deception. Care must be exercised when looking for indicators that the deception is working as this can activate the confirmation bias, causing indicators to the negative to be overlooked and ambiguous indicators to be interpreted as positive. Finally, the actor must work to ensure the deception indicators do not corrupt the friendly force's understanding of the situation.

6. Termination

At some point a deception operation will lose its utility; therefore, deception operations need to have a plan for the termination of the deception. JP 3-13.4 provides a list of possible termination triggers (Table 7). The termination plan should detail the steps taken to dismantle the deception, e.g., the release of units from a feint or demonstration and cessation of portrayal radio traffic. It is important to note that the termination plan should not be set in stone; as the mission progresses, there may be unforeseen opportunities to leverage the deceptions past the original objective. For example, Operation FORTITUDE SOUTH remained effective past D-Day with the First U.S. Army Group being "transferred" to France in order to maintain pressure on German forces; the last parts of FORTITUDE SOUTH were not terminated until early September 1944.[245]

[245] Roger Hesketh, *Fortitude: The D-Day Deception Campaign*, (Woodstock and New York, NY: The Overlook Press, 2000), 289 – 302.

Page 802 of 3957

Trigger	Description
Successful deception operation	The deception objective has been achieved its objectives, or run its course
Change in mission	The mission which the deception supports changes to a degree the deception no longer has utility
Recalculated risk or probability of success	Some element of the deception estimate changes such that the risks or costs to friendly forces are no longer acceptable
Poor timing	Deception is proceeding too slowly, or the window of opportunity has closed
New opportunity	Circumstances change where deception may be less risky or more effective if deception efforts are realigned
Deception compromise	There is cause to believe the target is aware of at least some aspects of the deception plan

Table 7. Potential Termination Triggers[246]

B. PRINCIPLES OF DECEPTION

In addition to the detailed planning processes, a number of authors have published sets of deception principles, factors, and maxims. *FM 100-5* (1954) and *FM 3-13* each present their own doctrinal set of principles. The CIA's maxims from *Deception Maxims: Fact and Folklore* are included in slightly altered form in *FM 90-2* (1988) and *JP 3-13.4* (2006). Michael Dewar, Jon Latimer, and Jock Haswell each offer their own take on deception principles; though there is a good deal of overlap. Finally, Daniel and Herbig provide a set of deception success factors; while Dudley Clarke muses on deception reflections. From these various sets of deception guidance, it is possible to synthesize seven broad principles for deception practitioners[247] (Table 8).

[246] Joint Staff, *JP 3-13.4*, IV-13.

[247] Daniel and Herbig acknowledge the strategic initiative factor is more of an observation than a controllable factor for the deception practitioner; therefore, this factor is not included as a principle in the composite list. Daniel and Herbig, "Propositions on Military Deception," 24 – 25.

***FM 100-5* (1954) Fundamentals**	**CIA Maxims**	***FM 3-13* Principles**	**Michael Dewar Principles**	**Jon Latimer Principles**	**Jock Haswell Principles**	**Daniel and Herbig Factors**	**Dudley Clarke Reflections**	**Synthesized Deception Principles**
must be executed in a realistic and natural manner and must fit logically into the overall situation	Magruder's principles Limitations to human information processing Care in the design and placement of deceptive material	Focus on the target Exploit target biases Avoid windfalls	Be what the enemy expects	Credibility and confirmation Focus	Credibility	Plausibility and confirmation of the lie Target Predispositions	Support the enemy's false notions Personal knowledge of the enemy is an asset	Know the target and exploit existing perceptions
must be supported by and coordinated with intelligence countermeasures to conceal our activities from the enemy.		Enforce strict OPSEC	Security	Security	Security	Secrecy, Organization, and Coordination		Security is Paramount
The method or means of deception should be constantly varied.	The multiple forms of surprise Jones' dilemma	Employ variety Minimize falsehood/ leverage truth	Use many channels for indicators	Flexibility	Flexibility Multi-channel support	Adaptability of deception		Utilize Flexibility, Variety, and Conditioning
Combat deception is a continuing action carried out by all echelons of command in activities such as cover and concealment, individual combat, use of dummy positions and installations, and decoys		Centralize control	Centralized coordination and control	Coordination and centralized control	Coordination and centralized control		Deception planner needs direct access to leadership	Coordination and Control
must be reasonably certain of causing the enemy to discard certain capabilities which are unfavorable to the success of our plan		Cause the target to act		Action			Deception plan must focus on what the enemy is to "do" not what the enemy is to "think"	Requirement for Target Action
must support and be based upon the main tactical plan. if successful, must further the real plan and if unsuccessful must not jeopardize the real plan. Enemy intelligence must be given the opportunities and time to develop the deception picture which has been planned Deception is effective only for a limited period of time.	Axelrod's contribution A sequencing rule The importance of feedback	Ensure integration Ensure timeliness Utilize space effectively Work within available competencies and resources	Sound and thorough preparation Timing is crucial	Preparation and timing	Preparation		Deception is an operations function Deception requires extensive intelligence support Building a false order of battle is essential	Preparation and Timing
may produce a surprise reaction contrary to the planner's expectations.	The monkey's paw							Beware Unexpected Consequences
						Strategic initiative		The Offense Offers Better Opportunity for Deception

Table 8. Deception Fundamentals, Principles, and Maxims[248]

[248] Headquarters, Department of the Army, *Field Manual 100-5: Field Service Regulations—Operations, 1954*, 37 – 38; Deception Research Program, *Deception Maxims: Fact and Folklore* (Washington, DC: Office of Research and Development, Central Intelligence Agency, 1980). Variations included in Headquarters, Department of the Army, *Field Manual 90-2: Battlefield Deception*, 1-3 and Joint Staff, *JP 3-13.4: Military Deception*, A1-A2; Headquarters, Department of the Army, *Field Manual 3-13: Information Operations: Doctrine, Tactics, Techniques, and Procedures*, 4-4; Dewar, *The Art of Military Deception in Warfare*, 14 – 15; Jon Latimer, *Deception in War* (New York: The Overlook Press, 2001), 60 – 70; Haswell, *The Tangled Web: The Art of Tactical and Strategic Deception*, 39 – 41; Daniel and Herbig, *Propositions on Military Deception*, 16 – 25; Dudley Clarke, 6 September 1972, "Some Personal Reflections on the Practice of Deception in the Mediterranean Theatre from 1941 to 1945," memorandum included in Mure, *Master of Deception: Tangled Webs in London and the Middle East*, 273 – 275.

1. Know the Target and Exploit Existing Perceptions

a. Understand the Target

Knowing the target is essential to successful deception as every target is unique. British deception efforts in the Pacific during World War II had to be significantly modified from the model of deception operations in North Africa and Europe; the Japanese commanders did not trust their intelligence staff like the German commanders did.[249] Every reasonable effort should be taken to develop an understanding of the target's personal, organizational, and cultural schemata; as well as, to identify any existing perceptions.

b. Exploit Existing Perceptions

Deception can be used to both reinforce the target's existing perceptions and to change the perceptions. Whenever possible, deceptions should seek to leverage existing perceptions as is the far easier of the two endeavors. The anchoring bias discussed in Chapter IV works against changing perception, as do several other cognitive biases. The idea of using the target's existing perceptions and beliefs is a common admonishment in deception writings, as shown in Table 8. The Magruder Principle from the set of deception maxims compiled by in the CIA's *Deception Maxims: Fact and Folklore* states: "It is generally easier to induce an opponent to maintain a preexisting belief than to present notional evidence to change that belief. Thus, it may be more fruitful to examine how an opponent's existing beliefs can be turned to advantage than to attempt to alter these views."[250] Reinforcing existing perceptions also leverages confirmation bias as discussed in Chapter IV. Operation FORTITUDE SOUTH during World War II is an exemplar of using deception to reinforce the target's existing perceptions. In this case, the German command expected the inevitable invasion of Europe would come at the Pas de Calais.

This principle is not a hard and fast rule; operational necessity may require changing the target's existing perceptions, as was the case with General Pershing and the

[249] Clarke, "Some Personal Reflections," 273 – 274.

[250] Deception Research Program, *Deception Maxims: Fact and Folklore*, 5.

reduction of the St. Mihiel salient during World War I. German forces expected General Pershing to attack where he intended to attack. General Pershing used a convincing demonstration supported by several pieces of disinformation to convince the Germans the attack would come elsewhere. As a result, the German's shifted forces away from the point of decision, facilitating General Pershing's success.[251]

c. Avoiding Windfalls

While the deception practitioner wants the target to receive the deception indicators, care must be taken that the deception indicators are not too easily presented to the target. Given how difficult intelligence collection can be, there is a natural tendency to be suspicious of information too freely gained. *FM 3-13* offers two methods to reduce target suspicion of windfalls. "The first is the unintentional mistake, designed to make the target believe that he obtained the indicator due to a friendly error or oversight."[252] An example of an unintentional mistake ruse occurred during deception operations in support of the American Expeditionary Force's assault on the Saint Mihiel salient during World War I; General Pershing's chief of staff left a crumpled sheet of carbon paper with the imprint of a disinformation laden memo in the wastebasket of his hotel room, knowing the German agents on the hotel staff would find the carbon paper.[253]

The second method of reducing suspicion of deception indicators is bad luck, which is designed to make the target believe the information was obtained "because the source fell victim to uncontrollable circumstances."[254] Though now considered apocryphal, Meinertzhagen's haversack ruse is still a good example of how this method can be employed.[255] In order to deceive Turkish forces of British intent to capture Beershaba, Meinertzhagen developed a notional set of documents indicating the focus of

---

[251] See Chapter VI for a detailed account of the deception in support of the St. Mihiel operation.

[252] Headquarters, Department of the Army, *FM 3-13*, 4-10.

[253] The Editors of the Army Times, *The Tangled Web*, 71.

[254] Headquarters, Department of the Army, *FM 3-13*, 4-10.

[255] Meinertzhagen has been accused of fraudulently taking credit for both the idea and execution of the haversack ruse. See: Brian Garfield, *The Meinertzhagen Mystery: The Life and Legend of a Colossal Fraud*

British efforts was the capture of Gaza, not Beershaba. Next, Meinertzhagen rode toward Turkish lines until he made contact with a Turkish patrol. Once the Turkish patrol began pursuit, Meinertzhagen fled, and in his haste lost his haversack containing the notional documents. Meinertzhagen took pains to increase the legitimacy of the lost haversack. First, Meinertzhagen spattered his haversack with blood so it appeared he had been wounded during the encounter. Second, in the days after the encounter, numerous British patrols were observed scouring the site of the encounter as if searching for the missing haversack.[256]

2. Security is Paramount

Maintenance of security is vital to a successful deception operation. Failure to properly secure the deception plan can result in leaked indicators that tip the hand to the target. If this occurs, there is a significant risk that the target will in turn deceive the practitioner, turning the tables. Hesketh states in the conclusion of his work that one of the cases against physical deception is the necessity to let too many people in on the secret, increasing security risks.[257] Similarly, von Greiffenberg admonishes: "If the strictest secrecy is not observed all deception projects—even the smallest—are doomed to failure from the very start."[258]

However, security must be balanced with the need for coordination, as too much security can undermine the coordination necessary for the deception to succeed. This is exemplified by British raid at Saint-Nazaire. The British Air Force was tasked with conducting a bombing mission on Saint-Nazaire as a feint to distract the German forces from the raiding force; however, the bomber crews were not told of the reason for their mission, so when low clouds obscured the target, the mission was called off with minimal bombing conducted. The short bombing mission put German forces on alert, rather than

[256] John Ferris, "'FORTITUDE' in Context: The Evolution of British Military Deception in Two World Wars, 1914-1945," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, Richard K. Betts, and Thomas G. Mahnken, eds. (London: Frank Cass, 2003), 120.

[257] Hesketh, *Fortitude*, 353.

[258] Hans von Greiffenberg, *Deception and Cover Plans Project #29*, ed. Harald Kehm, trans. J. B. Robinson (Koenigstein, Germany?: Foreign Military Studies Branch, 1950), 81.

the intended effect of providing cover for the raid force. In the after action review, the bombing crews were adamant that had they known the true purpose of the bombing mission, they would have not have cut the mission short.[259]

3. Utilize Flexibility, Variety, and Conditioning

a. Flexibility

Deceptions must be flexible and the practitioner ready to revise and adapt the plan based on feedback from the target. For example, Operation FORTITUDE SOUTH was expected to be terminated shortly after the Normandy landings as the landings would betray the Allies true intentions. However, in order to keep the German Fifteenth Army from assaulting the Normandy beachhead from its position in the Pas de Calais region, the Allies decided to adapt and continue OPERATION FORTITUDE SOUTH's fiction that the Allies still had the capability to attack Pas de Calais. The modified deception plan became Operation FORTITUDE SOUTH II, and succeeded in keeping the Fifteenth Army in place.[260]

b. Variety

Deceptions should employ variety, both in terms of indicators and channels in order to increase the likelihood of the deception story reaching the target. Reliance on a limited indicators or channels risks the indicator not being received by the target. This can occur either due to noise disrupting the indictor, or if the target is not monitoring the channel when the indicator is transmitted. The number of indicators and channels needed is dependent on the practitioner's knowledge of the target. While it is possible for a single indicator and channel to be used if the practitioner has direct access to the target; such as, General Nathan Bedford Forrest's' portrayal of additional troops during a parley with a Union stronghold's commander. However, in general practice, there should be multiple indicators and channels. For example, in support of Operation

[259] McRaven, *Spec Ops*, 131 and 154.

[260] Hesketh, *Fortitude*, 241.

FORTITUDE SOUTH, the Allies used a number of indicators and channels to include: several agents of the DOUBLE CROSS system, decoys and dummies to simulate units, radio teams to portray units, and disinformation.

c. Conditioning

Conditioning, also referred to in literature as "crying wolf," is a deception technique that relies on desensitizing the target to friendly actions. Conditioning seeks to create three misconceptions in the target's mind. First, friendly activities are following a routine. Second, the routine is set, with deviation unlikely. Third, because the friendly activities are following a set routine, the risk to the target is reduced.[261] The quintessential example of conditioning is the Egyptian preparations leading up to the 1973 Yom Kippur War. The Egyptian Army undertook a series of training exercises on its side of the Suez Canal, establishing a pattern of behavior. The staging of forces for the war followed the pattern of the training exercises, lulling Israeli intelligence into a false sense of understanding.

Stonewall Jackson provides an additional exemplar for conditioning the target. Early in the Civil War, the Baltimore and Ohio Railroad had been allowed to maintain its East-West line between Washington and the West, despite a portion of the line crossing through Virginia. Jackson, while serving as commander at Harper's Ferry, complained that the trains disrupted his men's sleep and requested all east bound trains run between 11pm and 1am. The railroad company complied in an effort to maintain good will. After a while, Jackson requested all west bound trains run at the same time as the east bound trains; again the railroad complied. Once the schedule was up and running, Jackson used his detachments at Point of Rocks and Martinsburg to trap all the rolling stock between them. The trains were then diverted to the south for use by the Confederacy.[262]

---

[261] Gerwehr and Glenn, *The Art of Darkness: Deception and Urban Operations*, 21.

[262] G. F. R. Henderson, and Garnet Wolseley, *Stonewall Jackson and the American Civil War* (London, New York [etc.]: Longmans, Green and Co., 1936), 1:121 – 122.

4. Coordination and Control

a. Control

Control of deception planning and execution should reside at the lowest echelon capable of executing the plan. For example, an infantry platoon conducting the camouflage aspects of cover should maintain control of the plan at the platoon level. Control of deception plans requiring external support, e.g., airborne jamming, should be controlled at the level capable of coordinating for the support. This allows for von Greiffenberg's guidance that: "One responsible agency issues the order, assigns what equipment may be necessary, and supervises the course of the operation as a whole."[263] At the same time, the commander overseeing the deception operation must "make one individual responsible for overseeing a [deception] operation."[264] Having too many people "in charge" results in no one being in charge.

b. Coordination

Coordination for a deception plan must be made with adjacent units and higher headquarters so that deceptive indictors do not contaminate the other units' intelligence collection efforts. Additionally, coordination helps to ensure the deception plan nests with and compliments higher and adjacent unit plans, and does not conflict or degrade these plans. An example of poor coordinate occurred during the assault on the German garrison at Brest during the summer of 1944; the 23rd Headquarters Special Troops executed a sonic simulation of tank activity to distract the Germans from the main effort. Through a lapse of coordination, Company D, 709th Tank Battalion assaulted through the area the 23rd had been conducting its simulation; as a result, the German line, alert and reinforced thanks to the deception, decimated the company.[265]

---

[263] Von Greiffenberg, *Deception and Cover Plans*, 80.

[264] Headquarters, Department of the Army, *FM 3-13*, 4-16.

[265] Gerard, *Secret Soldiers*, 183 – 184.

5. Requirement for Target Action

For deception to succeed, the target must execute the desired action or inaction; to merely change the target's perception is to waste time and resources. This requirement demands the deception practitioner never lose sight of the deception goal. As Dudley Clarke declares:

> It is important to appreciate from the start that the only purpose of Deception is to make one's opponent ACT in a manner calculated to assist one's own plans and to prejudice the success of his. In other words, to make him *do* something. Too often in the past we have set out to make him THINK something, without realizing that this was no more than a means to an end. Fundamentally it does not matter in the least what the enemy thinks; it is only what line of action he adopts as a consequence of his line of thought that will affect the battle. As a result we resolved the principle that a commander should tell his Deception staff what he wants the enemy to DO… while it is the duty of the latter to decide, in consultation with the Intelligence Staff, what he should be made to THINK in order to induce him to adopt the required course of action.[266]

6. Preparation and Timing

As German General Hans von Greiffenberg states in his survey of German deception during World War II: "Deception requires detailed preparation, in which details and seeming trifles cannot be overlooked. Only seldom will results be produced through improvisation."[267]

Adequate resources must be balanced with economy of force. Economy of force dictates that the minimum resources necessary to secondary tasks in order to maximize forces available for the main effort. Too many resources diverted to secondary efforts may leave insufficient forces for the main effort; conversely, too few resources allocated in support of deception can lead to failure. For example, one of the reasons for the failure of Operation COCKADE was insufficient forces in support of the deception. Operation COCKADE was an Allied deception designed to conceal the weakness of Allied Forces in Britain, and to discourage Germany from transferring forces out of Western Europe to the

[266] Dudley Clarke as quoted in Michael Howard, *British Intelligence in the Second World War: Strategic Deception*, vol. 5 (New York: Cambridge University Press, 1990), 41.

[267] Von Greiffenberg, *Deception and Cover Plans*, 80.

Eastern Front.[268] The plan required significant resources for execution, but the supporting commands successfully resisted tasking efforts, resulting in an ultimately unconvincing deception.[269]

With regards to timing, two adversaries arrive at the same conclusion. Von Greiffenberg states: "The enemy intelligence must be given opportunities to develop the picture which has been arranged."[270] While on the Allied side, Clarke states: "Every Deception Plan must be given time to work. It is no good telling a Deception Staff to try and influence an enemy 'at once.'"[271]

7. Beware Unintended Consequences

As with any operation, a deception can cause unintended consequences. These consequences can vary from insignificant to potentially catastrophic. "Under certain circumstances deceptions can produce effects exactly opposite to the planned objective. It is therefore advisable to reflect how such a reversal can be detected in time."[272] The famous example of a reversal was Dudley Clarke's deception of the Italian force in Abyssinia; rather than reinforcing the southern flank as intended, the Italian force withdrew to the north, directly into the intended path of the actual attack.[273]

Operation Desert Storm experienced unintended consequences of the deception operations as a result of the deception being perhaps too successful. The threat of an amphibious assault caused the Iraqi forces to pull their defenses forty kilometers north of the southern Kuwaiti border in an attempt to prevent any amphibious assault from flanking the lines. The lack of resistance in southeastern Kuwait allowed coalition forces operating in this area to rapidly outpace other elements in the attack. This caused the synchronization of coalition efforts to be disrupted; some initiative was sacrificed as units

---

[268] Deception Research Program, *Deception Failures, Non-Failures, and Why* (Washington, DC: Office of Research and Development, Central Intelligence Agency, 1982), 25.

[269] Charles Cruickshank, *Deception in World War II* (London: Book Club Associates, 1979), 61 – 84.

[270] Von Greiffenberg, *Deception and Cover Plans*, 81.

[271] Dudley Clarke as quoted in Howard, *British Intelligence*, 41.

[272] Von Greiffenberg, *Deception and Cover*, 82.

[273] Clarke, "Some Personal Reflections," 273.

were held back in an effort to regain synchronization. Additionally, the amphibious demonstrations sparked the withdrawal of Iraqi forces more quickly than expected, complicating the destruction of several key Iraqi elements.[274]

C. DECEPTION IN SUPPORT OF IRREGULAR OPERATIONS

History is replete with examples of deception in support of conventional operations; deception can support irregular operations as well. Irregular operations include unconventional warfare, counterinsurgency and foreign internal defense, stability and humanitarian assistance, counterterrorism, and cyber warfare.[275] While theoretically any deception technique can be used in support of any type of operation, certain deception techniques lend themselves to the nature of the various types of irregular operations.

1. Unconventional Warfare

A critical concern for unconventional warfare operations is security, especially during the nascent phases of the campaign when the state holds a distinct force advantage over the movement. Deception is a vital tool for maintaining the security of both the forces working with the guerrilla force and for the guerrilla force as well. Otto Heilbrunn in his work *Partisan Warfare* quotes extensively from an unnamed Vietminh manual on the utility of deception in support of guerrilla operations:

> We must act above all when the enemy, full of self-confidence, is underestimating us. We then order our men to disguise themselves as coolies, as enemy soldiers, as hawkers on their way to the market place. Our disguised fighters must exploit the element of surprise in order to wipe out the enemy in his fort or garrison. This technique requires constant and detailed information; one must be fully informed about the enemy's situation, from the first preparations to the time of execution.[276]

---

[274] Breitenbach, "Operation Desert Deception," 22 – 24.

[275] While cyber warfare and humanitarian assistance are not normally included in the set of irregular warfare, they are included here since they are not conventional operations.

[276] "Guerilla selon l'ecole communiste," *Bulletin Militaire* (Leopoldville: Etat-Major de la Force Publique, 1955) as quoted in Otto Heilbrunn, *Partisan Warfare* (New York: Frederick A. Praeger, 1962), 95. This is perhaps from Vo Nguyen Giap's *People's War, People's Army*.

Page 813 of 3957

The camouflaging aspects of deception would seem to be of particular importance to an unconventional warfare campaign in order to allow the special operations force and the guerrilla force to move amongst the population like Mao's fish.

The adoption of Afghan sartorial and grooming standards by special operations forces elements during the opening phase of Operation ENDURING FREEDOM served two purposes. First, the standards were adopted for the purposes of bridging the cultural divide between the SOF elements and the Northern Alliance forces, reducing the "out-groupness" of the SOF elements and leveraging the influence principle of liking. Second, the sartorial and grooming standards increased security for the SOF elements by serving as a form of blending cover, decreasing the visual signature of the SOF elements by merging them visually with the Northern Alliance forces.

FM 31-21: Guerrilla Warfare and Special Forces Operations suggests another method of deception in support of security:

> False rumors and false information concerning guerilla strength, location, operations, training, and equipment can be disseminated by counterintelligence through clandestine nets. Facts may be distorted intentionally to minimize or exaggerate guerilla' capabilities at any given time. Although such activities are handled within the intelligence section, they must be coordinated with the security section in order to prevent inadvertent violations of security.[277]

In this method, deception can cause the targeted regime to expend resources chasing ghosts, such as MACVSOG creating the perception there were far more agents operating within North Vietnam than actually present.

Finally, deception in support of subversion can be used to introduce friction to the regime's decision-making process through the use of ambiguity increasing measures. Slowing down the adversary's OODA process is as effective as increasing the speed of

[277] Headquarters, Department of the Army, *FM 31-21: Guerrilla Warfare and Special Forces Operations* (Washington, DC: Department of the Army, 1958), 106.

one's own. Sufficient ambiguity increasing active deceptions coupled strong cover deceptions increase friction to the point of inducing mental isolation, with the regime's leadership unable to act.[278]

2. Counterinsurgency/Foreign Internal Defense

Pseudo-operations like those employed by the British in Kenya during the Mau-Mau uprising may be of use in overcoming the information advantage enjoyed by the insurgency through intelligence gathering.[279] For example, a pseudo-operation might be designed to lure in supporters and potential supporters of the targeted group for the purposes of intelligence collection and nuanced influence activities. Care must be exercised with pseudo-operations as they thread a fine line with perfidy, international law stipulates that while combatants may wear enemy uniforms may be worn, combatants are prohibited from fighting in them.[280] The Selous Scouts of Rhodesia crossed the line into perfidy by attacking an insurgent base camp while portraying Mozambique military forces.[281]

In addition to pseudo-operations, other deceptions may work to illuminate the insurgency. For example, disinformation in the form of forged orders inserted into an insurgent network can be used to fix cells of the network in time and space for targeting by directing the cell to attend a meeting. The effectiveness of this approach depends on the nature of the insurgent group; a strict hierarchal structure will be more susceptible than a loose-knit structure. Likewise, disinformation about friendly collection capabilities can be used to canalize network communications onto less secure or fewer channels, facilitating collection efforts, or to protect existing collection capabilities. For example, during World War II, ULTRA was protected at times by attributing the intelligence collected to other means.

---

[278] Boyd, *The Strategic Game*, 47.

[279] See: Kitson, *Gangs and Counter-gangs*.

[280] Marie Anderson and Emily Zukauskas, eds., *Operational Law Handbook: 2008* (Charlottesville, VA: The Judge Advocate General's Legal Center and School, 2008), 23.

[281] Lawrence Cline, *Pseudo Operations and Counterinsurgency: Lessons from Other Countries* (Carlisle, PA: Strategic Studies Institute, 2005), accessed 20 April 2011, http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=607, 12.

Page 815 of 3957

Deception for the purpose of subversion could be used to sow discord amongst the insurgent network. This tactic could be particularly disruptive if the practitioner has a firm understanding of the network and is able to target the individuals serving as links between cells. The British used deception in support of subversion against the Irish Republican Army by creating the perception the IRA was riddled with British agents. The IRA acted on the perception by conducting an internal witch hunt. The resultant purge of misidentified "agents" greatly weakened the organization and allowed the British to reach favorable terms for a ceasefire.[282] Additionally, since there is an inverse ratio between security and efficiency, deception for subversion can be used to cause the target to increase security measures to the point of operational ineffectiveness.[283] Finally, as discussed in the unconventional warfare section, deception in support of subversion and mental isolation can be used to introduce friction in the OODA decision-making process, potentially negating an inherent advantage of networks.

One note of caution, as tempting as the idea might seem, false flag attacks on the populace for the purposes of discrediting the insurgent group are a fundamentally bad idea. The effects on popular support for the host nation government and the U.S. mission would be catastrophic if the true nature of the operation were revealed.

3. Stability Operations / Humanitarian Assistance Operations

Deception operations in support of stability operations and humanitarian assistance operations are probably most appropriate when in support of force protection or operations security. For example, in areas where banditry is a problem, a demonstration convoy might be useful to draw attention away from an actual relief convoy. Blending and disguising aspects of deception may be appropriate if a lower signature is desired. Rules of engagement and political sensitivities may significantly constrain the palette of deception techniques available.

---

[282] Benjamin Higginbotham, "On Deceiving Terrorists" (Master's thesis: Naval Postgraduate School), accessed 4 January 2010, http://handle.dtic.mil/100.2/ADA401353, 3 – 5.

[283] J. Bowyer Bell, "Aspects of the Dragonworld: Covert Communications and the Rebel Ecosystem," *International Journal of Intelligence and Counterintelligence* 3, no. 1 (1989): 17.

Page 816 of 3957

4. Counterterrorism

Benjamin Higginbotham, in his thesis "On Deceiving Terrorists," presents three compelling methods where deception can be used against terrorists and terrorist organizations:

- Create and exploit inefficiencies and weaknesses in the terrorist organization
- Facilitate counter-terrorist operations
- Conceal counter-terrorist capabilities and intentions[284]

Deception in support of subversion as discussed in the previous section on counterinsurgency is equally applicable against terrorist groups, and could prove quite useful at creating and exploiting internal inefficiencies and weaknesses of terrorist groups. For example, disinformation spread via rumors that there is an informant within the terrorist group could be spread in areas where the terrorist are suspected of operating in order to sow dissension. Alternatively, if previous purges have occurred, a disinformation program that suggests the group leadership is planning another purge could be used to increase distrust of the leadership, and perhaps an internal preemptive strike against the leaders.

Deception can facilitate counter-terrorist operations by creating surprise. In the Israeli raid on Entebbe, deception in the forms of portrayal and masking played a critical role in achieving surprise and retaining initiative. First, the Israeli aircraft masked their approach behind the signature of a regularly scheduled aircraft. Additionally, the Israeli commando force portrayed Ugandan military forces through the use of Ugandan uniforms and a Mercedes disguised to look like a Ugandan staff car. These techniques sowed confusion amongst the terrorists and their Ugandan guards, with the terrorists initially believing the Ugandans had turned on them.[285]

---

[284] Higginbotham, "On Deceiving Terrorists," 25 – 26.

[285] McRaven, *Spec Ops*, 341 – 376.

5. Cyberwarfare

Cyberspace as an emerging arena for military operations presents as many opportunities for deception as the physical world. For example, honeypots can be used to mislead the target for the purpose of intelligence gathering. Disinformation in the form of spoofed emails could be used to prompt any manner of actions by the target. Pseudo-operations in the form of websites portraying adversary websites can be used for disinformation, intelligence gathering, or influence operations. On the defense, ambiguity increasing deception can be used to protect sensitive information—e.g., operations plans, personnel rosters, or technical data—through the use of multiple files where only one is the true information

D. MILITARY DECEPTION FAILURES

Finally, no discussion of the practice of deception is complete without addressing deception failures. Somewhat optimistically, the CIA report, *Deception Failures, Non-Failures, and Why*, states the following with regard to deception failures: "It can accurately be stated that deception nearly always succeeds, at least to some degree. Indeed it should be emphasized that deception may succeed even when one or more … causes for failure is present."[286] Despite this assertion, the report provides eleven reasons why a deception may fail. These reasons were derived from an analysis of Allied and Axis deception failures during World War II:

- Detection by the intended victim
- Incomplete or incorrect understanding of the target's intelligence apparatus
- Incomplete or incorrect modeling of the deception process
- Inadequate or improper channels or vehicles to convey the deception story
- Incomplete or inadequate control over the significant variables of the deception process
- Incorrect assessment of the target's reaction
- Deception story falls outside the deception window, e. g., too sophisticated to be received or too simplistic to be believed

[286] Deception Research Program, *Deception Failures, Non-Failures, and Why*, 45 – 46.

Page 818 of 3957

- Unreasonable expected result
- Target unable to react in the intended manner even if deception considered credible
- Inadequate time for the deception process to run its course
- Bad luck[287]

With the exception of bad luck, each of these failures represents a shortcoming in the planning and/or execution of the deception plan. For example, "detection by the intended victim" can be caused by failure to properly cover the indicators of the true operation, by a poor deception story, or by shoddy execution of the deception tasks. Likewise, "inadequate or improper channels or vehicles to convey the deception story" represents a failure to either assess the channels available the target, or a failure to revise the plan after discovering the channels were insufficient. While no deception plan is perfect, proper adherence to the information requirements and principles laid out in this chapter can reduce the risk of deception failures.

[287] Deception Research Program, *Deception Failures*, 3 – 4.

Page 819 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 820 of 3957

VI. HISTORIC U.S. ARMY USE OF DECEPTION

Always mystify, mislead, and surprise the enemy.

– General Thomas "Stonewall" Jackson[288]

This chapter surveys the use of deception by the U.S. military from the Revolutionary War to Operation DESERT STORM. The purpose of this chapter is twofold; first to present additional examples of deception in action as prompts for the deception practitioner's creative processes, and second to reinforce the idea that deception has been of great utility for the U.S. military throughout its history.

A. REVOLUTIONARY WAR – BATTLE OF TRENTON

January 2, 1777 saw George Washington trapped against the banks of the Delaware River outside Trenton, New Jersey by a superior British force under General Cornwallis. Despite suggestions to attack straight away, Cornwallis was sufficiently satisfied that Washington was trapped and so waited to attack the next day. The British set camp inside Trenton. During the night, the American force built large bonfires of cedar rails along their lines and continued through the night working to reinforce the earthworks. British sentries could see movement and hear the sounds of the digging. Sporadic cannon fire from the American lines kept the British in Trenton jumpy. When Cornwallis and his men arose the next morning to quash the rebellion all they found was an abandoned camp with piles of fresh dirt and smoldering fires.

The fires and work crews served as demonstrations; and the cannon fire as a feint in order to reinforce Cornwallis's perception that Washington was trapped, and to mask the noise of the American army quietly marching away to attack Princeton. Wagon and cannon wheels were wrapped in cloth to deaden the noise of movement over the frozen ground. A group of 500 stayed behind to work the deception. These men pulled out

[288] General Jackson in a letter to Brigadier John Imboden, as quoted by Imboden, as quoted in: Henderson, *Stonewall Jackson*, 1:420.

Page 821 of 3957

before dawn to rejoin the main body.[289] Security of the plan was so tight that "no one below the rank of brigadier was privy to the plan; officers who were quartered in outlying farmhouses awoke the next morning to find the army gone…."[290]

Deception Objective (DO)	British forces do not impede withdrawal
Deception Target	General Cornwallis
Deception Story (THINK)	American Army preparing for morning battle
Deception Events (SEE)	Demonstration – bon fires Demonstration – men building fortifications Feint – cannon fire Securing – tight security on plan Masking – noise of work obscuring noise of movement
Termination Trigger	Main force withdrawal completed

Table 9. Deception Analysis of Battle of Trenton

B. CIVIL WAR

1. Peninsula Campaign

A classic example of an inferior force using deception to transform certain defeat to a tactical stalemate and strategic victory occurred during the Civil War. Major General Magruder was tasked with preventing the largest Union army yet assembled from reaching Richmond. To achieve this objective, Magruder utilized a number of deceptions, including the use of soldiers portraying deserters to feed General McClellan disinformation exaggerating the size and composition of the Confederate force. The "deserters'" information was confirmed by aerial observation which reported on the troop movements, cavalry, and camp fires carefully choreographed by Magruder. When McClellan approached the Confederate breastworks, he was presented with a now famous simulation—Quaker guns. In order to inflate the number of cannon available to the Confederate force, Magruder had tree trunks stripped, bored, and painted so that they simulated cannon to the casual eye. In McClellan's perception, the Confederate force was larger and better equipped than his, and so McClellan delayed his attack for over a month while he assembled the forces he felt necessary for the attack. This delay allowed ample

[289] Richard M. Ketchum, *The Winter Soldiers*, 1st ed. (Garden City, N.Y: Doubleday, 1973), 344 – 351.

[290] Ketchum, *The Winter Soldiers*, 348

time for the Army of Northern Virginia to place itself between McClellan and Richmond. Additionally, the delay subjected McClellan's force to the bad weather and mosquitos of the peninsula, resulting in many soldiers combat ineffective from illness. When McClellan finally attacked in early May, he found the Quaker guns, but not Magruder. Magruder had used the delay to withdraw his force back to the Army of Northern Virginia lines; Richmond was safe.[291]

Deception Objective (DO)	Union forces do not press attack until after arrival of Army of Northern Virginia
Deception Target	General McClellan
Deception Story (THINK)	Confederate force too large to attack without significant Union reinforcements
Deception Events (SEE)	Simulation – Quaker guns Portrayal – cavalry and infantry units replicating additional units Simulation – additional camp fires
Termination Trigger	Army of Northern Virginia in position

Table 10. Deception Analysis of Peninsula Campaign

2. Capture of Atlanta

During the summer of 1864, Major General Sherman attempted for several months to capture Atlanta, Georgia; however, the city was well fortified and Sherman was unsuccessful in compelling the surrender of the Confederate defenders under General John Hood. Unable to crack the nut that was Atlanta via siege, and unwilling to mount a potentially disastrous frontal assault, Sherman resorted to deception and the indirect approach.

The deception used by Sherman was a feigned withdrawal. Prior to 26 August, Sherman ordered his men be provisioned with 20 days rations, the unit trains reduced to what was absolutely necessary, and all sick and wounded evacuated. Additionally, Sherman cut communications with higher headquarters to reduce the chances of a leak or captured courier.[292] As part of the preparatory movements, Sherman had one brigade of dismounted cavalry from the 2nd Cavalry Division occupy the trenches of the 12th and

[291] The Editors of the Army Times, *The Tangled Web*, 4 – 13.

[292] The Editors of the Army Times, *The Tangled Web*, 15 – 17.

4th Corps in order to prevent the defenders from noticing the corps' movements.[293] After midnight on the 26th, in a move reminiscent of Washington at Trenton, Sherman's force began a near silent withdrawal under the cover of darkness. The withdrawal was not discovered by the Confederate defenders until the next morning. Initial caution transitioned into celebration as the defenders viewed the now empty Union positions strewn with cast off materials. The idea that the Union forces had withdrawn was reinforced by reports of Union cavalry to the west scrounging for rations.[294] The Hood telegraphed Richmond reporting his belief that "…the hungry Union army was giving up the siege and withdrawing across the Chattahoochee."[295] Sherman's forces maintained tight security until seizing Jonesborough, south of Atlanta. By 2 September, Atlanta was in Union hands.[296]

Deception Objective (DO)	Confederate forces fail to react to flanking maneuver
Deception Target	General Hood
Deception Story (THINK)	Union forces have retreated in defeat
Deception Events (SEE)	Portrayal – 2nd Cavalry Division posing as 12th and 4th Corps Demonstration - withdrawal Disinformation – cavalry claim to be short on rations Blending – silence during withdrawal and movement Securing – communications silence
Termination Trigger	Seizure of Jonesborough

Table 11. Deception Analysis of Atlanta

3. Athens, Alabama

In 1864, Nathan Bedford Forrest elicited the surrender of a Union stronghold at Athens, Alabama through the artful use of portrayal. After a short siege of the fort, Forrest arranged a parley with the fort's commander, Colonel Wallace Campbell. During the parley, Campbell was provided with a seemingly impromptu tour of the Confederate camp. Unbeknownst to Campbell, as he completed the tour of a campsite, many of the

[293] William Sherman, *Memoirs of General William T. Sherman*, 2nd ed. (New York: D Appleton and Company, 1904), 2:105; Basil Liddell Hart, *Sherman: Soldier, Realist, American* (New York: Dodd, Mead, and Company, 1929), 296.

[294] The Editors of the Army Times, *The Tangled Web*, 17 – 22.

[295] Liddell Hart, *Sherman*, 298.

[296] The Editors of the Army Times, *The Tangled Web*, 21 – 22.

Confederate infantry from first campsites were portrayed by dismounted cavalry. After Campbell passed, the cavalry remounted and moved to other campsites to be counted again. Artillery pieces were similarly shuffled around, so Campbell was presented the image of a Confederate force four times its actual size. Rather than risk his men against this overwhelming force, Campbell surrendered the fort without further bloodshed.[297] Though Forrest could have reduced the fort through traditional means, the deception both saved lives, and afforded Forrest the freedom of maneuver to turn his force on the Union relief column heading for the fort.

Deception Objective (DO)	Union stronghold surrenders
Deception Target	Colonel Campbell
Deception Story (THINK)	Confederate force is overwhelming, so resistance is futile
Deception Events (SEE)	Portrayal – troops replicating additional forces
Termination Trigger	Surrender by Colonel Campbell

Table 12. Deception Analysis of Athens, Georgia

C. PHILIPPINE INSURRECTION – RAID ON PALANAN

By February 1901, the United States had lost over four thousand Soldiers in two years of combatting insurrection on the Philippines island of Luzon, with no end in sight. The leader of the insurrection was Emilio Aguinaldo. Aguinaldo fought a classic guerrilla campaign, with his troops seemingly everywhere but himself nowhere to be found. On 8 February 1901, a U.S. Army brigade commanded by Colonel Frederick Funston captured one of Aguinaldo's couriers with a message from Aguinaldo which "…ordered insurgent General Lacuna to send 200 soldiers from his brigade to Aguinaldo's headquarters."[298] The courier revealed that the headquarters was located six miles inland at Palanan, in an isolated region of Luzon. As important as the location was the information that there were only 50 rebel troops guarding Aguinaldo.[299] While Funston wanted to act on the

[297] Dunnigan and Nofi, *Victory and Deceit : Dirty Tricks at War*, 124 – 125; John Weyth, *Life of Lieutenant-General Nathan Bedford Forrest* (New York and London: Harper and Brothers Publishers, 1905), 491 – 493.

[298] Barton Whaley, "The One Percent Solution," in *Information Strategy: A Guide to Theory and Practice*, edited by John Arquilla and Douglas Borer, 127 – 159 (New York and London: Routledge, 2007), 151.

[299] Frederick Funston, *Memories of Two Wars* (London: Constable & Co., Limited, 1912) 384 – 389.

information, he knew there was no way for a large American force to reach Aguinaldo's lair without providing enough forewarning to give Aguinaldo opportunity to escape. Funston, not willing to let the opportunity to strike a hard blow to the insurrection, turned to deception.[300] Funston in his memoir states:

> So the only recourse was to work a stratagem, that is, to get to [Aguinaldo] under false colors. It would be so impossible to disguise our own troops that they were not even considered, and dependence would have to be placed on the Macabebes… As it would be absolutely essential to have along some American officers to direct matters and deal with such emergencies as might arise, they were to accompany the expedition as supposed prisoners who had been captured on the march, and were not to throw off that disguise until there was no longer necessity for concealment.[301]

With approval from General MacArthur, Funston ordered 85 Macabebe troops to be outfitted with the weapons and uniforms of the insurgents. Funston and the four American Soldiers accompanying him were dressed as privates and pretended to be prisoners of the disguised Macabebe force. In addition to the disguises, Funston carried several pieces of Lacuna's personal stationary with his forged signature. These would be used to send messages from the insurgent leader to Aguinaldo legitimizing the arrival of the "reinforcements."[302] After a month's training for the Macabebe force, Funston's group set off for Palanan. The pseudo-operation worked exquisitely; when the force arrived in Palanan on March 26th, Aguinaldo was captured with only five casualties—all rebels.[303] The forged letters played an essential role in the ruse with Aguinaldo admitting the letters were key to his letting his guard down and allowing the band into his camp.[304] Shortly after Aguinaldo's capture, he ordered the end of the insurrection. Of the operation, Aguinaldo opined: "It was a bold plan, executed with skill and cleverness, in the face of difficulties which to most men would have seemed insurmountable."[305]

---

[300] The Editors of the Army Times, *The Tangled Web*, 24.

[301] Funston, *Memories of Two Wars*, 393.

[302] The Editors of the Army Times, *The Tangled Web*, 24 – 25.

[303] Bell, *Cheating*, 42 – 43.

[304] Funston, *Memories of Two Wars*, 394.

[305] As quoted in The Editors of the Army Times, *The Tangled Web*, 29.

It's interesting to note that while Funston's deception was a tactical and strategic victory, breaking the back of the insurgency; Funston was pilloried in American press, and even on the Senate floor for committing a war crime. Indeed, but current international law, Funston would be accused of perfidy for allowing the Macabebes to attack while wearing the enemy's uniforms.[306]

Deception Objective (DO)	Allow entry of Funston's force into Aguinaldo's camp
Deception Target	Aguinaldo and rebel forces enroute to camp
Deception Story (THINK)	Funston's force is the requested reinforcements with prisoners
Deception Events (SEE)	Portrayal – Macabebe troops dressed as rebel troops Portrayal – Funston and other Americans as captured privates Disinformation – forged messages
Termination Trigger	On order after arrival into camp

Table 13. Deception Analysis of Raid on Palanan

D. WORLD WAR I – SAINT MIHIEL

While a deception practitioner should seek to leverage existing target perceptions, there are times when this is impossible. For example, when the true objective is already perceived by the adversary to be the objective, reinforcing this perception would be—to say the least—counterproductive. In these cases, deception can be used to change the target's perception. General Pershing's use of deception in support of the assault on the Saint Mihiel salient during World War I demonstrates a successful execution of this scenario.

Pershing saw the reduction of the salient as a necessary step to winning the war; however, the German High Command fully expected an attack by American forces at Saint Mihiel. To increase the prospects of success, Pershing undertook a deception to make the German High Command believe the true focus of the American attack would be the Belfort Gap, 125 miles southeast of Saint Mihiel, with the deception goal of the German High Command shifting resources from Saint Mihiel. On 25 August, 1917, a French liaison officer informed the American press corps—off the record—that the American objective might be further to the South, perhaps the German town of Mulhouse that located on the other side of the Belfort Gap. Not surprisingly, this leak made it by military censors. On 27

[306] The reaction in the U.S. to Funston's operation is discussed in detail in Chapter 3.

August 1917, General Pershing sent Major General Bundy, Commander VI Corps, to the town of Belfort on secret orders to plan for an offensive through the gap. Major General Bundy was an unwitting actor and took to his mission with alacrity. Soon American reconnaissance parties were seen around Belfort marking out locations for supply depots, field hospitals, and artillery positions. To create the impression of troop movements, radio sets from the 91st Infantry Division were used to mimic the transmissions of the VI Corps. The military preparations were reinforced with civil-military operations as pained efforts were made to ensure the local populace had evacuation plans. The crowning piece of disinformation supporting the deception was a piece of carbon paper discarded by Colonel Conger, Pershing's witting actor on the scene, in the waste basket of his hotel room in Belfort. Conger had used to carbon paper for a letter to the American Expeditionary Force Headquarters detailing the Belfort preparations as only needing an execution date. After depositing the carbon in the trash, Conger took a walk, and the German spies on the hotel staff did their part stealing the carbon.

In response to the deception, German High Command moved three divisions from Saint Mihiel to reinforce the Belfort Gap. With German perceptions changed and behavior suitably modified, Pershing's 12 September attack against the Saint Mihiel salient was a success. After the war, Colonel Conger received confirmation from the German commander at Belfort that when he requested the additional divisions he understood the buildup might be a ruse, but could not risk it being real. A deception using a minimum of resources was able to alter the perception of the German High Command in 19 days.[307]

Deception Objective (DO)	German High Command shifts forces from Saint Mihiel
Deception Target	German High Command
Deception Story (THINK)	American Expeditionary Force plans on attacking through the Belfort Gap
Deception Events (SEE)	Demonstration – Major General Bundy Demonstration – reconnaissance parties Disinformation – leak to press Disinformation – Colonel Conger memorandum Portrayal – 91st Division creating radio traffic of VI Corps
Termination Trigger	Execution of attack on Saint Mihiel

Table 14. Deception Analysis of Saint Mihiel

[307] The Editors of the Army Times, *The Tangled Web*, 61 – 75.

Page 828 of 3957

E. DECEPTION IN WORLD WAR II

1. Operation FORTITUDE SOUTH

With an Allied invasion of Western Europe inevitable, the Allies sought to obscure the true landing site—Normandy. Operation FORTITUDE SOUTH sought to convince the Germans the true location of the invasion would be at Pas de Calais so that the German forces located there would not react to the Normandy landings. Fortitude South consisted of two phases. During phase I, the objective was to cause the German forces to make faulty troop dispositions by convincing German High Command that Pas de Calais was the true target for invasion, with a target date of 45 days after the Normandy landings. For phase II, the objective was to cause German High Command to keep the units in Pas de Calais in place. This was to be accomplished by convincing German High Command the Normandy landings were a diversionary feint, and that once the German reserves were committed at Normandy, the true invasion would take place.[308] FORTITUDE SOUTH leveraged the existing German perception that Pas de Calais was the logical invasion choice.

The primary elements of FORTITUDE SOUTH were a simulated command and disinformation transmitted via the DOUBLE CROSS agents. The First U.S. Army Group [FUSAG] was a real headquarters without forces. General Patton was assigned as the FUSAG commander as part of the deception plan. FUSAG simulated and portrayed an army group through the use of decoys, dummies, and tasked units.[309] Many of the simulated units assigned to FUSAG were not created for FUSAG; rather, they were part of a long running effort to inflate the Allied order of battle and had been used in previous deceptions. In addition to the simulated units, a number of real units were notionally assigned to FUSAG, while actually remaining under the command of the 21st Army.[310] Much of the information on the location, composition, and activities of FUSAG was fed to German intelligence through the DOUBLE CROSS system.[311] Additional indicators were

[308] Hesketh, *Fortitude*, 384.

[309] Whaley, *Stratagem* (2007), 376 – 377.

[310] Hesketh, *Fortitude*, 174 – 185.

[311] Hesketh, *Fortitude*, 174 – 185. Agents GARBO and BRUTUS were the primary channels used.

presented by radio nets portraying the notional units. The few German reconnaissance aircraft flying over the FUSAG simulation were fired upon for realism, but intentionally missed so the photos would make it back.[312] As D-Day neared, additional events were staged in support of FORTITUDE SOUTH. Pas de Calais was included in the preparatory bombings to reinforce that it was the target.[313]

After the successful landings at Normandy, FORTITUDE SOUTH was continued into July, until a sequel plan could be executed. The objective of Operation FORTITUDE SOUTH II was "To contain the maximum number of enemy forces in the Pas de Calais area for as long as possible."[314] As elements notionally assigned to FUSAG arrived to reinforce the Normandy beachhead, local German commanders quickly realized the Pas de Calais threat was over; however, FORTITUDE SOUTH II convinced Hitler of the threat, keeping the German Fifteenth Army unable to respond to the growing threat in Normandy.[315] Elements of FORTITUDE SOUTH II remained in effect until the beginning of September.[316]

Deception Objective (DO)	Phase I – German forces commit to faulty troop distributions Phase II – German forces in Pas de Calais do not respond to Normandy landings
Deception Target	Hitler and German High Command
Deception Story (THINK)	Pas de Calais is the primary target of Allied efforts, the Normandy landings are a diversion
Deception Events (SEE)	Simulation – Decoy and dummy equipment Simulation – Radio traffic Portrayal – Assigned units Demonstration – Assignment of Patton as FUSAG Commander Disinformation – plans fed through DOUBLE CROSS agents Feint – Inclusion of Pas de Calais in preparatory bombing
Termination Trigger	Initially successful Normandy landings, extended via sequel

Table 15. Deception Analysis of Operation FORTITUDE SOUTH

[312] The Editors of the Army Times, *The Tangled Web*, 133 – 134.

[313] Whaley, *Stratagem* (2007), 377.

[314] Hesketh, *Fortitude*, 414.

[315] Hesketh, *Fortitude*, 267 – 268.

[316] Hesketh, *Fortitude*, 302.

2. 23rd Headquarters Special Troops

The 23rd Headquarters Special Troops was a purpose built unit specifically intended to conduct deception operations at the tactical level. The unit consisted of a Headquarters and Headquarters Company; the 603rd Engineer Camouflage Battalion (Special); the Signal Company (Special); the 402nd Engineer Combat Company (Special); and the 3132nd Signal Company (Special).[317] The 23rd utilized a variety of means to simulate or portray other army units to include: decoys, dummies, loudspeakers, pyrotechnics, and imitative radio transmissions. Furthermore, the 23rd employed disinformation—the 23rd called this "Special Effects—to corrupt the German perceptions of the Allied Order of Battle. "Special Effects" included the wear of other unit's patches, stenciling vehicles with other unit designations, creating phony generals, and crafting fictional stories; all to be picked up by the German agent networks operating behind Allied lines.[318]

The techniques implemented by the 23rd played a vital role in operations throughout the campaign in Western Europe by depriving German intelligence of the true picture of Allied force dispositions. In particular, the 23rd played a critical role in the relief of Bastogne during the Battle of the Bulge. The objective of Operation KODAK was:

> To confuse German radio intelligence as to the real location of the 80th Infantry Division and the 4th Armored Division, both of which were committed to action in a counterattack against the south flank of the St. Vith-Bastogne salient, by giving radio indication of those Divs in an area to the southeast of that in which they were employed. The area chosen for the radio deception was such as to indicate their presence as a reserve in case of extention [*sic*] of the German counterattack through Echternacht.[319]

The surprise arrival of two divisions of reinforcements broke the back of the siege of Bastogne.[320]

---

[317] *Official History of the 23rd Headquarters Special Troops*, 2 – 3.

[318] *Official History of the 23rd Headquarters Special Troops*, 8 – 9.

[319] *Official History of the 23rd Headquarters Special Troops*, 42.

[320] Gerard, *Secret Soldiers*, 232 – 233.

Deception Objective (DO)	
Deception Target	Field Marshall von Rundstedt – German commander outside Bastogne
Deception Story (THINK)	The 4th Armored Division and 80th Infantry Division were being held in reserve
Deception Events (SEE)	Portrayal – Radio traffic by 23rd Securing – Radio silence by actual units
Termination Trigger	Arrival of the 4th and 80th at Bastogne

Table 16. Deception Analysis of Operation KODAK

3. Operation WEDLOCK

In 1943, Joint Security Control—the staff element of the Joint Chiefs of Staff charged with coordinating U.S. strategic deception—directed Lieutenant General Simon Bolivar Buckner Jr., the commander of the Alaska Department to develop a strategic plan for the North Pacific. The objective given Buckner was:

> …to deceive the Japanese about US plans for Alaska and the Aleutians by exaggerating current American forces and their activities there, and more specifically, to convince the Japanese of a build-up intended to invade the Kurile Islands. Tentatively this fictional assault was first slated for 1 August 1944.[321]

Buckner's initial plan was altered after consultation with Admiral Nimitz. Nimitz assumed command of the strategic aspects of the deception, while Buckner retaining command of the tactical aspects. Nimitz also accelerated the target date for the assault to 15 June so as to provide cover for Operation FORAGER, the planned real assault on Saipan. The revised deception plan became Operation WEDLOCK. In order to present the appearance of increased U.S. preparations for the invasion of the Kurile Islands, WEDLOCK called for the simulated activation of the 9th Amphibious Force consisting of five U.S. and one Canadian division. Additionally, the 9th Fleet would be notionally increased in size in order to support the assault. To create the simulated radio traffic necessary for these formations, a joint communications center was established.[322]

[321] Katherine Herbig, "American Strategic Deception in the Pacific," in *Strategic and Operational Deception in the Second World War*, edited by Michael Handel, 260 – 300, (London: Frank Cass, 1987), 266.

[322] Herbig, "American Strategic Deception," 266 – 267.

In addition to the notional forces, WEDLOCK included a number of other deception events in support of the story. WEDLOCK coopted the American press—ULTRA intercepts confirmed that Japanese intelligence used the press as a means of collection. Rather than keeping the meeting between Buckner and Nimitz a secret, the press was encouraged to report the meeting and speculate on its meaning. In addition, Joint Security Control fed disinformation directly to Japanese intelligence through double agents in the U.S.; via military attaches in neutral countries; and by incorporating disinformation into shared intelligence with Russia—expecting the disinformation to be collected by Japanese agents. Furthermore, troops embarking for the tropics through Seattle were issued artic gear so as to appear that they were heading north. Finally, an entire simulated airbase was constructed at Holtz Bay on the westernmost Aleutian island.[323]

After the invasion of Saipan was completed, it was decided to maintain aspects of the WEDLOCK deception, specifically the simulated divisions. Therefore, a sequel plan was implemented under the name Operation HUSBAND. Operation HUSBAND was later followed by another sequel plan, Operation BAMBINO, which in turn was eventually followed by Operation VALENTINE. Each of the sequel plans maintained the simulated forces, though with less and less effort in maintaining the deception. As a result, the Japanese Imperial Command over time withdrew ships and planes from the Kurile Islands to meet more imminent threats; however, the troop levels remained steady throughout the series of deceptions.[324]

The effect of WEDLOCK can be seen in Japanese troop strengths in the Kurils. Whereas there were initially 25,000 troops and 38 aircraft stationed in the Kurils before WEDLOCK, after WEDLOCK the garrison had grown to 70,000 troops and 590 aircraft.[325] However, while WEDLOCK succeeded in convincing the Japanese of a serious threat from the North:

---

[323] Herbig, "American Strategic Deception," 270 – 272.

[324] Herbig, "American Strategic Deception," 279 – 281.

[325] Milan Vego, *Joint Operational Warfare* (Newport, RI: United States Naval War College, 2007), VII-103 – VII-105, as cited in Leonard Wells, "Military Deception: Equivalent to Intelligence, Maneuver and Fires" (Paper, Navy War College, 2008), accessed 20 May 2012, http://handle.dtic.mil/100.2/ADA494225, 9 – 10.

> …it failed to convince him that this menace was immediate or of primary importance. Rather than misleading the Japanese into reordering their priorities for the threats which faced them, the deception added another plausible threat to an already ambiguous situation.[326]

While not as successful as desired, WEDLOCK could be classified as good enough.

Deception Objective (DO)	Japanese shift forces to defense of Kurile Islands
Deception Target	Japanese Imperial Command
Deception Story (THINK)	U.S. intends to liberate Kurile Islands from Japanese occupation
Deception Events (SEE)	Portrayal – increased size of the 9th Fleet Portrayal – Troops issued artic gear Simulation – radio traffic Simulation – 9th Amphibious Force Disinformation – Press stories Disinformation – Double agent network Disinformation – Military attaches Disinformation – Russia information exchange
Termination Trigger	

Table 17. Deception Analysis of Operation WEDLOCK

F. KOREAN WAR – INCHON LANDING

In 1950, General MacArthur approved Operation CHROMITE, an audacious plan to conduct an amphibious assault at Inchon to break the impasse with North Korean forces to the South. To conduct the operation, General MacArthur directed the formation of X Corps under the command of Major General Edward Almond, General MacArthur's Chief of Staff. As cover for the preparations for Operation CHROMITE, Major General Edward Almond remained as the Chief of Staff, while the staff for X Corps was formed as the Special Planning Staff, and the forces assigned to X Corps were carried as GHQ reserves.[327]

Since it was impossible to camouflage the amphibious assault preparations, a deception plan was needed to mislead the North Korean People's Army [NKPA] command as to the true point of decision. A multi-faceted effort was undertaken to mislead the NKPA command into believing the port city of Kunsan as the actual target so

[326] Herbig, "American Strategic Deception," 275.

[327] *Headquarters X Corps War Diary Summary for Operation Chromite: 15 August to 30 August 1950* (1950), accessed 24 January 2012, http://cgsc.cdmhost.com/utils/getfile/collection/p4013coll11/id/831/filename/832.pdf, 2.

the NKPA would not disrupt the actual landing. Kunsan, located one hundred miles to the south of Inchon, was a likely target for assault—it had been one of the three courses of action during planning. First, Kunsan was given particular attention during the preparatory bombing operations, to include a massive operation four days prior to the Inchon landing. Second, the 1st Marine Division was publicly given briefings on the hydrology at Kunsan. Third, an amphibious feint/portrayal was conducted at Kunsan using an ad hoc special operations element, whose purpose was to create the perception of a much larger force.[328] Additionally, the 1st Marine Brigade, which was the primary landing force at Inchon, was assigned to the Pusan 'general reserve' in an effort to blend it in with other less essential units.[329] In order to add a bit of ambiguity to the situation, similar efforts—preparatory naval bombardments—were made for Samch'ok, a plausible amphibious landing objective on the east coast of the peninsula.[330] The Inchon landing could not have succeeded without the operational surprise created by the deception plan.

Deception Objective (DO)	North Korean forces do not disrupt Inchon landing
Deception Target	North Korean People's Army command
Deception Story (THINK)	Actual amphibious landing will occur at Kunsan or Samch'ok
Deception Events (SEE)	Feint/Portrayal – Special Operations Company landing at Kunsan Feint – Kunsan focus of major bombing attack at D-4 Feint – Samch'ok focus of preparatory naval bombardment Demonstration – public briefing on hydrology at Kunsan Blending – preparatory bombings at Inchon blended into larger bombing operation Blending – assault element assigned to the Pusan 'general reserve' Blending - Major General Almond remaining Chief of Staff
Termination Trigger	

Table 18. Deception Analysis of Operation CHROMITE

[328] Whaley, *Stratagem* (2007), 448.

[329] George Womack, "Operational Deception and the Principles of War" (Paper, Naval War College, 1994), accessed 20 May 2012, http://handle.dtic.mil/100.2/ADA279632, 13.

[330] *Reference Book 31-40: Techniques for Deception*, 6-8.

G. VIETNAM WAR

1. MACVSOG

a. Sacred Sword Patriots League

When MACVSOG was established in 1964, one of the objectives in OPLAN 34A was to "create the impression that an active, unified, internal opposition exists in North Vietnam."[331] OPLAN 34A directed the creation of an impression because MACVSOG was prohibited by policy decisions made in Washington from implementing an actual unconventional warfare campaign in North Vietnam.[332] As a result, MACVSOG implemented a complex deception program to create the perception of a growing and active underground movement with the objective of forcing the North Vietnamese government to withdraw support for the Viet Cong. The notional resistance movement was part of Project HUMIDOR, MACVSOG's psychological operations program.[333] The centerpiece of MACVSOG's plan was the Sacred Sword Patriots League [SSPL]. The SSPL was presented as an anti-foreign power, Vietnamese nationalist party with its roots in the anti-colonial struggles against the French.[334]

The SSPL deception was supported by a number of operations. First, North Vietnamese fishermen captured as part of MACVSOG's maritime operations were taken to

---

[331] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Appendix A Summary of MACSOG Documentation Study* (Washington, DC: Joint Chiefs of Staff, 1970), accessed 2 September 2011, http://www.dod.gov/pubs/foi/International_security_affairs/vietnam_and_southeast_asiaDocuments/520-22.pdf, a-18.

[332] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Annex A to Appendix C Psychological Operations* (Washington, DC: Joint Chiefs of Staff, 1970), accessed 2 September 2011, http://www.dod.gov/pubs/foi/International_security_affairs/vietnam_and_southeast_asiaDocuments/520-1.pdf, C-a-7 to C-a-13. MACVSOG attempted on three separate occasions between 1965 and 1968 to gain approval to execute an actual unconventional warfare plan against North Vietnam.

[333] John Plaster, *SOG: The Secret Wars of America's Commandos in Vietnam* (New York: Penguin Group, 1998), 125.

[334] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Annex A to Appendix C Psychological Operations*, C-a-14 to C-a-15. The sacred sword was a reference to a Vietnamese legend about a heaven-sent sword used by Le Loi during his nationalist campaign to drive the Chinese from Vietnam in the 15th Century. The SSPL story reflects an exceptional attention to detail with regards to the targeted culture. See Shultz, *Secret War*, 139 – 14.

the Paradise Island facility that portrayed an active SSPL camp.[335] While the fishermen were subjected to SSPL indoctrination, the primary objective was not to actually turn the fishermen into operatives; rather:

> The primary objective of capturing prisoners and leading them to believe that they were captives of the SSPL was to establish credibility for the organization and convince elements of the populace of [North Vietnam] that an opposition organization does exist in [North Vietnam].[336]

In addition to the Paradise Island facility, support for the SSPL deception included the Voice of the Sacred Sword Patriots League, a portrayed radio station ran by MACVSOG's psychological operations element, and leaflet drops of SSPL propaganda.[337]

While the SSPL program did not achieve its primary objective of forcing the North Vietnamese government to stop or reduce support for the insurgency in the South, the program was effective at forcing the North Vietnamese government to increase internal security measures. A study of North Vietnam's response to covert operations, concluded that "Hanoi interprets allied special operations in North Vietnam as a major facet in the US strategy. As such it views these operations with considerable alarm."[338] Additionally, the end to all covert activities in North Vietnam was included in the initial 'price for peace' demands by the North Vietnamese contingent at the Paris peace talks.[339] The SSPL program was effectively ended with the 1 April 1968.[340]

---

[335] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Annex A to Appendix C Psychological Operations*, C-a-40.

[336] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Annex A to Appendix C Psychological Operations*, C-a-62.

[337] Shultz, *Secret War*, 142 – 144.

[338] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Annex A to Appendix C Psychological Operations*, C-a-129

[339] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Annex A to Appendix C Psychological Operations*, C-a-110. Additionally, Ho Chi Minh issued several directives aimed specifically at suppressing internal dissent.

[340] Special Assistant for Counterinsurgency and Special Affairs (SACSA), *Draft MACSOG Documentation Study Annex A to Appendix C Psychological Operations*, C-a-40.

Deception Objective (DO)	North Vietnam reduces support to South Vietnamese insurgency
Deception Target	Ho Chi Minh and North Vietnam leadership
Deception Story (THINK)	The SSPL is an active resistance movement challenging the Communist government of North Vietnam
Deception Events (SEE)	Portrayal – Paradise Island operations Disinformation – SSPL radio station and leaflet drops
Termination Trigger	Since deception was in support of the overall campaign there was no defined termination trigger. Termination occurred in response to North Vietnamese negotiation demands.

Table 19. Deception Analysis of SSPL

b. Deception in Support of Security

In addition to the SSPL program, MACVSOG utilized deception in support of a robust organizational security program. As part of the security program, MACVSOG, as well as all the major subordinate components, had an official cover story in an attempt to disguise the true nature of the organization. The official cover story for MACVSOG was:

> Studies and Observations Group (SOG): "Studies and Observations Group is a special staff section of Headquarters, United States Military Assistanct [*sic*] Command, Vietnam (USMACV) under the supervision of the Chief of Staff, USMACV. It is responsible for the study an observation of joint or combined counterinsurgency operations of a comprehensive nature. The studies and observations include intelligence and psychological activities as well as combat actions that may involve any forces or resources of any service of the Republic of Vietnam Armed Forces (RVNAF) and USMACV. SOG is not an implementing agency, the operations it studies and observes are conducted by the RVNAF commands which have responsibility for the areas of observations.[341]

In addition to the overarching cover stories, individual missions were given cover stories. For example, if an aircraft conveying agent teams or equipment between South Vietnam and Thailand had an incident necessitating an explanation for the mission, the explanation was that the aircraft was diverted from routine operations in South Vietnam in order to respond to a distress call.[342]

---

[341] Special Assistant for Counterinsurgency and Special Affairs, *Draft MACSOG Documentation Study Appendix H Security, Cover & Deception*, H-10.

[342] Special Assistant for Counterinsurgency and Special Affairs, *Draft MACSOG Documentation Study Appendix H Security, Cover & Deception*, H-12.

Deception Objective (DO)	Ignore MACVSOG
Deception Target	Everyone without need-to-know
Deception Story (THINK)	MACVSOG is a staff element used to collect data, not an operational headquarters
Deception Events (SEE)	Disinformation – cover stories
Termination Trigger	Since deception was in support of the overall campaign there was no defined termination trigger

Table 20. Deception Analysis of MACVSOG Security

2. MACV

Elements of the Military Assistance Command, Vietnam (MACV) utilized deception in their operations against the Viet Cong and the North Vietnamese Army. In one case, the 25th Infantry Division learned of an inexperienced NVA regiment with orders to seek out an allied base as a way of building experience and morale. At the recommendation of the division staff, the commander of the 25th decided to provide the enemy with a suitable target. In February 1969, an infantry company established firebase DIAMOND I in the vicinity of the enemy force. What the NVA saw as a vulnerable target was in reality ringed with sensors and ground radar systems, and supported by three artillery support bases and air support. When the NVA decided to attack the firebase the sensor array deprived the NVA of surprise. Supported by the artillery bases and air support, the firebase repulsed two attacks with minimal casualties, while the NVA regiment was decimated. This stratagem was repeated by the 25th Infantry Division with at three additional firebases with similar successes. Repetition of the stratagem was achievable because establishing new firebases was a routine occurrence. While using troops as bait may seem distasteful, the stratagem was effective; moreover, by establishing DIAMOND I, the 25th Infantry Division was able to influence the NVA into attacking on the 25th's terms. The alternative would have meant allowing the NVA force to attack any one of a number of bases.[343]

In analyzing this deception, it is interesting to note that the deception was not the force, rather the purpose of the force. As the report noted, had the NVA not acted on the

[343] *Reference Book 31-40: Techniques for Deception*, 6-16.

Page 839 of 3957

deception, the unit was still available to conduct patrolling operations.[344] The deception goal was to incite the NVA to attack a specific firebase in order to neutralize the threat. The deception story was that the DIAMOND firebases were just more of many firebases, but conveniently located for attack: a variation of cry-wolf with an element of honeypot.

Deception Objective (DO)	NVA attacks DIAMOND firebases
Deception Target	NVA leadership in 25th Infantry Division area of operations
Deception Story (THINK)	DIAMOND firebases are perfectly positioned for NVA attack
Deception Events (SEE)	Portrayal – DIAMOND as typical firebase
Termination Trigger	On order once threat around firebase was disrupted

Table 21. Deception Analysis of DIAMOND I

In another example, prior to an attack on a Viet Cong (VC) stronghold, a ranger battalion conducted operations with heavy artillery support leading away from the VC base area. At the same time an Army of the Republic of Vietnam (ARVN) battalion similarly conducted operations moving away from the stronghold. After the feints were completed, the Ranger and ARVN troops were airlifted back to attack the stronghold. A prisoner captured during the assault on the stronghold indicated that the Ranger and ARVN battalion's movements lulled the VC into believing the base area was not the target of the operation. Usually feints are used to draw enemy forces away from the decisive point, but knowing how the enemy will react allowed the feints to achieve the opposite result. In this case, the feints of the Ranger and ARVN battalions were successful in convincing the VC to remain at the decisive point.[345]

Deception Objective (DO)	VC force remains at the stronghold
Deception Target	VC stronghold commander
Deception Story (THINK)	It is safe to remain at the stronghold because the Ranger and ARVN battalions do not know about it
Deception Events (SEE)	Feint – Ranger battalion operation moving away from stronghold Feint – ARVN battalions operation moving away from stronghold Simulation – additional camp fires
Termination Trigger	Assault on stronghold

Table 22. Deception Analysis of Ranger Assault

[344] *Reference Book 31-40: Techniques for Deception*, 6-17.

[345] Headquarters, U.S. Military Assistance Command, Vietnam, *Combat Experiences 2-69* (San Francisco: Headquarters, U.S. Military Assistance Command, Vietnam, 1969), accessed 11 July 2011, http://handle.dtic.mil/100.2/AD0504303, 3.

H. OPERATION DESERT STORM

Operation DESERT STORM provides an exemplar of how the concepts of deception work together to achieve the desired effect. According to General Schwartzkopf, Coalition forces implemented the "Hail Mary" plan because unfavorable force ratios—the Iraqi forces in Kuwait had numerical superiority and were in the defensive—precluded a frontal assault. Therefore, the flanking maneuver was essential for countering the Iraqi force advantage. [346] Deception became key to distracting Saddam from the "Hail Mary" preparations:

> The goal of the deception was to convince the Iraqis that the main attack would come up Wadi Al Batin along the Kuwaiti-Iraqi western border. This attack would be supported by an amphibious attack from the northern Gulf and attacks directly into the defenses along the southern Kuwaiti border. The desired effect was to hold the RGFC and the professional army, the regular armor and mechanized divisions, oriented upon the Wadi and coast. This disposition would expose them to the VII and XVIII Airborne Corps enveloping maneuver and facilitate their destruction.[347]

This deception plan played to Saddam's expectations, as early intelligence reports indicated a concern about amphibious operations and a belief that an attack through the desert was impossible.[348]

The first step of the deception plan was the removal of Saddam's primary channel for intelligence—the Iraqi Air Force.[349] Prior to the start of the air campaign, reconnaissance and logistical preparations for the envelopment were prohibited, with all activity limited to reinforcing the perception of the main effort coming through Wadi Al Batin. In response to the staging of forces at the mouth of the wadi, Iraqi forces reinforced their positions on the other side. Within the assembly areas, "Virtually every division constructed replicas of Iraqi defensive positions and conducted extensive

---

[346] H. Norman Schwarzkopf, "Central Command Briefing," *Military Review*, 71, no. 9 (September 1991): 96 – 97.

[347] Breitenbach, "Operation Desert Deception," 2 – 3.

[348] Breitenbach, "Operation Desert Deception," 10 – 11.

[349] Schwarzkopf, "Central Command Briefing," 97.

training against them."[350] The press pool was allowed access to report on this training, but not to the maneuver training necessary for the flanking maneuver. Once the air campaign was started, and the threat of the Iraqi Air Force removed, VII Corps and XVIII Corps moved from their staging areas south of Wadi Al Batin to their new staging areas in the western desert. As a security measure for the movement, and to maintain the illusion that the two Corps were still in place, other units still located in the original staging areas portrayed the XVIII Corps using false radio traffic.[351]

Portraying a secondary effort, the II Marine Expeditionary Force conducted several amphibious training exercises, including Operation IMMINENT THUNDER. These demonstrations had the intended effect of causing seven Iraqi divisions to shift to the Kuwaiti Coast.[352] The press was given access to cover these amphibious training operations as well, providing another channel to Saddam on the Coalition's intent to conduct an amphibious landing.[353] The amphibious demonstrations were further reinforced by PSYOP leaflets showing a tidal wave shaped like a Marine washing over Iraqi soldiers.[354] On the morning of 24 February, SEAL Task Force Mimke conducted an amphibious feint, supported by naval gunfire, to reinforce the threat of landings in order to prevent the reallocation of the Iraqi divisions on the coast.[355]

The deception operations may have worked a little too effectively. When the 1st Cavalry Division launched its feint on 24 February through Wadi Al Batin, it met little resistance. The Joint Forces Command East and I Marine Expeditionary Force similarly met little resistance along the coast. The Iraqi forces were so concerned with being flanked by an amphibious landing they had withdrawn forty kilometers north. The quick advance of these forces necessitated the launch of the Hail Mary eighteen hours early.

---

[350] Breitenbach, "Operation Desert Deception," 5.

[351] Breitenbach, "Operation Desert Deception," 5.

[352] Breitenbach, "Operation Desert Deception," 4.

[353] Schwarzkopf, "Central Command Briefing," 102. It's important to note that the press were not actively deceived or given disinformation to publish. They were afforded the opportunity to observe actual training and allowed to draw their own conclusions and report on it as they saw fit.

[354] Herbert Friedman, "Leaflets of Operation Desert Shield and Desert Storm," accessed 25 May 2012, http://www.psywarrior.com/HerbDStorm.html.

[355] Breitenbach, "Operation Desert Deception," 7.

The rapid withdraw of Iraqi forces and the resultant rapid advance of Coalition forces into Kuwait sufficiently upset the operation's synchronization that Schwarzkopf and his ground commanders were forced to sacrifice some initiative in order to reset synchronization.[356]

Deception Objective (DO)	Iraqi forces concentrate away from "Hail Mary" flanking movement
Deception Target	Saddam
Deception Story (THINK)	Coalition main effort will come through Wadi Al Batin with supporting amphibious landing
Deception Events (SEE)	Demonstration – 1st Cavalry Division entry into Wadi Al Batin Demonstration – II Marine Expeditionary Force's amphibious training Demonstration – Training facilities in the assembly areas Disinformation – PSYOP using amphibious imagery Portrayal – Radio traffic of XVIII Corps Blending – Radio silence by XVIII Corps
Termination Trigger	On order

Table 23. Deception Analysis of Operation DESERT STORM

[356] Breitenbach, "Operation Desert Deception," 21 – 25.

Page 843 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 844 of 3957

VII. CONCLUSIONS AND RECOMMENDATIONS

> *As a nation we are bred up to feel it a disgrace even to succeed by falsehood… we will keep hammering along with the conviction that 'honesty is the best policy,' and that truth always wins in the long run. These pretty little sentences do well for a child's copy-book, but the man who acts upon them in war had better sheathe his sword forever.*
>
> *– Colonel Sir Garnet Wolseley*[357]

A. CONCLUSION

Deception has demonstrated its utility in the exercise of war since the dawn of recorded history. Even within the more limited scope of U.S. Army operations, deception has proven its worth time and again, from helping to save the Continental Army from sure destruction during the Revolutionary War to assisting in the rapid and complete defeat of a numerically superior foe during Operation DESERT STORM. Likewise, deception has proven its worth against conventional foes such as the German and Iraqi Armies, and against irregular foes like the Viet Cong and the Philippine insurgents. Given the demonstrated worth of deception across the spectrum of operations and against myriad opponents, it is unacceptable to see the lack of emphasis given deception in current Army doctrine.

The level of emphasis of deception within U.S. Army doctrine has waxed and waned between 1905 and 2012. A number of explanations for this fluctuation have been presented, e.g., morality, the American style of war, and a professional officer class. The fluctuation is perhaps best explained by the perceived balance of power with the nation's adversaries and the resultant leaning towards either the cumulative destruction or systemic disruption styles of war. When the U.S. Army perceives it has a force advantage—as has been the case since the end of the Cold War—then weight is given towards cumulative destruction, while systemic disruption and deception wanes. Conversely, when the U.S. Army perceives a force disadvantage—as was the case during World War II and the period of the 1970s through Operation DESERT STORM—then

[357] Garnet Wolseley, *The Soldier's Pocket-book for Field Service*, 2nd ed. (London and New York: MacMillian and Co., 1871), 81.

weight is given systemic disruption and deception, while cumulative destruction wanes. If this is indeed the case, then the emerging era of austerity and economy of force roles would seem to suggest a shift towards systemic disruption and with it deception is in the offing. Furthermore, since balance of power ratios are essentially meaningless against adversaries relying on heavily systemic disruption approaches—e.g., Al Qaeda and other non-state actors—deception would appear to be of increased utility. However, the most recent capstone doctrine publications *ADP 3-0 and ADRP 3-0* between them have a single bullet point mentioning deception without elaboration.[358] As the U.S. Army seeks to do more with less, it must take to heart Whaley's observation about the cost of deception:

> Stratagem is cheap. It requires a very small initial investment of men and materiel. Effective stratagem can be the part-time work of only one man, particularly if he is the commander. And the most elaborate of such operations involved only diverting for a few weeks the services of several hundred men, a dozen or so small boats, a few aircraft, a fair amount of radio and other electronic gear, some wood, canvas, and paint, and bits of aluminum scrap. None of this was permanently lost to inventory, except the aluminum.[359]

B. RECOMMENDATIONS

What follows are some recommendations the U.S. Army should adopt to address the current shortfall of deception emphasis within doctrine and operations. These recommendations are an economy of force middle ground between the current doing nothing, and the actions of a resource rich U.S. Army. If resources and personnel were as effectively unlimited as they were in World War II, these recommendations would include a call for purpose built deception support battalions—modern versions of 23rd Headquarters Special Troops. However, this recommendation is unfeasible in the current fiscal and force cap environment, thus the recommendations focus on increasing the capabilities of existing units and personnel.

---

[358] Headquarters, Department of the Army, *Army Doctrine Reference Publication 3-0: Unified Land Operations* (Washington, DC: Department of the Army, 2012), 3-2; Headquarters, Department of the Army, *FM 100-5, 1954*, 37.

[359] Whaley, *Stratagem* (1969), 232.

1. Doctrine

"Capstone doctrine establishes the Army's view of the nature of operations, the fundamentals by which Army forces conduct operations, and the methods by which commanders exercise mission command;" therefore, in order for deception to be fully integrated into U.S. Army operations, deception must be fully integrated into U.S. Army doctrine.[360] The current single bullet guidance in *Army Doctrine Reference Publication 3-0: Unified Combat Operations* of "conduct military deception" without further elaboration must change to something along the lines of the guidance in *FM 100-5* (1954), which stated: "It is imperative that commanders constantly realize the importance of combat deception and that they train their troops and staff in the techniques and planning for combat deception."[361]

To achieve full integration of deception within Army doctrine, an office dedicated to the proponency of military deception must be created at either the Mission Command Center of Excellence or the Special Warfare Center and School. The office must have the single mission of proponency for deception, because prior history indicates that deception suffers when it is a secondary task. This office must have the mandate for active military deception and coordination authority with the proponents for the cover aspects of deception, e.g., camouflage, OPSEC, and counterintelligence. In addition to coordination authority, the deception office must be incorporated into the approval process for doctrine related to the covering aspects of deception so as to ensure unity of effort in the presentation of deception doctrine. Finally, all formal education on active deception must be either consolidated under the auspices of, or the programs of instruction approved by, the deception office; again to ensure unity of effort and message.

In the development of deception doctrine, the focus should be on theory with illustrative examples illuminating the theory in an operational context. The purpose of the doctrine should be to spark creative thought on how deception might be practiced, not to dictate how deception is practiced. Additional emphasis should be given to the

[360] Headquarters, Department of the Army, *Army Doctrine Publication 3-0*, 1.

[361] Headquarters, Department of the Army, *Army Doctrine Reference Publication 3-0*, 37.

information requirements needed to develop a full understanding of the target. Particular care must be taken to ensure that doctrine does no prescribe particular techniques or template approaches; a doctrinaire or dogmatic approach would create the potential disastrous situation of predictable deception.

2. Leadership, Education, and Training

Integration of deception into U.S. Army operations demands that leaders embrace the potential of deception as part every operation. There are two ways to inculcate a respect for the utility of deception in leaders. First is for senior leaders at the upper echelons of the U.S. Army to direct deception integration into all training operations as a forcing function, especially at the combined arms training centers. Commanders who are accustomed to integrating deception into field training exercises beginning during the formative stages of their careers will be more apt to integrate deception into actual operations. Care must be exercised to ensure that the integration of deception into training does not degenerate into a templated, predictable process, as the use of variety is an essential factor in deception success.

Second is for leaders at the lowest echelon practical to receive formal education in deception (Table 24). As the earlier a leader is trained and aware of the utility of deception the more likely deception will be integrated into the leader's planning methodology. Additionally, the educating and implementing at the lowest levels helps to ensure that as personnel advance, their experience with deception advances as well. If company commanders receive formal education on deception, then as they move up into senior leadership and staff positions they will carry the education with them, so that the majority of staff members from battalion and up will have training and experience in deception. The combination of the top down forcing function coupled with the bottom up education will serve to inculcate the idea of deception in the force more thoroughly than either approach by itself. This will help to bring the situation described in 1941 *Field Service Regulations of Operations* to fruition:

> A commander who is ingenious and resourceful in the use of tactical strategems [*sic*] and ruses often will find methods of deceiving or misleading the enemy and of concealing his own intentions.[362]

As with deception doctrine, formal deception education should focus on the theory of deception, especially the target's decision-making process, and the concepts of biases, schemata, and heuristics. In addition to theory, formal education should include an emphasis on the information requirements for profiling potential targets. Illustrative examples drawn from prior uses of deception should be used to illuminate the theory within an operational context, but not as examples of "how to conduct" deception. What must be avoided in the formal education are any deception planning templates or guides that could result in a dogmatic approach to deception.

Organization	Echelon	Minimum	Optimum (In addition to minimum)
General Purpose Forces	Corps/Division	Commander G3 G2 G5	Deputies G3/NCOICs MISO OIC / NCOIC Inform and Influence OIC
	Brigade/Battalion	Commander S3 S2 S3 Plans	Command Sergeant Major S3/S2 NCOICs Inform and Influence OIC MISO NCOIC
	Company	Commander	First Sergeant Platoon Leaders Platoon Sergeants
Special Forces	Group/Battalion	Commander S3 S2 S5 Battalion Operations Warrant	Assistant S3 / S2 Command Sergeant Major S3/S2 NCOICs
	Company	Commander Company Operations Warrant	Company Operations Sergeant Major Operations Sergeant Operations/ Intelligence Sergeant
	Detachment	Asst Detachment Commander Operations/ Intelligence Sergeant	Detachment Commander Operations Sergeant
Military Information Support Operations	Command/Group/Battalion	Commander S3 S2	Deputy Commander S3/S2 Deputies Command Sergeant Major S3/S2 NCOICs
	Company	Commander	First Sergeant
	Detachment	OIC	NCOIC
	Team	NCOIC	

Table 24. Recommended Personnel for Formal Deception Education

[362] War Department, *Field Service Regulations of Operations, 1941*, 58.

3. Personnel Selection

The personnel holding the positions in Table 24 are the recommended recipients of formal deception education; however, this should not be interpreted as saying these personnel are the only ones involved in deception planning. Depending on the deception plan, other personnel may be needed, e.g., developing a notional order of battle will require a witting actor in the personnel section. Additionally, the fact a person occupies a position indicated in Table 24 does not imply the person is cut out for deception planning; more important than either the rank or the position are the personal characteristics of a deception planner. Deception planning requires a certain type of strategic thinker who has initiative and is creative, intelligent, mentally agile, and security conscious. A deception planner does not need to be "immoral" or "morally flexible;" rather, a planner needs to be able to set aside personal considerations for the accomplishment of the mission. Lieutenant Colonel Simenson, the operations officer for 23rd Headquarters Special Troops, was personally against the use of deception, but he did not let his personal feelings interfere with the mission.[363] That said, a person who is unable to set aside personal feelings on deception is best left as an unwitting actor.

A commander may feel the need to reach outside his staff for the best candidate; much like General Wavell requested Dudley Clarke by name to head up British deception efforts in North Africa during World War II.[364] Regardless of whom the commander chooses to lead his deception planning, the planner must be assigned to the unit. It is unrealistic and counterproductive to expect an outside element to assume deception planning for a unit. First, delegating responsibility to an outside element undermines the integration of deception into unit training and operations; when the outside element is not present during routine field training exercises neither is deception. Second, attaching a deception planning function serves to inhibit the growth of an organic capacity for deception within the unit by absolving the supported commander and staff of the planning responsibility. The commander responsible for the overall mission must also plan and execute the supporting deception stratagem.

---

[363] Gerard, *Secret Soldiers*, 85.

[364] Mure, *Master of Deception*, 58.

4. Facilities

Deception planning requires a segregated facility in order to control access to the deception plan. The segregated facility can be as simple as a lockable room to secure compartmentalized information. The critical requirement is that the facility is commensurate with the level of classification of the plan and supporting resources. At the same time, the deception planner cannot work in complete isolation from the rest of plans and operations. In order to ensure the deception plan is fully nested in the supported plan, the deception planner must also be physically integrated into overall operations planning, and therefore also needs to have a space that is connected to the plans space.

C. FINAL NOTE

As a final word of caution, the deception practitioner must remember that the past is a guide not a blueprint. As Roger Hesketh notes in his report on Operation FORTITUDE: "It is always unsafe to apply too literally the experiences of one war to the changed circumstances of another."[365] A good example of a historic technique which may no longer be appropriate is the use of troops to convey disinformation as prisoners. Magruder used troops portraying deserters to convey disinformation to McClellan; this tactic would be rightfully unacceptable today for U.S. planners—though interrogators must still watch for this deception in use by our adversaries.[366] Likewise, the use of a corpse as the central prop in Operation MINCEMEAT might have trouble making it through legal review today, or more importantly, the target's forensic capabilities. And the deliberate use of the press to convey disinformation as was the case with Operation WEDLOCK would surely cause significant blowback today. [367] This is not to say that these techniques cannot be adapted for use in the current operational environment; rather, that historic examples of deception must be adapted for usage in the current operating environment, with careful consideration given to the changes since the time the deception was executed.

---

[365] Hesketh, *Fortitude*, 351.

[366] The Editors of the Army Times. *The Tangled Web, 5.*

[367] Herbig, "American Strategic Deception," 270 – 271.

Page 851 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Acosta, David A. “The Makara of Hizballah: Deception in the 2006 Summer War.” Master’s thesis, Naval Postgraduate School, 2007. Accessed 9 March 2012. http://handle.dtic.mil/100.2/ADA469918.

Adams, John, Abigail Adams, and Charles Adams. *Familiar Letters of John Adams, and His Wife Abigail Adams during the Revolution. with a Memoir of Mrs. Adams*. New York: Hurd and Houghton, 1876. Google e-book, http://books.google.com/books?id=fYEEAAAAYAAJ.

Allison, Graham and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd ed. New York: Addison Wesley Longman, Inc., 1999.

Anderson, Marie and Emily Zukauskas, eds. *Operational Law Handbook: 2008*. Charlottesville, VA: The Judge Advocate General’s Legal Center and School, 2008.

Baker, Richard. “The Lost and found Art of Deception.” Paper presented at the Conference of Army Historians, Arlington, VA, 25 – 28 July 2011.

Bell, J. Bowyer. “Aspects of the Dragonworld: Covert Communications and the Rebel Ecosystem.” *International Journal of Intelligence and Counterintelligence* 3, no. 1 (1989): 15 – 43.

———. “Toward a Theory of Deception.” *International Journal of Intelligence and Counterintelligence* 16, no. 2 (2003): 244 – 279. Accessed 8 March 2012. http://dx.doi.org/10.1080/08850600390198742.

Bell, J. Bowyer and Barton Whaley. *Cheating and Deception*. New Brunswick, NJ Transaction Publishers, 1991.

Bennett, Michael and Edward Waltz. *Counterdeception Principles and Applications for National Security*. Artech House Intelligence and Information Operations Library. Norwood, MA: Artech House, Inc., 2007.

Boyd, John. “Organic Design for Command and Control,” Working Paper, 1987, Accessed 19 February 2012. http://www.danford.net/boyd/organic.pdf.

———. “The Strategic Game of ? and ?” Presentation, 1987, Accessed 19 February 2012. http://www.danford.net/boyd/strategic.pdf.

Breitenbach, Daniel. “Operation Desert Deception: Operational Deception in the Ground Campaign.” Paper, Naval War College, 1991. Accessed 24 May 2012. http://handle.dtic.mil/100.2/ADA253245.

Page 853 of 3957

Center for Army Lessons Learned. *CALL Bulletin 3-88: Deception*. Fort Leavenworth, KS: Combined Arms Training Activity, 1988.

Chisholm, Roderick M. and Thomas D. Feehan. "The Intent to Deceive." *The Journal of Philosophy* 74, no. 3 (March, 1977): pp. 143 – 159. Accessed 11 January 2012. http://www.jstor.org/stable/2025605.

Clausewitz, Carl von. *On War*. Translated by Michael Howard and Peter Paret. 3rd ed. New York: Alfred A. Knopf, Inc., 1993.

Cline, Lawrence. *Pseudo Operations and Counterinsurgency: Lessons from Other Countries*. Carlisle, PA: Strategic Studies Institute, 2005. Accessed 20 April 2011, http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=607.

Concepts and Force Design Group. *Tactical Cover and Deception: Final Report*. Alexandria, VA: U.S. Army Combat Developments Command, 1972, Accessed 8 August 2011. https://www.dtic.mil/DOAC/document?document=ADB966185&collection=ac-tr&contentType=PDF&citationFormat=1f.

Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. New York, NY: Back Bay Books, 2002.

Cruickshank, Charles. *Deception in World War II*. London: Book Club Associates, 1979.

Daniel, Donald C. and Katherine L. Herbig. "Propositions on Military Deception." In *Strategic Military Deception*. Edited by Donald C. Daniel and Katherine L. Herbig, 3 – 30. New York: Pergamon Press, 1982.

Deception Research Program. *Deception Maxims: Fact and Folklore*. Washington, DC: Office of Research and Development, Central Intelligence Agency, 1980.

Dempsey, Martin. "America's Military—a Profession of Arms." Washington, DC: Joint Chiefs of Staff, 2012. Accessed 24 February 2012. http://www.jcs.mil/content/files/2012-02/022312120752_Americas_Military_POA.pdf.

Dewar, Michael. *The Art of Military Deception in Warfare*. 1st ed. Newton Abbot, UK: David & Charles, 1989.

Director of Central Intelligence. *Special National Intelligence Estimate, Number 100-2-57: Soviet Capabilities for Deception*. Washington, DC: Central Intelligence Agency, 1957. Accessed 30 January 2012. http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&res_dat=xri:dnsa&rft_dat=xri:dnsa:article:CSE00201.

Page 854 of 3957

Dunnigan, James F. and Albert A. Nofi. *Victory and Deceit: Dirty Tricks at War*. New York: William Morrow and Company, Inc., 1995.

Eisenhower, Dwight D. *The Papers of Dwight David Eisenhower: The Chief of Staff*. Edited by Louis Galambos. Vol. VIII. Baltimore: Johns Hopkins Press, 1978.

Epstein, Edward. *Deception: The Invisible War between the KGB and the CIA*. New York, NY: Random House Value Publishing, 1991.

Erfurth, Waldemar. *Surprise*. Translated by Stefan T. Possony and Daniel Vilfroy. Harrisburg, PA: Military Service Publishing Company, 1943.

Ferris, John. "'FORTITUDE' in Context: The Evolution of British Military Deception in Two World Wars, 1914-1945." In *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*. Richard K. Betts, and Thomas G. Mahnken, eds. 117 – 165. London: Frank Cass, 2003.

Funston, Frederick. *Memories of Two Wars*. London: Constable & Co., Limited, 1912.

Gerwehr, Scott and Russell W. Glenn. *The Art of Darkness: Deception and Urban Operations*. Santa Monica, CA: RAND, 1999. Accessed 16 August 2011. http://www.rand.org/publications/MR/MR1132.

———. *Unweaving the Web: Deception and Adaptation in Future Urban Operations*. Santa Monica, CA: Rand, 2002. Accessed 16 August 2011. http://www.rand.org/publications/MR/MR1495/.

Gilovich, Thomas. *How We Know What Isn't So*. New York, NY: The Free Press, 1991.

Godson, Roy and James J. Wirtz. "Strategic Denial and Deception." In *Strategic Denial and Deception: The Twenty-First Century Challenge*. Edited by Roy Godson and James J. Wirtz, 1 – 14. Piscataway, NJ: Transaction Publishers, 2002.

Goldhamer, Herbert. *Reality and Belief in Military Affairs: A First Draft (June 1977)*. Santa Monica, CA: The Rand Corporation, 1979. Accessed 25 August 2011. http://www.rand.org/content/dam/rand/pubs/reports/2005/R2448.pdf.

Goldsmith, Robert and Ralph Gerenz. *Techniques for Detecting Cover and Deception*. Billerica, MA: Betac Corporation, 1983. Accessed 16 May 2012, http://handle.dtic.mil/100.2/ADP002896.

Grabo, Cynthia. *Anticipating Surprise: Analysis for Strategic Warning*. Edited by Jan Goldman. Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, 2002. Accessed 14 May 2012, www.ni-u.edu/ni_press/pdf/Anticipating_Surprise_Analysis.pdf, 125.

Page 855 of 3957

Handel, Michael I. *Masters of War: Classical Strategic Thought*. 3rd rev. and expanded ed. London; Portland, OR: Frank Cass, 2001.

Harris, Stanley G. "Organizational Culture and Individual Sensemaking: A Schema-Based Perspective." *Organization Science* 5, no. 3 (August, 1994): 309 – 321. Accessed 24 February 2012. http://www.jstor.org/stable/2635133.

Haswell, Jock. *The Tangled Web: The Art of Tactical and Strategic Deception*. Buckinghamshire, UK: John Goodchild Publishers, 1985.

Headquarters, Department of the Army. *Army Doctrine Publication 3-0: Unified Land Operations*. Washington, DC: Department of the Army, 2011.

———. *Army Doctrine Reference Publication 3-0: Unified Land Operations*. Washington, DC: Department of the Army, 2012.

———. *Army Tactics, Techniques, and Procedures 3-34.39: Camouflage, Concealment, and Decoys/Marine Corps Reference Publication 3-17.6A*. Washington, DC: Department of the Army, 2010.

———. *Field Manual 1: The Army, 2005*. Washington, DC: Department of the Army, 2005.

———. *Field Manual 100-1: The Army*. Washington, DC: Department of the Army, 1994.

———. *Field Manual 100-5: Field Service Regulations—Operations, 1949*. Washington, DC: Department of the Army, 1949.

———. *Field Manual 100-5: Field Service Regulations—Operations, 1954*. Washington, DC: Department of the Army, 1954.

———. *Field Manual 100-5: Field Service Regulations—Operations, 1962*. Washington, DC: Department of the Army, 1962.

———. *Field Manual 100-5: Operations, 1976*. Washington, DC: Department of the Army, 1976.

———. *Field Manual 100-5: Operations, 1982*. Washington, DC: Department of the Army, 1982.

———. *Field Manual 100-5: Operations, 1986*. Washington, DC: Department of the Army, 1986.

Page 856 of 3957

———. *Field Manual 100-5: Operations, 1993*. Washington, DC: Department of the Army, 1993.

———. *Field Manual 1-02: Operational Terms and Graphics*. Washington, DC: Department of the Army, 2004.

———. *Field Manual 20-3: Camouflage, 1993*. Washington, DC: Department of the Army, 1990.

———. *Field Manual 20-3: Camouflage, Concealment, and Decoys, 1999*. Washington, DC: Department of the Army, 1999.

———. *Field Manual 3-0: Operations, 2001*. Washington, DC: Department of the Army, 2001.

———. *Field Manual 3-0: Operations, Change 1*. Washington, DC: Department of the Army, 2011.

———. *Field Manual 30-101: Aggressor, the Maneuver Enemy, 1959*. Washington, DC: Department of the Army, 1959.

———. *Field Manual 31-21: Guerrilla Warfare and Special Forces Operations*. Washington, DC: Department of the Army, 1958.

———. *Field Manual 3-13: Information Operations: Doctrine, Tactics, Techniques, and Procedures* Department of the Army, 2003.

———. *Field Manual 5-20: Camouflage Basic Principles and Field Camouflage, 1959* . Washington, DC: Department of the Army, 1959.

———. *Field Manual 5-20: Camouflage, 1968*. Washington, DC: Department of the Army, 1968.

———. *Field Manual 90-2: Battlefield Deception* 1988. Washington, DC: Department of the Army, 1988.

———. *Field Manual 90-2: Battlefield Deception (HTF)*. Washington, DC: Department of the Army, 1978.

———. *General Orders no. 20*. Alexandria, VA: Department of the Army, 1955. Accessed 28 February 2012. www.armypubs.army.mil/epubs/pdf/go5520.pdf
.

———. *Training Circular No. 30-1: Tactical Cover and Deception*. Washington, DC: Department of the Army, 1969. Photocopy, University of Texas A&M, College Station, Texas.

Headquarters, U.S. Military Assistance Command, Vietnam. *Combat Experiences 2-69*. San Francisco: Headquarters, U.S. Military Assistance Command, Vietnam, 1969. Accessed 11 July 2011. http://handle.dtic.mil/100.2/AD0504303.

Headquarters X Corps War Diary Summary for Operation Chromite: 15 August to 30 August 1950. 1950. Accessed 24 January 2012. http://cgsc.cdmhost.com/utils/getfile/collection/p4013coll11/id/831/filename/832.pdf.

Heilbrunn, Otto. *Partisan Warfare*. New York: Frederick A. Praeger, 1962.

Heiman, Leo. "War in the Middle East: An Israeli Perspective." *Military Review* 47, no. 9 (1967): pp. 56 – 66.

Henderson, G. F. R., and Garnet Wolseley. *Stonewall Jackson and the American Civil War*. 2 vols. London, New York [etc.]: Longmans, Green and Co., 1936.

Herbig, Katherine. "American Strategic Deception in the Pacific: 1942-44." In *Strategic and Operational Deception in the Second World War*, edited by Michael Handel, pp. 260 – 300. New York: Routledge, 1987.

Hesketh, Roger. *Fortitude: The D-Day Deception Campaign*. Woodstock and New York, NY: The Overlook Press, 2000.

Heuer, Richards J., Jr. *Psychology of Intelligence Analysis*. Reston, VA: Pherson Associates, LLC, 2007.

Hicinbothom, James, Wayne Zachary, Beverly Knapp, Allen Zaklad, and Alvah Bittner, Jr. *Doing Deception: Attacking the Enemy's Decision Processes*. Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, 1990. Accessed 10 March 2012. http://handle.dtic.mil/100.2/ADA221529.

Higginbotham, Benjamin. "On Deceiving Terrorists." Master's thesis, Naval Postgraduate School, 2001. Accessed 4 January 2010. http://handle.dtic.mil/100.2/ADA401353.

Howard, Michael. *British Intelligence in the Second World War: Strategic Deception*. Vol. 5. New York: Cambridge University Press, 1990.

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1976.

Page 858 of 3957

Johnson, Dominic and Dominic Tierney. "Crossing the Rubicon: The Perils of Committing to a Decision." Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2011. Accessed 27 September 2011. http://belfercenter.ksg.harvard.edu/files/johnson-and-tierney-sep-2011.pdf.

Joint Staff. *JP 3-13.4: Military Deception*. Department of Defense, 2006.

Ketchum, Richard M. *The Winter Soldiers*. 1st ed. Garden City, NY: Doubleday, 1973.

Kitson, Frank. *Gangs and Counter-gangs*. London: Barry and Rockliff, 1960.

Kuhn, Thomas. *The Structure of Scientific Revolutions*. 3rd ed. Chicago: University of Chicago Press, 1996.

Latimer, Jon. *Deception in War*. New York: The Overlook Press, 2001.

Liddell Hart, Basil. *Sherman: Soldier, Realist, American*. New York: Dodd, Mead, and Company, 1929.

———. *Strategy*. 2d rev ed. New York: Meridian, 1991.

Lind, William. "The Case for Maneuver Doctrine." In *The Defense Reform Debate*. Edited by Asa Clark, Peter Chiarelli, Jeffrey McKitrick, and James Reed, 88 – 100. Baltimore: The John Hopkins University Press 1984.

———. "Defense Reform: a Reappraisal." In *The Defense Reform Debate*. Edited by Asa Clark, Peter Chiarelli, Jeffrey McKitrick, and James Reed, 327 – 333. Baltimore: The John Hopkins University Press 1984.

Luttwak, Edward. "Notes on Low-Intensity Warfare." *Parameters* 8, no. 4 (1983): 11 – 18. Accessed 14 July 2011. http://www.carlisle.army.mil/usawc/Parameters/Articles/1983/1983%20luttwak.pdf.

Luttwak, Edward and Steven Canby. *MINDSET: National Styles in Warfare and the Operational Level of Planning, Conduct and Analysis*. Pontiac, MA: C&L Associates, 1980. Accessed 11 March 2012. http://handle.dtic.mil/100.2/ADA142722.

Markus, Hazel. "Self-Schemata and Processing Information about the Self." *Journal of Personality and Social Psychology* 35, no. 2 (1977): 63 – 78. Accessed 24 February 2012. http://psycnet.apa.org/doi/10.1037/0022-3514.35.2.63.

McRaven, William H. *Spec Ops: Case Studies in Special Operations Warfare Theory & Practice*. Novato, CA: Presidio Press, 1995.

Page 859 of 3957

Mure, David. *Master of Deception: Tangled Webs in London and the Middle East*. London: William Kimber & Co. Limited, 1980.

Nelson, Bradley K. "Battlefield Deception: Abandoned Imperative of the 21st Century." Monograph, U.S. Army Command and General Staff College, 1997. Accessed 2 January 2012. http://handle.dtic.mil/100.2/ADA339425.

The New York Times. "Funston Subject of Sermon." *New York Times (1857-1922).* April 15, 1901, ProQuest (96118056).

Noane, Erica. "Hijacking Satellite Navigation." Massachusetts Institute of Technology. Accessed February 25, 2012. http://www.technologyreview.com/computing/21452/.

Office of the Adjutant General. *Lessons Learned, Headquarters, 4th Infantry Division Artillery*. Washington, DC: Department of the Army, 1969. Accessed 22 January 2012. http://handle.dtic.mil/100.2/AD0505964.

Office of the Chief of Army Field Forces. *Strategic and Tactical Cover and Deception Training*. Fort Monroe, VA: Department of the Army, 1948. Photocopy, U.S. Army Military History Institute, Carlisle, PA.

Official History of the 23rd Headquarters Special Troops. Photocopy from the National Archives.

Paddock Jr, Alfred *US Army Special Warfare. Its Origins: Psychological and Unconventional Warfare, 1941-1952*. Washington, DC: National Defense University, 1982. Accessed 16 February 2012. http://handle.dtic.mil/100.2/ADA118758.

Plaster, John. *SOG: The Secret Wars of America's Commandos in Vietnam*. New York: Penguin Group, 1998.

Plutarch, John Dryden, and Arthur Hugh Clough. *Plutarch's Lives.* Modern Library paperback ed. Vol. 1. New York: Modern Library, 2001.

Prados, John. *Presidents' Secret Wars*. Revised and updated ed. Chicago: Elephant Paperbacks, 1996.

Random House Webster's Unabridged Dictionary. New York: Random House Reference, 2001.

Reese, William. "Deception within a Communications Theory Framework." In *Strategic Military Deception*, edited by Donald C. Daniel and Katherine L. Herbig, 99 – 114. Elmsford, NY: Pergamon Press Inc, 1982.

Page 860 of 3957

Schwarzkopf, H. Norman. “Central Command Briefing.” *Military Review* 71, no. 9 (September 1991): 96 – 108.

Sherman, William. *Memoirs of General William T. Sherman*. Vol 2. 2nd ed. New York: D Appleton and Company, 1904.

Shulsky, Abram. “Elements of Strategic Denial and Deception.” In *Strategic Denial and Deception: The Twenty-First Century Challenge*. Edited by Roy Godson and James J. Wirtz, 15 – 39. Piscataway, NJ: Transaction Publishers, 2002.

Shultz, Richard H. *The Secret War Against Hanoi: Kennedy and Johnson’s Use of Spies, Saboteurs, and Covert Warriors in North Vietnam*. New York: HarperCollins, 1999.

Special Assistant for Counterinsurgency and Special Affairs (SACSA). *Draft MACSOG Documentation Study Annex A to Appendix C Psychological Operations*. Washington, DC: Joint Chiefs of Staff, 1970. Accessed 2 September 2011. http://www.dod.gov/pubs/foi/International_security_affairs/vietnam_and_southeast_asiaDocuments/520-1.pdf.

———. *Draft MACSOG Documentation Study Appendix A Summary of MACSOG Documentation Study*. Washington, DC: Joint Chiefs of Staff, 1970. Accessed 2 September 2011. http://www.dod.gov/pubs/foi/International_security_affairs/vietnam_and_southeast_asiaDocuments/520-22.pdf.

———. *Draft MACSOG Documentation Study Appendix H Security, Cover & Deception*. Washington, DC: Joint Chiefs of Staff, 1970. Accessed 2 September 2011. http://www.dod.gov/pubs/foi/International_security_affairs/vietnam_and_southeast_asiaDocuments/520-18.pdf.

Team “B”. *Soviet Strategic Objectives: An Alternative View*. Washington, DC: Director of Central Intelligence, 1976. Accessed 16 April 2012. http://www.foia.cia.gov/docs/DOC_0000278531/DOC_0000278531.pdf.

The Editors of the Army Times. *The Tangled Web: True Stories of Deception in Modern Warfare*. Washington, DC: R. B. Luce, 1963.

Tse-tung, Mao. “On the Protracted War “ In *Selected Works of Mao Tse-Tung*. Vol. 2, 113 – 194. Peking: Foreign Language Press, 1965.

Tversky, Amos and Daniel Kahneman. “Belief in the Law of Small Numbers.” *Psychology Bulletin* 76, no. 2 (1971): 105 – 110. Accessed 25 February 2012. http://pirate.shu.edu/~hovancjo/exp_read/tversky.htm

Page 861 of 3957

U.S. Army Command and General Staff College. *Reference Book 31-40: Techniques for Deception*. Fort Leavenworth, KS: U.S. Army Command and General Staff College, 1976.

U.S. Department of the Army. General Staff, G-3. "Combat Deception." 1954. Photocopy from U.S. Army Military History Institute, Carlisle, PA.

Von Greiffenberg, Hans. *Deception and Cover Plans Project #29*. Edited by Harald Kehm. Translated by J. B. Robinson (Koenigstein, Germany: Foreign Military Studies Branch, 1950), 80.

War Department. *Field Manual 100-5: Tentative Field Service Regulations of Operations, 1939*. Washington, DC: Government Printing Office, 1939.

———. *Field Manual 21-45: Basic Field Manual of Protective Measures, Individuals and Small Units*. Washington, DC: Government Printing Office, 1942.

———. *Field Manual 5-20: Camouflage Basic Principles, 1944*. Washington, DC: War Department, 1944.

———. *Field Manual 5-20: Engineer Field Manual of Camouflage, 1940*. Washington, DC: War Department, 1940.

———. *Field Service Regulations of Operations, 1941*. Washington, DC: Government Printing Office, 1941.

———. *Field Service Regulations, United States Army. 1905, with Amendments to 1908*. Washington, DC: Government Printing Office, 1908.

———. *Field Service Regulations, United States Army. 1910*. Washington, DC: Government Printing Office, 1910.

———. *Field Service Regulations, United States Army. 1914*. New York, NY: Government Printing Office, 1914.

———. *Field Service Regulations, United States Army. 1923*. Washington, DC: Government Printing Office, 1924.

The Washington Post. "Gen. Funston's Action." *The Washington Post (1877-1922)*, March 28, 1902, ProQuest (144350948).

Wass de Czege, Huba. "Army Doctrinal Reform." In *The Defense Reform Debate*, edited by Asa Clark, Peter Chiarelli, Jeffrey McKitrick, and James Reed, 101 – 120. Baltimore: The John Hopkins University Press 1984.

Weigley, Russell Frank. *The American Way of War: A History of United States Military Strategy and Policy*. Indiana University Press paperback ed. Bloomington, IN: University Press, 1977.

Wells, Leonard. "Military Deception: Equivalent to Intelligence, Maneuver and Fires." Paper, Navy War College, 2008. Accessed 20 May 2012. http://handle.dtic.mil/100.2/ADA494225.

Weyth, John. *Life of Lieutenant-General Nathan Bedford Forrest*. New York and London: Harper and Brothers Publishers, 1905.

Whaley, Barton. "The One Percent Solution." In *Information Strategy: A Guide to Theory and Practice*. Edited by John Arquilla and Douglas Borer, 127 – 159. New York and London: Routledge, 2007.

———. *Stratagem: Deception and Surprise in War*. Cambridge, MA: Center for International Studies Massachusetts Institute of Technology 1969. Accessed 16 February 2012. http://www.vietnam.ttu.edu/virtualarchive/items.php?item=2171516001.

———. *Stratagem: Deception and Surprise in War*. Norwood, MA: Artech House, 2007.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press, 1962.

Wolseley, Garnet. *The Soldier's Pocket-book for Field Service*. 2nd ed. London and New York: MacMillian and Co., 1871.

Womack, George. "Operational Deception and the Principles of War." Paper, Naval War College, 1994. Accessed 20 May 2012. http://handle.dtic.mil/100.2/ADA279632.

Page 863 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Joint Special Operations University
   Hurlburt Field, Florida

4. HQ 4th MISOC
   Ft. Bragg, North Carolina

5. HQ 5th Battalion, USAJFKSWCS
   Ft. Bragg, North Carolina

6. Marine Corps Information Operations Center
   Quantico, Virginia

7. Asymmetric Warfare Group
   Fort Meade, Maryland

8. SOCCENT J5-IO
   Tampa, Florida

9. SOCOM, J39
   MacDill Air Force Base, Florida

Page 865 of 3957

Report of the
Defense Science Board Task Force

on

DEFENSIVE INFORMATION OPERATIONS

Volume II- Part 2
Annexes

June 2001

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

Office of the Undersecretary of Defense
For Acquisition, Technology and Logistics
Washington, D.C. 20301-3140

20010718 091

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2001	Final Technical, 2001

4. TITLE AND SUBTITLE
Defense Science Baord Task Force on Defensive Information Operations, Volume II - Part 2 (Protecting the Homeland)

5. FUNDING NUMBERS
N/A

6. AUTHOR(S)
Mr. Larry Wright
Task Force Chairman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Science Board
Office of the Under Secretary of Defense (AT&L)
3140 Defense Pentagon
Room 3D865
Washington DC 20301-3140

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Science Board
Office of the Under Secretary of Defense (AT&L)
3140 Defense Pentagon
Room 3D865
Washington DC 20301-3140

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

11. SUPPLEMENTARY NOTES
N/A

12a. DISTRIBUTION AVAILABILITY STATEMENT
Distribution Statement A: Unlimited Distribution

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

15. NUMBER OF PAGES
378

16. PRICE CODE
N/A

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	N/A	N/A

Standard Form 298 (Rev. 2-89) (EG)
Prescribed by ANSI Std. 239.18
Designed using Perform Pro, WHS/DIOR, Oct 94

TABLE OF CONTENTS

DSB VOLUME II – DEFENSIVE INFORMATION OPERATIONS
PART 2

Annex A – Information Architecture Assurance

Annex B – Technology

Annex C – Organization & Operations

Annex D – Policy

Annex E – Legal

Annex F – 1996 DSB Status Matrix

Annex G – Thought Pieces:

Tab G-1: The Insider Threat & The Low and Slow Attack

Tab G-2: Data/Information/Knowledge/Understanding

Tab G-3: Oversight and Management of the GIG Executive Director

Tab G-4: Red Teaming and the Cyber Operations Readiness Triad (CORT)

Annex H – Reference Data:

Tab H-1: CERT and IO POC List

Tab H-2: Terms of Reference

ANNEX A

Defense Science Board Task Force
on
Defensive Information Operations

Panel Report on Information Assurance Architecture

REPORT OF FINDINGS,
DISCUSSION/OBSERVATIONS
AND RECOMMENDATIONS

TABLE OF CONTENTS

Executive Summary 1

Chapter 1. Introduction 3

Chapter 2. Vision 7

Chapter 3. IAA Framework 17

3.1 IAA Reference Model 17
3.2 System Architecture 22
3.3 Operational Architecture 28
3.4 Technical Architecture 30
3.5 Metrics 33
3.6 Wireless 35
3.7 Summary of Findings 35

Chapter 4. "What Might Be Done" Panel Suggestions 41

4.1 The GIG is a Weapon System 41
4.2 Architecture Suggestions 44
4.3 Defense in Depth 49
4.4 Metric Suggestions 60
4.5 Wireless Suggestions 66
4.6 GIG IA Summary 74

Chapter 5. Recommendations 77

APPENDIX A. Terms of Reference A-1

APPENDIX B. Bios B-1

APPENDIX C. Agendas C-1

APPENDIX D. Acronyms D-1

Page 870 of 3957

Page 871 of 3957

EXECUTIVE SUMMARY

The Information Assurance Architecture (IAA) Panel was tasked to review the implementation of the 1996 Defense Science Board Task Force on Information Warfare Defense recommendations, to identify specific issues associated with information assurance goals of Joint Vision 2020 (JV2020), and to evaluate the adequacy of progress made in achieving these goals. The panel addressed the status of the Department of Defense's (DoD) efforts to establish an IAA framework and standards, and to develop promising IAA techniques. The panel invited representatives from the Services, various agencies, and information technology industries to brief on IA related technologies, trends and market demands. In general, the panel found that significant progress has been made in implementing the 1996 DSB recommendations, but critical issues need to be resolved in the context of JV2020.

The ability to achieve information superiority is the pacing item in realizing the goals of JV2020. The Global Information Grid (GIG) is the underlying infrastructure that will support information superiority. The panel believes the key to success is in implementing a standards-based, metric-driven, end-to-end integrated global information grid. The GIG will incorporate near-term information technologies to globally interconnect information capabilities, associated processes and personnel. Further, the GIG must exploit technologies, standards and architectural frameworks based on commercial information technologies (IT). The panel believes that the implementation of the GIG, in the context of JV2020, is one of those significant events that occur once every decade or two, and that how it is managed and architected will have a major impact on DoD for the next decade or more.

The panel argues that the GIG should be viewed as a weapon system since it leads to information/decision superiority and therefore will be attacked by our adversaries. However, unlike traditional weapons systems, the DoD does not own the critical elements of the GIG; it will be built from rapidly evolving commercial-off-the-shelf (COTS) components. In addition, the GIG can be more readily attacked due to low cost of entry for attackers and the fact that attack attribution is difficult.

The GIG today comprises the Non Secure Internet Protocol Router Network (NIPRNET), Secure Internet Protocol Router Network (SIPRNET), Joint Worldwide Intelligence Communications System (JWICS) and Service Tactical Command, Control, Communications, and Intelligence (C3I) systems. The panel found that each service is pursuing its own architectural implementation of the GIG and observes that, absent an office of primary responsibility, the GIG will not achieve Joint Weapons Systems status. The panel identified a set of DoD strategies for providing information assurance for the GIG: (1) pursue a disciplined implementation through consistent architectural framework; metrics; and commercial standards; (2) segment the communities, i.e., separate DoD from the general public and segment by classification and enclaves; (3) counter denial-of-service by segmentation, redundancy, diversity, and a restricted set of Internet access points; and (4) establish fine grained access control of computing and communication resources.

Page 872 of 3957

In addition to developing a strategy, the panel made several assumptions. The first is that the DoD will establish the Internet protocol (IP) as the convergence layer for the GIG. The second is that the Defense Information Infrastructure will migrate from Asynchronous Transfer Mode (ATM) to Internet Protocol (IP) services. The third is that the DoD will fully execute its Public Key Infrastructure/Public Key Enabler (PKI/PKE) strategy.

The panel recommended an Information Assurance (IA) reference model protocol stack that is almost consistent with the reference models used by International Organization of Standardization (ISO) and by the Transmission Control Protocol/Internet Protocol (TCP/IP) community, and is based entirely on commercial protocols. The panel also recommended a standard defense-in-depth approach that spans common user networks, command enclaves, and workstations or servers. It is recommended that all common user networks (SIPRNET, JWICS, and NIPRNET) adopt this approach, which has the feature of providing significant barriers to insider attacks.

The panel observed that the GIG includes commercial as well as DoD wireless connectivity and that the best protection for all wireless systems is at the physical layer. DoD has developed and deployed techniques for such protection; however, commercial wireless systems do not offer equivalent capabilities. Furthermore, both military tactical internets and commercial wireless systems depend on higher-level network processing (routers, user location databases, etc.) that are largely unprotected. Protection needs to be extended to these facilities to ensure robust mobile wireless operations. It will be essential to establish a consistent engineering approach for wireless use in the GIG.

The panel observed that metrics for information assurance are an important and inadequately addressed need. Researchers, designers, vendors and operators of information systems need a broad spectrum of metrics to achieve their respective objectives. The panel observes that it will be necessary to develop different sets of metrics for technical-, systems-, and mission-level evaluation. For instance, mission-level metrics would involve time to complete a mission, targeting and situation awareness accuracy. System-level metrics might include system downtime and response time to neutralize attacks. Technical-level metrics might include probability of attack detection vs. false alarms. The panel also observes that an architectural environment/testbed will be required for development of metrics and measurement of system performance in DoD-relevant operational scenarios and related information traffic flows. To achieve these objectives the testbed must facilitate collaboration and participation of research and development, evaluation and operational communities (services and agencies).

Based on the above, the panel made four principal recommendations: 1) the Secretary of Defense (SecDef) should establish a board of directors to provide oversight of the GIG (Deputy SecDef [Chair], Under Secretary of Defense for Acquisition, Technology & Logistics, VCJS, ASD/CSI, DCI); 2) the Board should establish an Executive Director and systems engineering organization to implement the GIG; 3) the executive director should be given responsibility for implementing the GIG based on a consistent systems architecture; and 4) the executive director should establish a GIG IA research and development (R&D) testbed to meet the need to continually test, evaluate, and evolve the GIG.

By implementing the recommendations and pursuing the layered architectural strategy, vulnerability to attack will be significantly reduced and attribution capabilities will be increased.

Page 873 of 3957

CHAPTER 1. INTRODUCTION

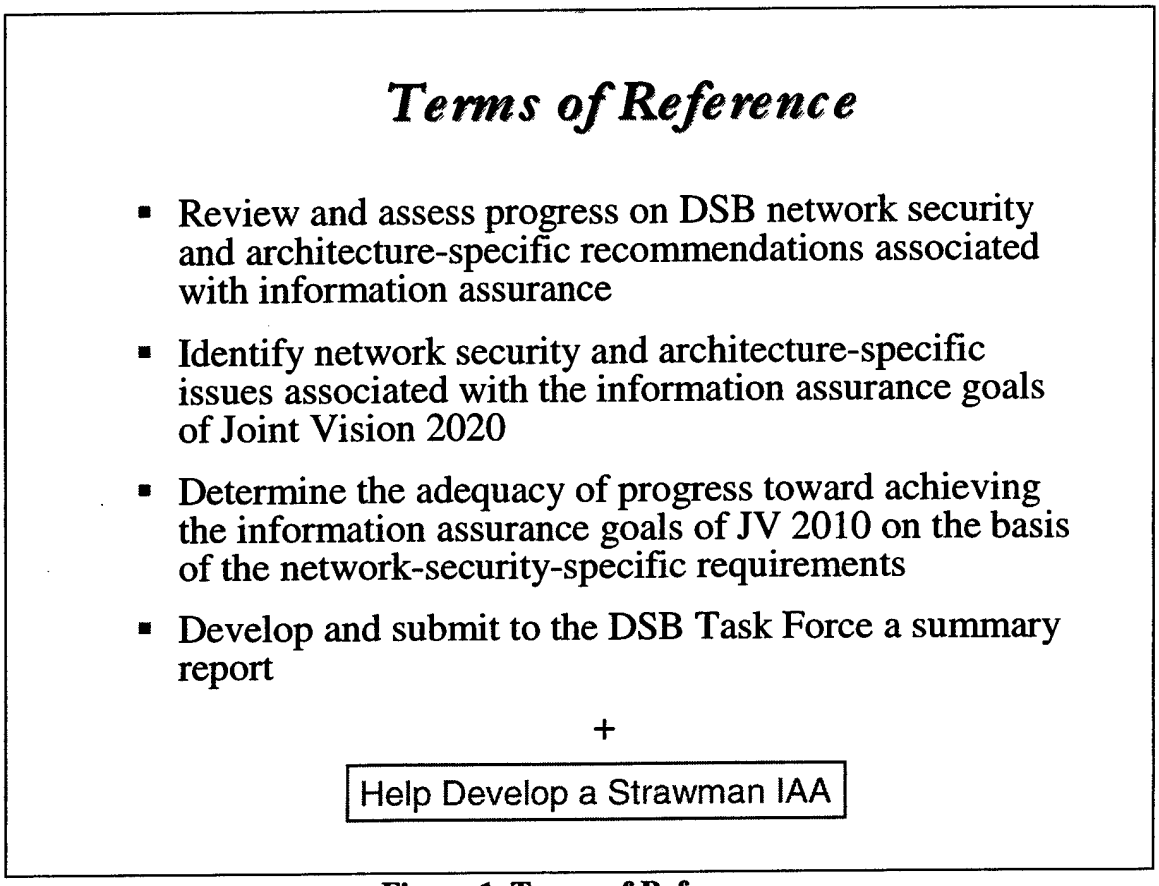


Figure 1. Terms of Reference

The Information Assurance Architecture (IAA) Panel was asked to review progress made by DoD toward implementing the recommendations made by the Defense Science Board's (DSB) 1996 Study on Information-Warfare-Defense (IW-D).[1] The panel was asked to specifically focus its analysis on those recommendations related to issues associated with DoD information infrastructure architecture initiatives.

At the first meeting of the IAA Panel, the members decided to extend their tasking to include a review of the status of DoD's efforts to establish an IAA framework. The panel felt that such a framework is a necessary foundation for deploying, over time, a DoD information infrastructure that provides a reasonable and understood degree of IA. The panel reviewed the following DoD information-system architectural components: (1) operational architecture (OA), (2) system architecture (SA), and (3) joint technical architecture (JTA). For purposes of IA, the panel added to this triumvirate the need for a reference model for IA – a model that sets a high level perspective of where and how IA services should be provided within the DoD information

[1] Reference 1996 DSB Study "Tactics and Technology for 21st Century Military Superiority"

infrastructure. The need and utility of an IA reference model was predicated upon the fact that such a tool exists and is used in the private sector. We sought to determine if a parallel was developed within DoD as part of its architectural framework for IA. The panel's Terms of Reference (TOR) are provided in Figure 1.

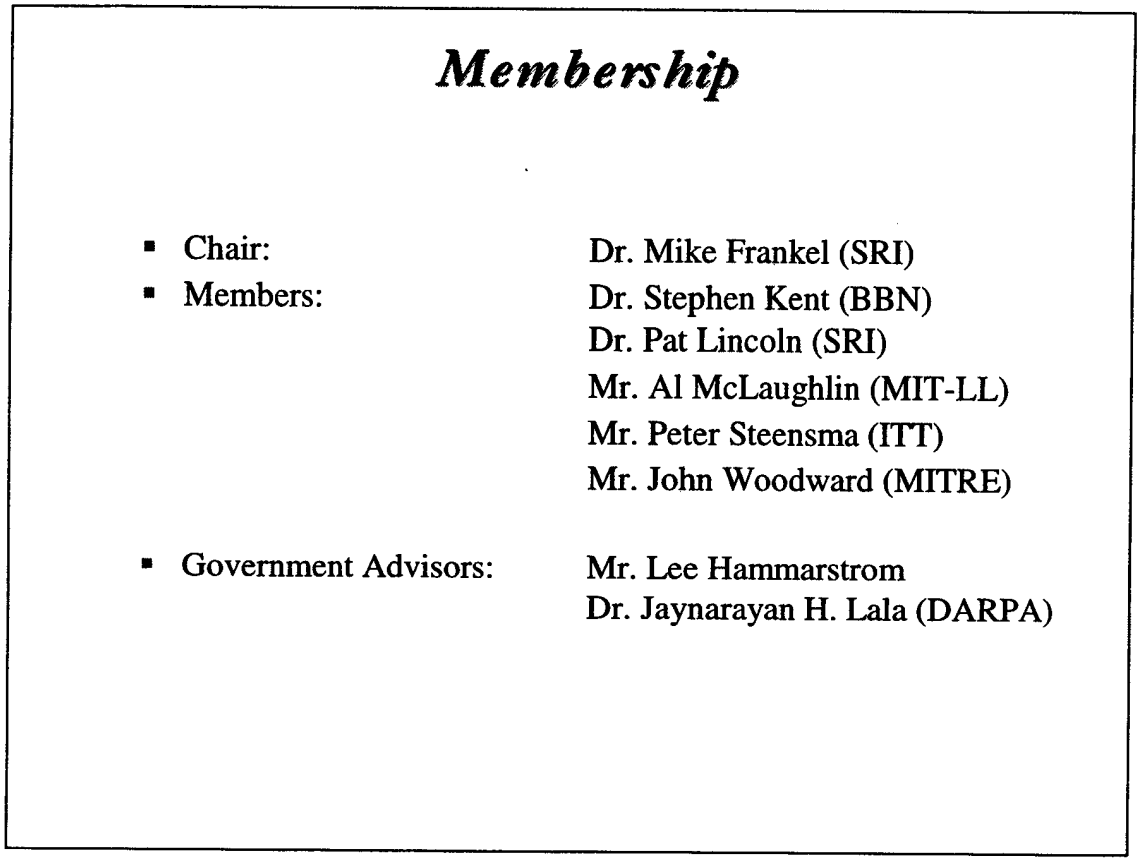


Figure 2. Panel Membership

The members of the IAA Panel who undertook the challenge of addressing the TOR are listed in Figure 2. The members include internationally recognized experts in IA. Their collective expertise included a deep understanding of IA technologies, systems and concepts for both wired and wireless information systems. This understanding included both commercial practices as well as DoD IA implementation and research/development initiatives.

The panel was supported by two government advisors who brought complementary backgrounds and knowledge regarding DoD IA initiatives. One advisor has been a key member of the DoD community architecting, developing, and deploying DoD IA technology for use by DoD Services and Agencies; the second individual brought an understanding of the present DoD IA Science and Technology (S&T) programs.

Brief biographies of the IAA Panel members are provided in Appendix B. Relevant IA backgrounds and experience are noted therein.

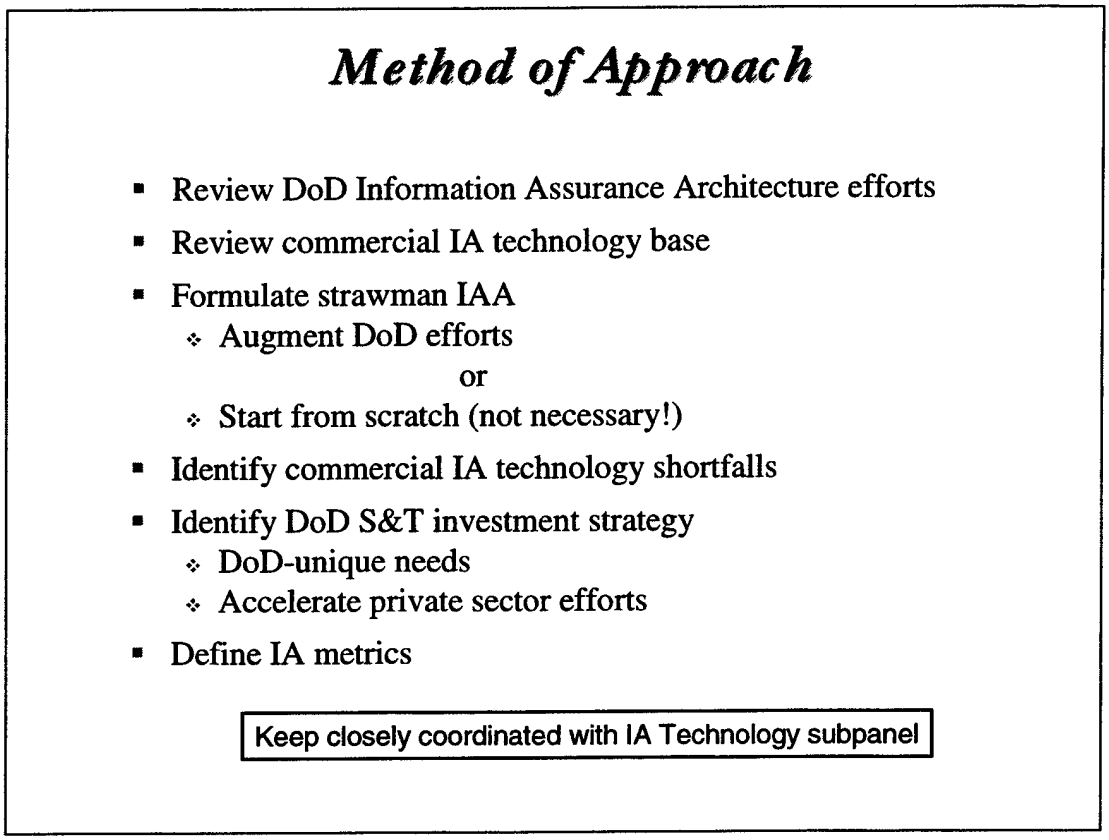


Figure 3. Method of Approach

The panel's method of approach for addressing its TOR was to invite DoD representatives from the various organizations supporting DoD IAA programs to brief the panel. Representatives from Office of the Secretary of Defense (OSD), the Services, and Agencies were selected. In addition, representatives from the private-sector information technologies (IT) industry were invited to brief the panel on IA-related technologies, trends, and market demands. Because DoD's information infrastructure, including IA elements, is highly dependent on the private-sector offerings, the panel felt that understanding the needs, goals, and IA architecture frameworks from both perspectives was critical to formulating the panel's findings and recommendations.

Based on this dual track assessment, the panel provided inputs to its companion IA Technology Panel. These inputs were intended to help identify DoD IA requirements for which the private sector would not necessarily provide solutions; thus, a DoD Science and Technology (S&T) investment would be appropriate.

Finally, the panel noted that to measure progress in achieving adequate IA for DoD's information infrastructure, metrics are necessary. At the outset, the panel realized that the definition and development of IA metrics within DoD has only started. The panel, therefore, decided to make IA metrics a key part of its deliberations, as noted in Figure 3.

Meeting Schedule/Planned Topics

2000	Briefings Received	Subject
Feb 22-23	11	Kick-off and IA Service Overviews and Threat Briefings
March 27-28	9	Panel Chairs Outbrief Progress and DoD requirements
April 19-20	15	Joint Vision 2010-2020, DARPA Initiatives, Adequacy of DoD architectures capable of meeting forecasted service and joint requirements
May 24-26	8	DSB Quarterly, DIO Panel briefings to DSB Members. Briefings from Industry and DARPA perspectives.
June 13-14	7	IA metrics, security standards, briefing on Chessmaster.
July 12-13	2	Network information assurance protection measures and Common operating environment. Present findings, develop recommendations and write draft report.
August 7-18	0	DSB Summer Study, final report.

Figure 4. Meeting Schedule

The panel was formed in February 2000 and conducted its business over a period of six months. The first several meetings were dedicated to receiving briefings and the latter to panel discussions and formulation of the findings and recommendations provided in this report.

As noted in Figure 4, a total of 52 briefings were received covering the topics and organizations noted therein. The major themes for each of the six meetings held are also noted in the figure. The specific briefings and briefers presented are provided in Appendix C.

The briefings and the backgrounds of the panel members provided the contextual and technical information that formed the basis of the findings and recommendations provided herein.

CHAPTER 2. VISION

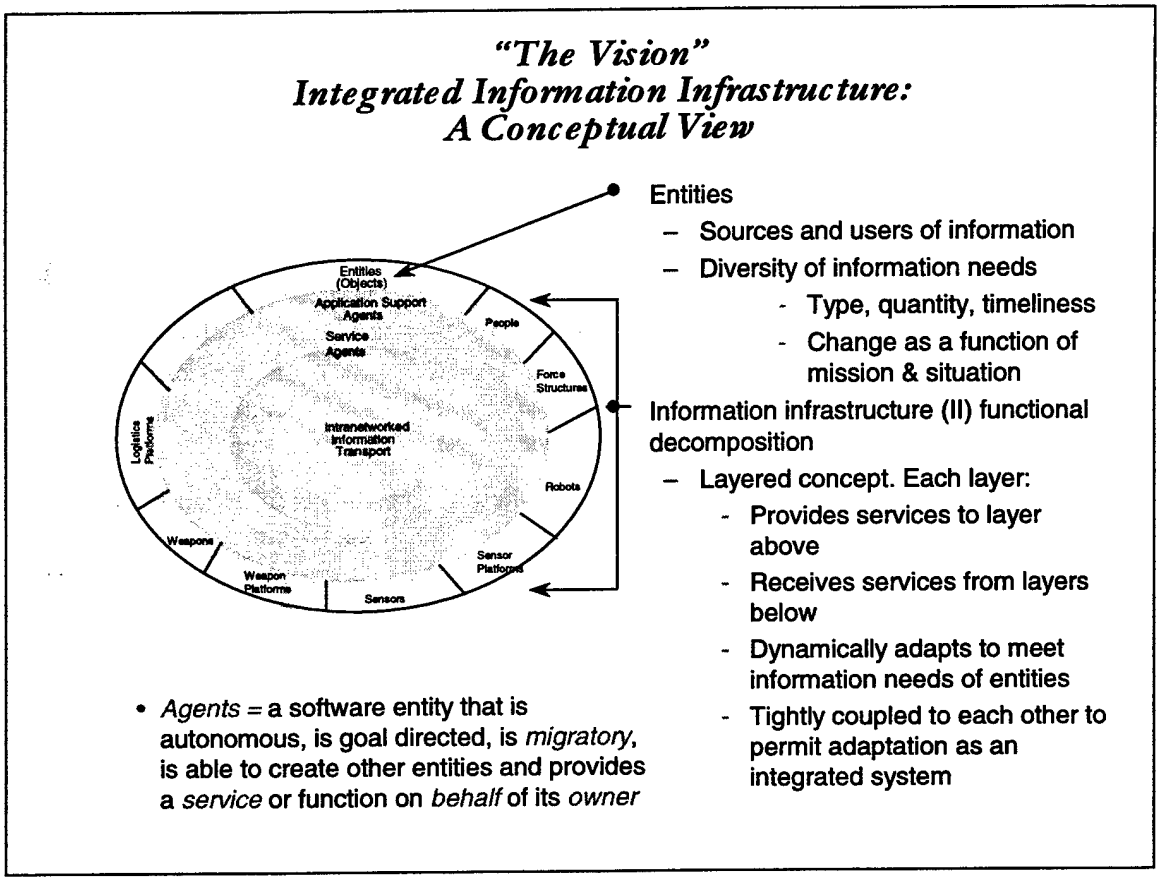


Figure 5. III Vision

In prior DSB studies, a vision, called the Integrated Information Infrastructure (III), was developed for DoD[2]. This vision, as discussed below, has become the foundation within DoD for many of its information infrastructure initiatives today. The vision sets goals and directions for DoD-wide information services that will come about through the exploitation of private sector information technology (IT), to include associated IA technologies. The III then sets both a long-term vision and a road map for the evolution of the DoD infrastructure. Figure 5 provides a conceptual view of the III.

The ability to achieve information superiority is the pacing item in realizing the goals of Joint Vision 2020. The inadequacies of current service information infrastructures prevent commanders from realizing the full benefit of the current family of intelligence, surveillance, and reconnaissance (ISR) systems – space-based, airborne, or surface – much less profiting from advances in sensors and weapons. Because of uncertainties whether crucial information will be available when needed, commanders are driven to develop unique, local-only reconnaissance,

[2] Reference 1996 DSB Study "Tactics and Technology for 21st Century Military Superiority"; 1998 DSB Summer Study "Joint Operations Superiority in the 21st Century"; 1999 DSB Summer Study "21st Century Defense Technology Strategies"

surveillance, and target acquisitions (RSTA) systems. Overall, this tendency has resulted in redundant investment in, and proliferation of, "stovepipe[3]" communication and sensor systems.

Increasingly, the armed forces are shifting to an operational concept wherein surveillance and targeting sensors are separated physically from the command node location, which in turn may be remote from the weapons launch platform. In the case of air platforms, for example, no longer will the sensors, commander (pilot), and weapons necessarily be collocated in a single aircraft. Further, third party targeting data sources and weapons magazines are proliferating. Examples of this evolving trend appear in such concepts as forward pass, cooperative engagement capabilities (CEC), the arsenal ship, and the transfer of tactical situation data derived from a variety of off-board sources directly into cockpits.

This evolution promises major improvements in the tactical flexibility and combat effectiveness of forces. The realization of this promise is not without challenges, however, because the operational concept is inhibited by the inadequacy of the traditional military communication and information-services infrastructure as well as continuing interoperability problems between military services and between systems within a given service.

To realize the potential benefit of this new concept, our future information infrastructure must be capable of reliable transmission, storage, retrieval and management of large amounts of data. Today all systems are segmented into communications links, computers, and sensors that in turn are stovepiped to support specific functions (i.e., intelligence, logistics, and fire control). Furthermore, these component entities are now constrained by a lack of (1) the bandwidth necessary for high-resolution imagery transfer; (2) the processor capacity needed for target recognition and interpretation; (3) memory sufficient to handle massive amounts of archival data; and (4) software to search the many data repositories quickly in order to provide commanders with tactical information in a timely manner. These constraints are magnified by difficulties in integrating a myriad of legacy information systems with newly developed, service-unique stovepipe and joint systems. These limitations can be overcome, and the full capability of joint forces realized, if we set as our goal the integration of all military C4ISR[4] systems into a ubiquitous, flexible, interoperable C4ISR system of systems – the Integrated Information Infrastructure.

The Integrated Information Infrastructure must meet several key requirements if it is to enable future combat operations to support a wide spectrum of missions, threats, and environments.

As stated in Joint Vision 2020, a military force must be able to receive or transmit all of the information it needs for the successful and efficient prosecution of its mission, from any point on the globe, in a flexible, adaptive, reconfigurable structure capable of rapidly adapting to changing operational and tactical environments. The information infrastructure must support this need, while allowing force structures of arbitrary composition to be rapidly formed and fielded. Furthermore, the infrastructure must adapt to unanticipated demands during crises, and to stress imposed by adversaries.

---

[3] "Stovepipe" systems are those designed with one application or uses in mind without consideration of interfaces with other systems.

[4] C4ISR: Command, control, communications, computers, and intelligence surveillance and reconnaissance.

The infrastructure must allow information to be distributed to and from any source or user of information at any time: its architecture must not be constrained to support a force-structure (enterprise) hierarchy conceived *a priori*. Most importantly, the information and services provided to an end user through the infrastructure *must be tailored to the user's needs, and be relevant to the user's mission, without requiring the user to sort through volumes of data or images*.

The information infrastructure must include multimode data transport including landline, radio, and space-based elements. All of these media must be integrated into a ubiquitous, store-and-forward data internetwork that dynamically routes information from source(s) to destination(s), transparently to the user. This data transport segment of the infrastructure must be self-managed, be adaptive to node or link failure, and provide services to its users based on quality-of-service (QoS) requests. These services include bandwidth, latency, reliability, precedence, distribution mechanisms (point to point, point to multipoint), and the like.

The infrastructure interface will link the user to a distributed processing environment that includes all types of computers situated at locations appropriate to their needs for power, environment, and space. This distributed computing environment will be integrated via the transport component of the infrastructure, thus enabling these processors to exchange data dynamically, share computation loads, and cooperatively process information on behalf of and transparent to the user.

The infrastructure should be an adaptive entity that integrates communication systems, computers, and information management resources into an intelligent system of systems. Each component of the III will exchange state information with each other, in order to enable the entire infrastructure to adapt to user requirements and any stresses imposed on the network by an adversary. This adaptability will also enable the infrastructure to change its scale as necessary to support force structure(s) of arbitrary size, or to incorporate new processing, network, and communication technologies as they are developed. Thus, this infrastructure is a scaleable computing environment.

The information infrastructure must provide tailored information services to diverse users ranging from a single person to a collection of people, sensors, and/or weapons by means of intelligent agents – software entities, under the general control of the user, that are goal-directed, migratory, and able to create other software entities, and provide services or functions on behalf of the user.

Each user will be served by one or more intelligent software agents that *proactively* provide and disseminate appropriately packaged information. These agents will perform such functions as fusing and filtering information and delivering *the right information to the right user at the right time*. They must be proactive in the sense that they are aware of the user's situation and needs, and can provide information relevant to those needs without a specific user request.

These agents will multiply the personnel resources available to combat units by gathering and transforming data into actionable information to support unit operations, just as unit members would have to do, were the software agents not provided. Warfighters will therefore be freed of routine chores in favor of actual operations.

Page 880 of 3957

To the maximum extent feasible, the infrastructure's transport layer will take advantage of commercial technology and networks, by utilizing open-systems standards and protocols, and will minimize the use of service- or function-unique hardware and software. For applications where military-unique capabilities (such as antijam, low probability of intercept, spread-spectrum waveforms and the like) are required, military products will be developed or adapted to interface with the overall architecture.

We must set as a goal the realization of the III vision in an evolutionary manner. As we succeed, we will enable, over time, the following military capabilities:

- Geographic separation and functional integration of command, targeting, weapons delivery, and support functions
- Support for split-base operations, force projection, information reach back, combat, and force protection for units large and small
- Common situational understanding, common operating picture, and informed and rapid decision making for joint forces
- Enhanced operational flexibility for commanders at all levels
- Reduced logistics footprints in immediate combat areas
- Full exploitation of sensor, weapon, platform and processing capabilities
- Real-time or near real-time responsiveness to commanders' requests for information, fire support, and urgent logistics support

The first phase for realizing the III is the implementation of the Global Information Grid (GIG). The GIG will incorporate near-term information technologies to provide the warfighting capabilities noted above. The GIG will, over time, evolve into the longer-term vision for the III. As we proceed to implement and secure the GIG, we must keep the evolution toward the III in mind.

Page 881 of 3957

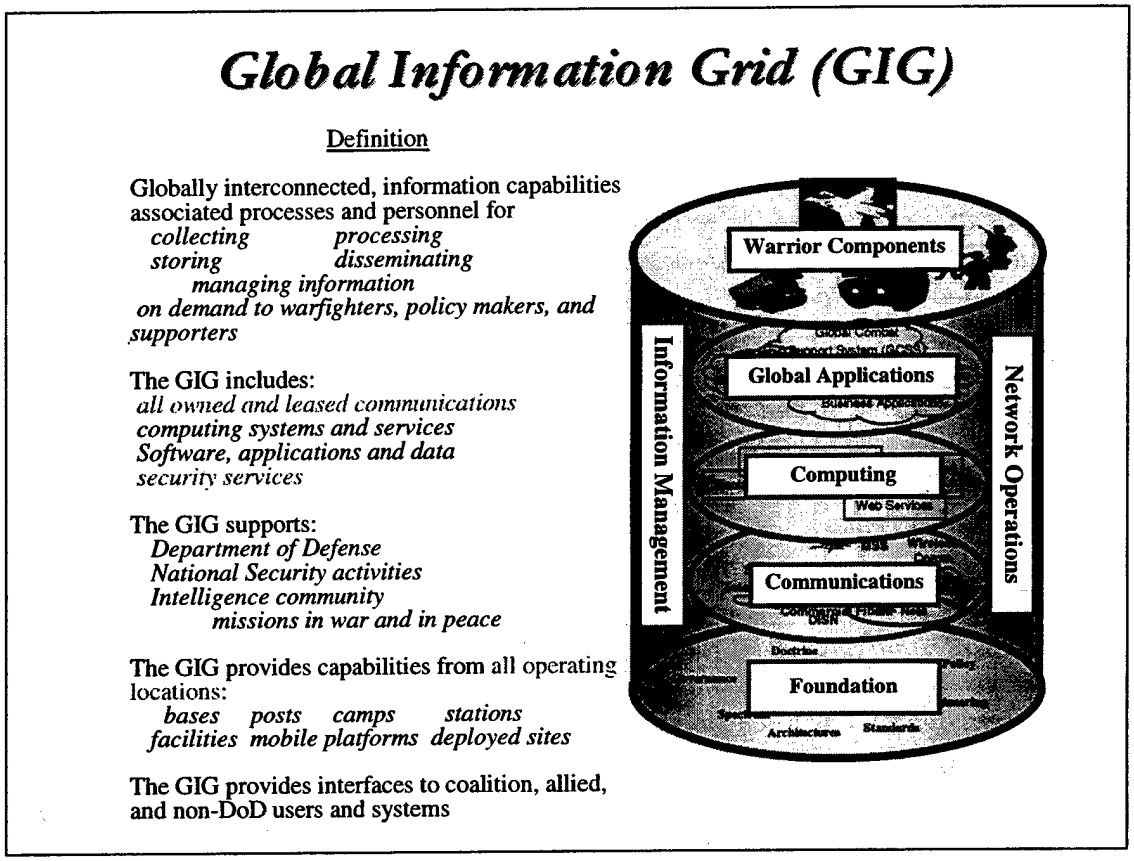


Figure 6. Global Information Grid

The III vision was formulated in 1996. It, along with similar visions such as Network Centric Warfare (NCW) and the Advanced Battlefield Information System (ABIS), has helped DoD formulate and articulate a vision for a near-term version of the III. This near-term vision is shown in Figure 6. The GIG is intended to be the means by which information superiority (IS), as envisioned in the Joint Vision 2020, is achieved. The following quotes define the GIG.

> *The GIG is the vision of the Assistant Secretary of Defense for Command, Control, Communications, Computers, and Intelligence (ASD/C3I) for achieving IS. The GIG is focused on the warfighters' needs for IS plus the critical concerns of frequency spectrum and improving the management of the information infrastructure investment along with the coevolution of Doctrine, Organization, Training and Education, Materiel, Leadership, Personnel, and Facilities (DOTMLPF).* [5]

The September 22, 1999, Office of the Assistant Secretary of Defense Director, Command, Control Communications and Intelligence Systems (ASD/C3I) memorandum, Subj: Global Information Grid, defines the Global Information Grid (GIG) as:

---

[5] Reference: *Enabling the Joint Vision*, The Joint Staff, C4 Systems Directorate, Information Superiority Division (J6Q), Pentagon, Washington, D.C., March 2000

The globally interconnected, end-to-end set information capabilities, associated processes and personnel for collecting, processing, sorting, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operations locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). GIG provides interfaces to coalition, allied, and non-DoD users and systems.

The GIG's interoperability builds upon the existing Defense Information Infrastructure (DII) Common Operating Environment (DII-COE). The building blocks of Joint Technical Architecture, Joint Operational Architecture, Joint Systems Architecture, a shared data environment, the migration of legacy systems, and adherence to commercial standards provide the necessary structure for the GIG.

The key to achieving information superiority lies in implementing *a standards based, metric-oriented*, end-to-end integrated Global Information Grid. The concept of IS may be situational but the GIG, which will implement IS, is quantifiable. Important initiatives to implement the GIG are described in the following sections.

The emphasis on the standards-based and metrics-oriented aspect of the GIG description is believed by the panel to be key to its being successfully deployed, used and evolved to continuously meet DoD needs.

Page 883 of 3957

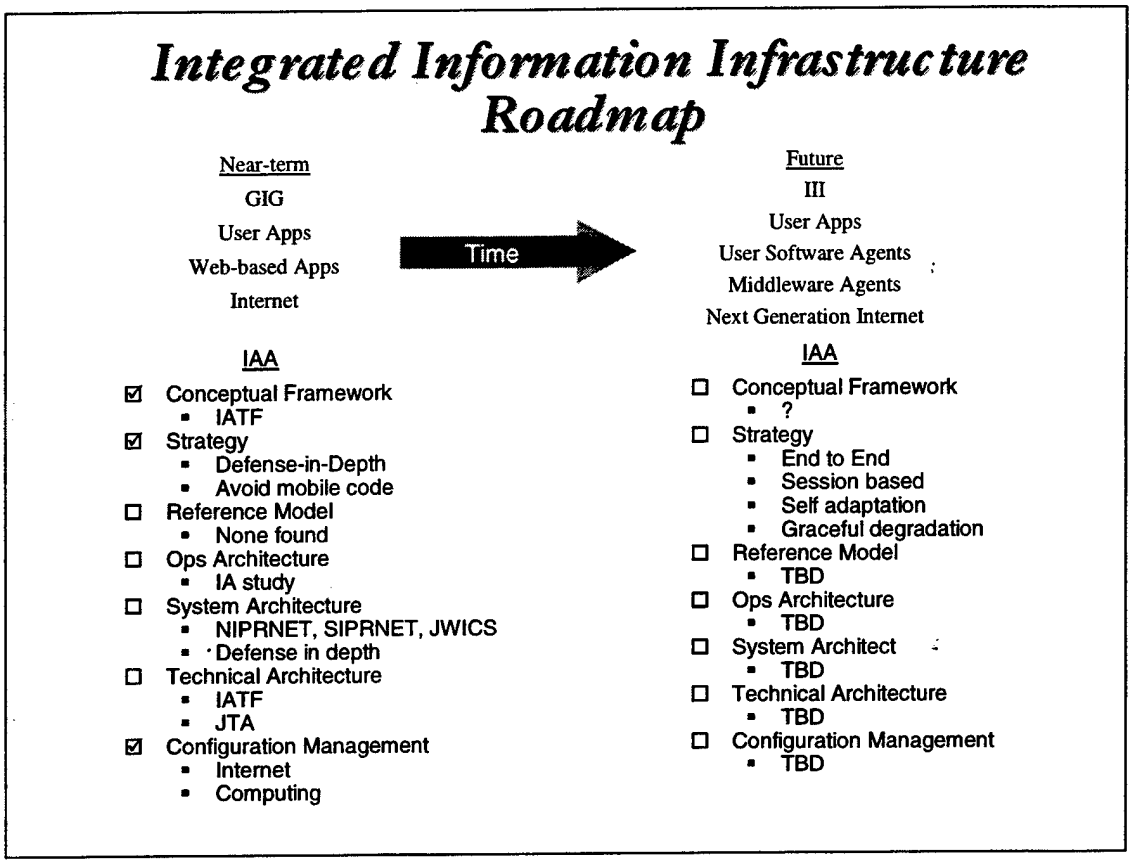


Figure 7. III Roadmap

The evolution of today's GIG into the III envisioned by the DSB requires that the GIG exploit technologies, standards and architectural frameworks based on information technologies (IT). It is within the private sector that significant investment in and rapid evolution of IT is occurring. DoD must position its evolving GIG to take advantage of this technological evolution.

Figure 7 shows the evolution of the GIG. As noted, its foundation architectural framework must be sufficiently flexible to allow transition from more conventional relational/procedural-based information services to services supported by intelligent mobile code (software agents). Keeping this evolution in focus today will help DoD augment the GIG when necessary as well as help to guide DoD's science and technology (S&T) investments over the next several years.

Page 884 of 3957

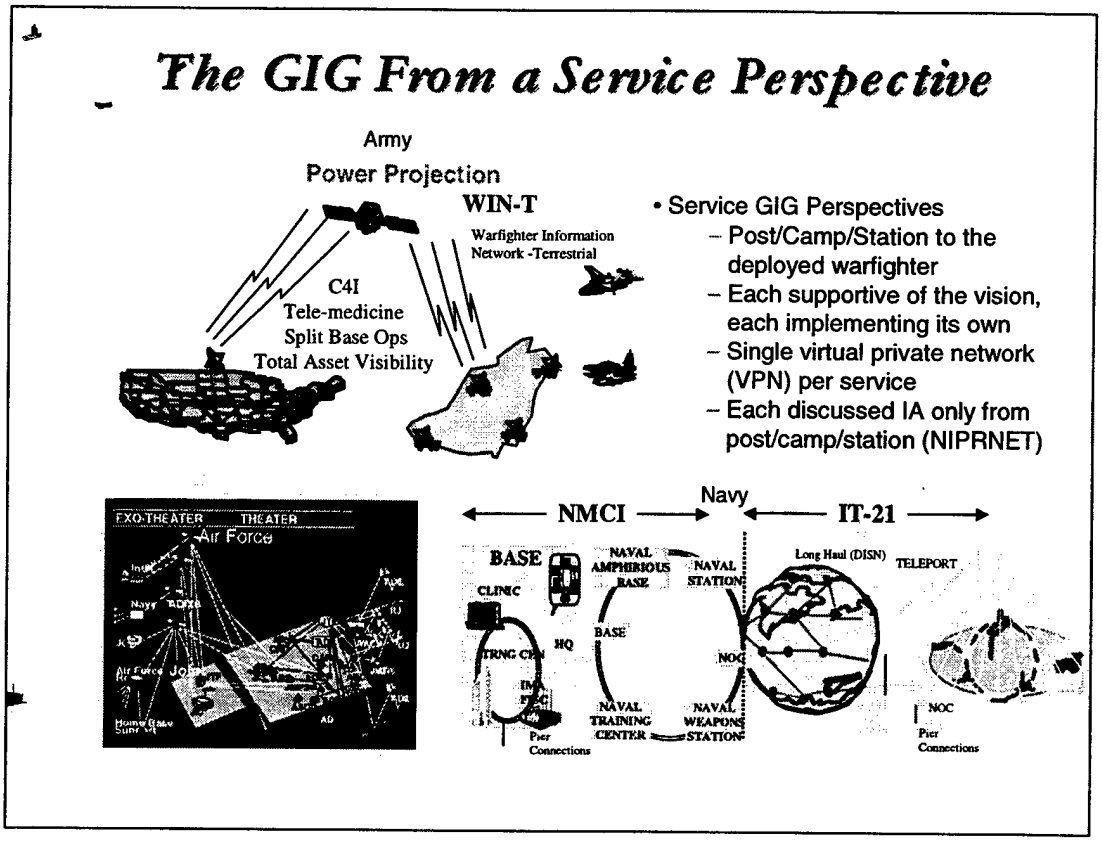


Figure 8. The GIG from a Service Perspective

In addition to hearing the OSD perspective, plans, and strategy for the GIG, the panel heard the service views on GIG. In each case, as shown in Figure 8, the Services presented an overview of the GIG that was consistent with the notion of an integrated infrastructure connecting post, camp, or station to deployed forces. The infrastructure, from each service's perspective, would support warfighter applications, combat service functions, and business functions for each of its user communities wherever they are situated.

The panel noted, though, that each service presented and talked to *its* implementation of a global information grid – none presented a concept of a single, joint, DoD-wide GIG which would be leveraged and used for its information needs. The panel did not hear how the services' need for various levels of security (unclassified through top secret) would be supported in their respective implementations. In fact, the panel noted that the primary focus of the Services' presentations was supporting post/camp/station unclassified information services. The panel also heard that each service anticipated having wireless access media integrated into its respective segment of the GIG. This wireless media is necessary to support our highly mobile, forward-deployed forces. In addition, the panel noted that wireless point-to-point extensions exist in the "wire-based" (fiber or copper) segments of the GIG that support the interconnection of the post/camp/station locations. These wireless media need to be considered when one addresses IAA for the GIG. This issue, not discussed in DoD briefings, is addressed more fully in subsequent sections of this report.

Page 885 of 3957

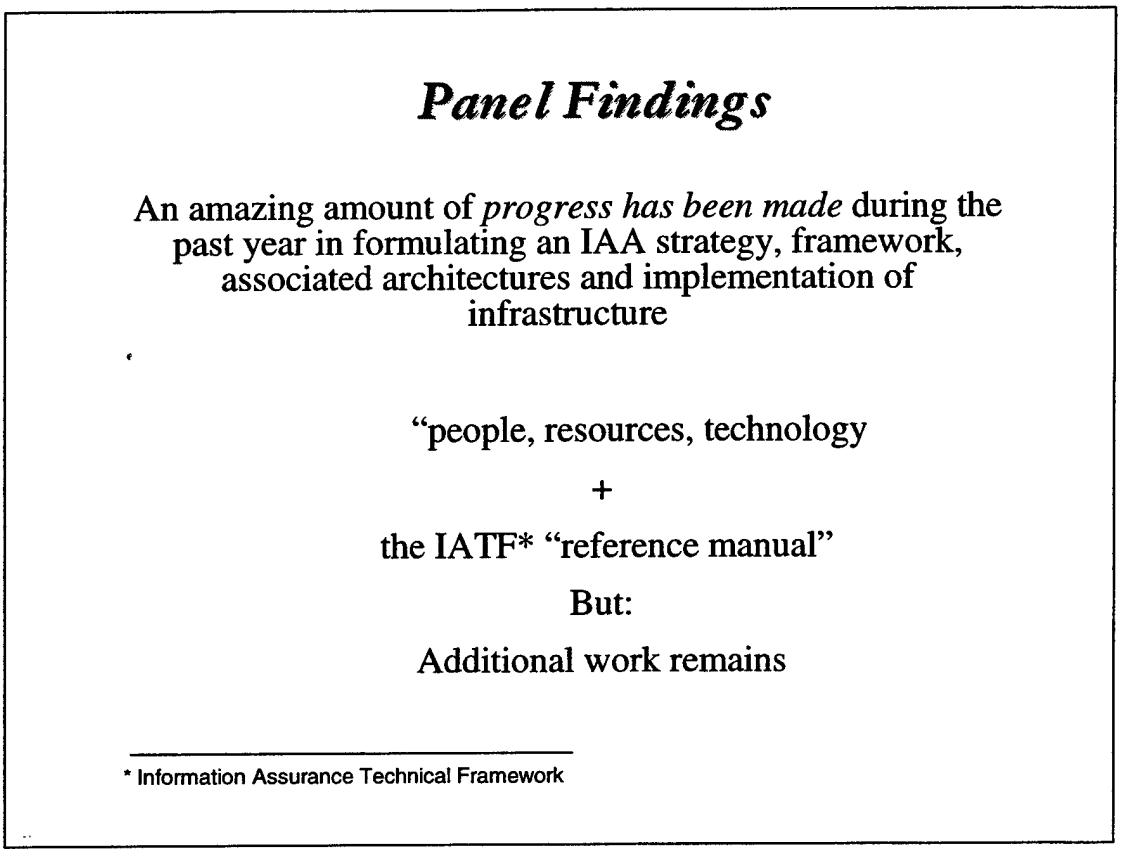


Figure 9. Panel Findings

From the DoD and service-related briefings, the panel noted that significant progress has been made in formulating an IAA strategy, framework, and associated architecture and in implementing infrastructure. The IAA Panel noted that significant people, funds and technology have been allocated and deployed toward providing a more robust DoD information infrastructure. This section of our report presents the panel's findings related to this progress.

Page 887 of 3957

CHAPTER 3. IAA FRAMEWORK

3.1 IAA REFERENCE MODEL

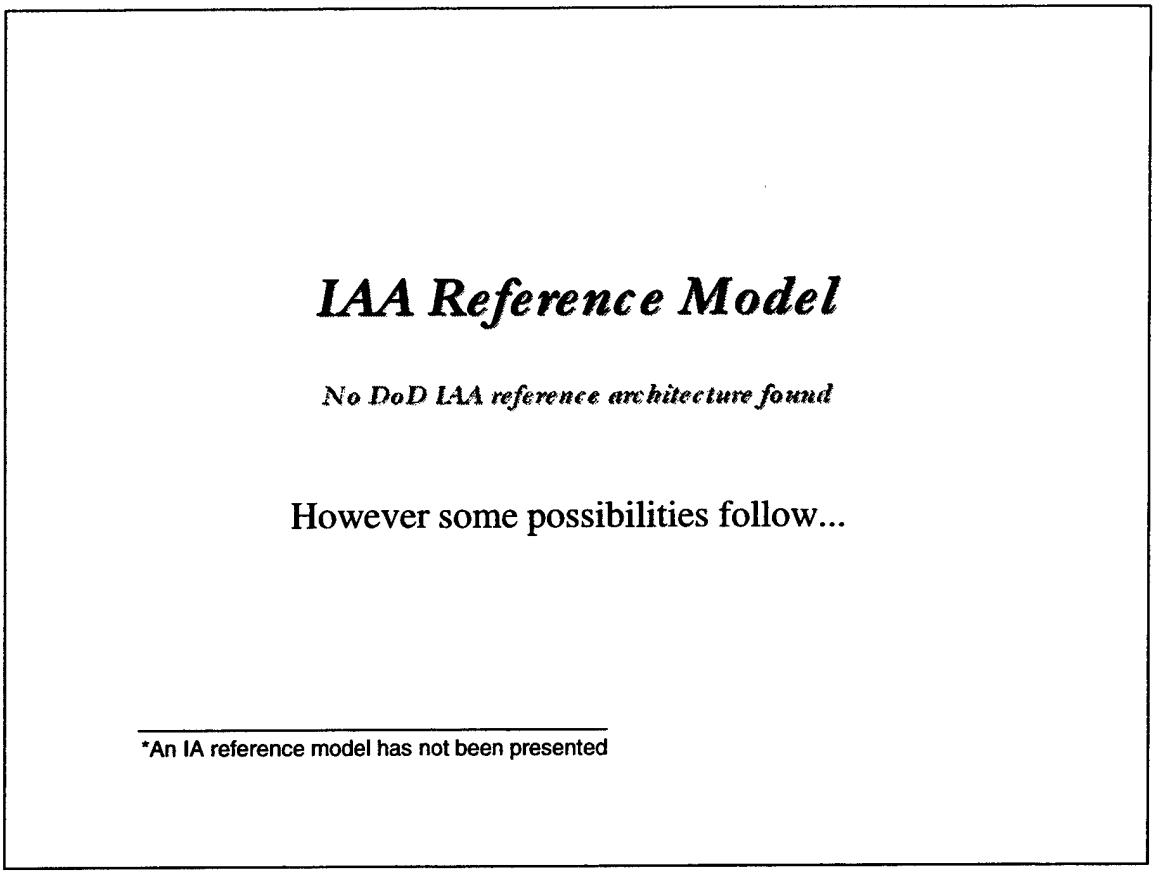


Figure 10. IAA Reference Model

As shown in Figure 10, no single IAA reference model (RM) has been selected or developed by DoD. Such a reference model would help the DoD IA community understand where appropriate IA standards and services are provided within the GIG. Given that a RM has not been selected, the panel noted that various options do exist.

Page 888 of 3957

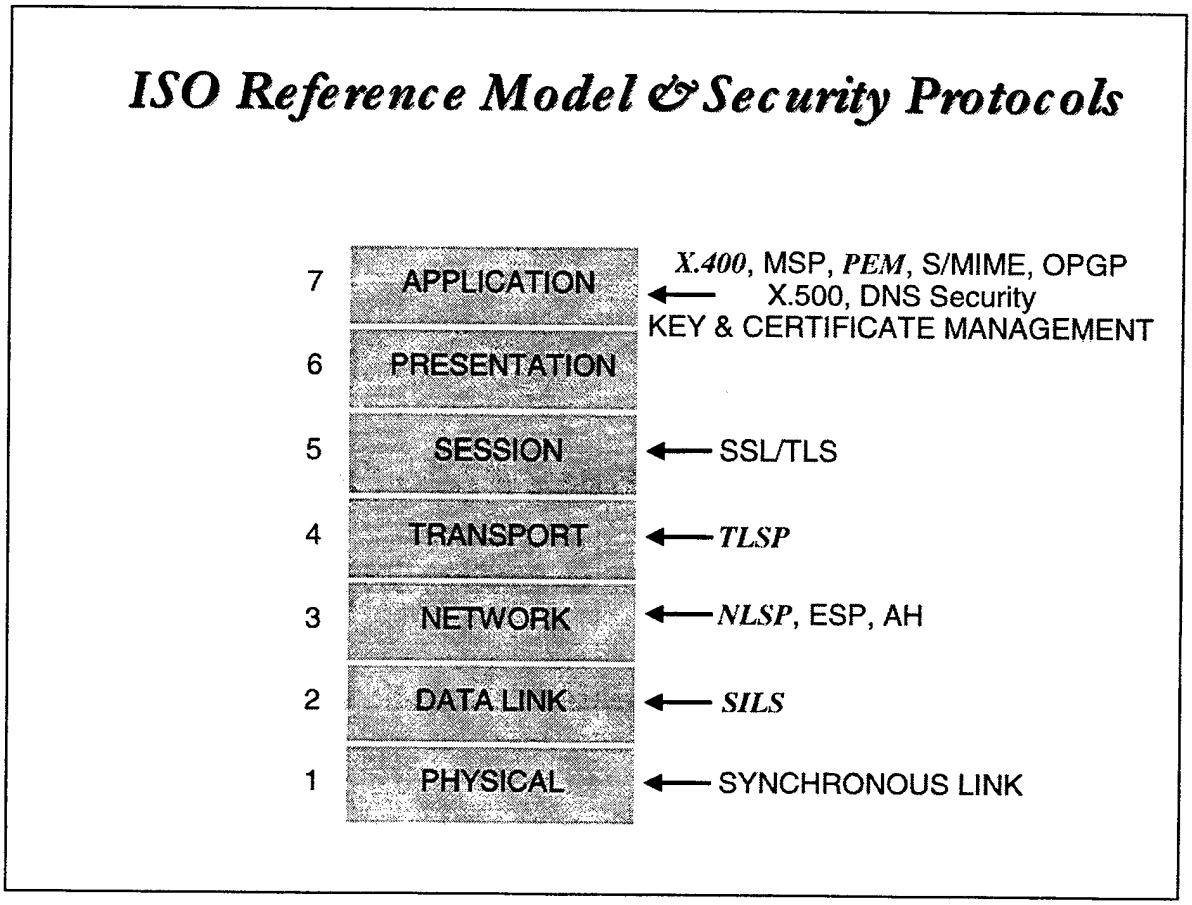


Figure 11. ISO Reference Model and Security Protocols

Figure 11 presents one option. This figure illustrates the International Organization of Standardization (ISO) reference model (ISO 7498) annotated with a mix of International Telecommunications Union (ITU-T) (see ISO and Consultive Committee on International Telegraph and Telephone [CCITT]) and Internet Engineering Task Force (IETF) security protocol standards. (The term "synchronous link encryption" is non-standard and refers to physical layer cryptographic devices employed on a per-link basis. The term "key and certificate management protocols" is also non-standard.) The standards highlighted in *italics* are obsolete, either superceded by newer standards or never adopted by vendors and integrated into products.

The protocols noted in Figure 11 include:

- Standard for Interoperable LAN Security (SILS), Institute of Electrical and Electronics Engineers (IEEE) 802.10
- Network Layer Security Protocol (NLSP), an ISO protocol
- Encapsulating Security Payload (ESP) and Authentication Header (AH), Internet Engineering Task Force (IETF) protocols defined in RFCs 2402 and 2406
- Transport Layer Security Protocol (TLSP), an ISO protocol

- Secure Sockets Layer (SSL)/ Transport Layer Security (TLS); the former is a commercial security protocol, the latter is the IETF version
- X.400, Message Security Protocol (MSP), Privacy Enhanced Mail (PEM) Secure MIME (S/MIME) and Open PGP (OPGP), all are secure e-mail protocols. X.400 is a CCITT standard, MSP is a DoD standard, and PEM, S/MIME and OPGP are IETF standards
- X.500 and DNS Security are directory security standards from the CCITT and IETF, respectively

ISO Reference Model:

Mapping Services to Protocol Layers

Service	Layers 1	2	3	4	5	6	7
Peer Entity Authentication	•	•	Y	Y	•	•	Y
Data Origin Authentication	•	?	Y	Y	•	•	Y
Access Control Services	•	?	Y	Y	•	•	Y
Connection Confidentiality	Y	Y	Y	Y	•	•	Y
Connectionless Confidentiality	•	Y	Y	Y	•	•	Y
Selective Field Confidentiality	•	•	•	•	•	Y	Y
Traffic Flow Confidentiality	Y	•	Y	•	•	•	Y
Connectionless Integrity	•	?	Y	Y	•	•	Y
Selective Field Integrity	•	•	•	•	•	•	Y
Non-repudiation, Origin	•	•	•	•	•	•	Y
Non-repudiation, Receipt	•	•	•	•	•	•	Y

Figure 12. ISO Reference Model

Figure 12 illustrates the mapping of security services (as defined in ISO 7498-2) to the seven layers of the ISO reference model shown in Figure 11. It is extracted from a more comprehensive larger table in ISO 7498-2. The table is intended as a guide for protocol developers, suggesting which security services may be appropriate to offer at which layers. Even without examining each cell in detail, several issues are apparent. The question marks at layer 2 represent a disagreement between ISO and IEEE, which was eventually resolved in favor of the IEEE (re SILS). Layers 3 & 4 offer similar security features. No security services are recommended for the

session layer (5), and little is appropriate for layer 6. Any security service can be offered at layer 7.

Note that the same service may be offered at multiple layers without being redundant, because different layers provide different communication services. So, for example, excellent traffic flow confidentiality can be offered at layer 1, but end-to-end confidentiality requires use of layer 3, 4 or 7.

In the IA reference model recommended by the panel, we propose adoption of standard security protocols at layers 3, 5, and 7. We also emphasize the use of layer 1 (physical layer) security technology (i.e., link encryption or Transmission Security [TRANSEC] for wireless links) to connect DoD network elements.

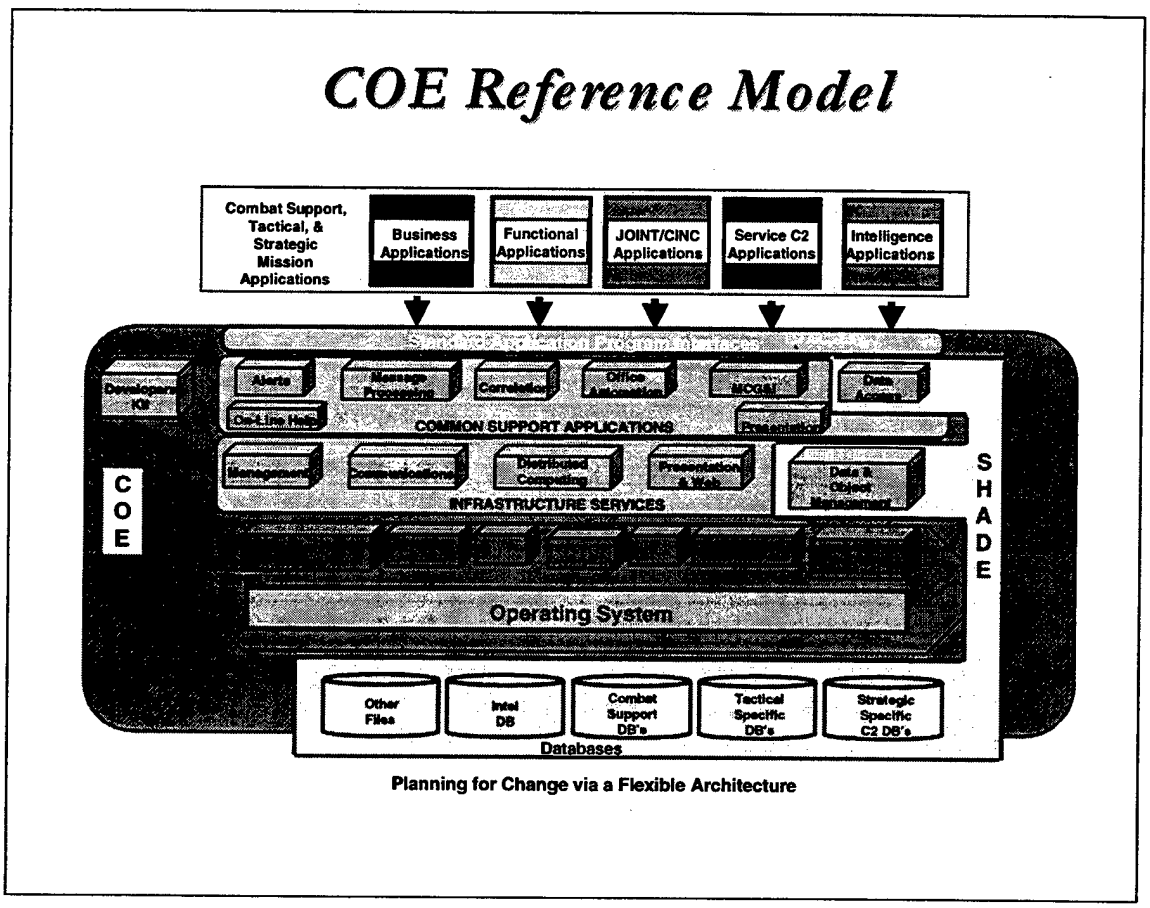


Figure 13. COE Reference Model

A second option for a GIG RM is extending the Common Operating Environment RM (COE) shown in Figure 13. This reference model illustrates the segmentation and layering of code and services in the COE. The panel noted, however, that the COE does not yet address IA (security) services within either its RM or within the run time environments or segmented code libraries it provides to DoD customers. Through discussions with DoD COE representatives, the panel learned that IA extensions to the COE RM, to identify IA services, are presently underway, but there are no near-term plans to add IA (security) code to the COE run time environments. The

panel also noted that the COE is a product-centric framework as opposed to a standards-centric framework that is one of the underlying tenets of the GIG (see discussion in Figure 6).

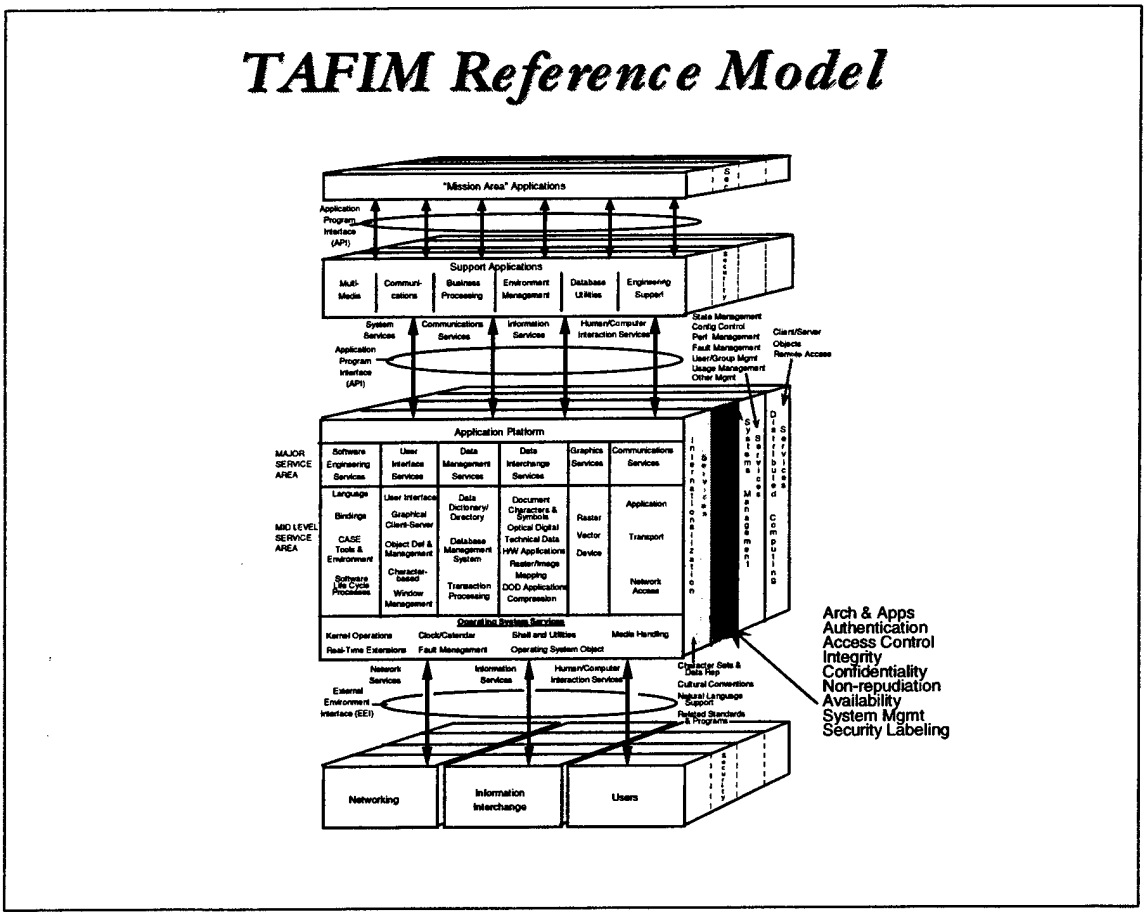


Figure 14. TAFIM Reference Model

A third possible IA reference model is shown in Figure 14. This model comes from an earlier DoD initiative to establish a vision and framework for information systems and services within the Department. This earlier effort, called the Technical Architecture for Information Management (TAFIM), attempted to compile industry and DoD standards, practices and architectures associated with enterprise-scale, distributed, information systems. In this reference model, security services are identified as a backplane of the application platform. The security services provided to the "mission-area" applications include: authentication, access control, integrity, non-repudiation, availability, system management, and security labeling.

The TAFIM RM did not provide sufficient information to allow system implementers to select a specific set of protocols to provide IA services for their users. Because of its lack of specificity the TAFIM has been replaced with more current and focused technical guidance documents (i.e., the Joint Technical Architecture – [JTA]) and run time environments (i.e., the COE).

Page 892 of 3957

Of the three possible IA RMs presented, the panel suggests that DoD select the Open Systems Interconnect (OSI) framework. In the section of this report entitled "what can be done," (see Section 4) the rationale for this suggestion is presented.

3.2 SYSTEM ARCHITECTURE

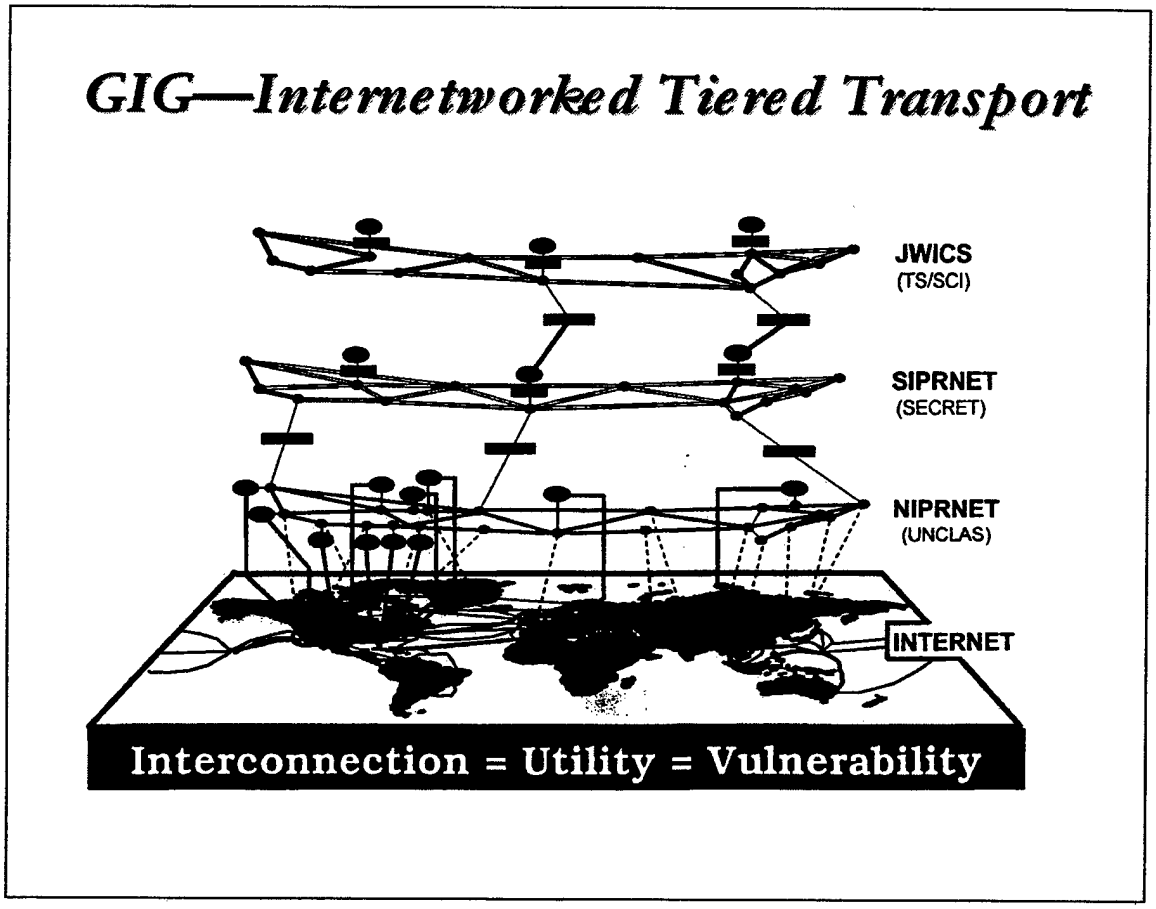


Figure 15. GIG—Internetworked Tiered Transport

As shown in Figure 15, the system architecture for the telecommunications component of the GIG, as it exists today, comprises three virtual, worldwide data networks. These networks include the non-secure Internet Protocol (IP) network (NIPRNET), the secret IP network (SIPRNET), and the Joint World-Wide Intelligence Communication System (JWICS). The NIPRNET, which supports unclassified (but possibly sensitive) DoD data communications, has been part of the private sector World Wide Web (WWW). It is accessible, in principle, by all WWW users and is connected to the packet-switched routing infrastructure (the public Internet) that underlies the WWW. Interconnection points between DoD NIPRNET systems (host, routers, and access points) and the public Internet have been many hundred and mostly unmanaged by DoD.

Recently, DoD has decided to limit these access points to 8 to 11 monitored gateways between a virtual NIPRNET and the public Internet. Additional connection points could be allowed but are planned, at present, to be few in number and carefully controlled by DoD.

The SIPRNET is a secret-high virtual private DoD network. This system uses encrypted links between the routers that connect user sites, to secure transmission of secret data. User sites, and their corresponding competing resources, are all run at secret high. The panel notes that the SIPRNET traffic can (and probably does) transit the same physical transmission links (fiber, copper, and wireless systems) as does NIPRNET traffic – the former being encrypted, the latter being transferred primarily in the clear.

JWICS is also a virtual private network supporting the exchange of Top Secret (TS), Sensitive Compartmented Information (SCI) between user sites. JWICS, similar to SIPRNET, appropriately encrypts information for transmission over the communication links that connect the routers at each user site and transfers this data across the same commercial (and government-owned) transmission facilities used by the NIPRNET. Thus, JWICS, SIPRNET, and NIPRNET are cryptographically segmented virtual private networks (VPNs) that likely share common physical communication media. In the current system, these VPNs are implemented at the physical layer, which offers good security in many respects. Somewhat different features arise if one also creates VPNs at the IP layer, as we discuss later.

The panel was also informed that traffic can flow between JWICS and SIPRNET and between SIPRNET and the NIPRNET via trusted guards. These guards automatically filter the type and quantity of data that flows between these virtual networks. Their use is a risk/benefits tradeoff that has placed user and enterprise value on allowing limited traffic flow of appropriately sanitized information between virtual networks of different classification levels while accepting the risk of having unfiltered information pass the network boundaries or possibly opening covert channels of information flow from the classified to the unclassified communities (possibly by virtue of an insider threat).

Another key aspect of the system architecture suggested by Figure 15 is that all DoD general information resources are on the NIPRNET. Thus, private sector users needing access to this general, public information are required to gain access to the DoD computer servers storing this information. Although DoD has had issues with hackers and malicious entities trying to deface or gain access to their Web sites, the present plan is still to filter access to these sites – yet everyone must still be granted access to this general information at many DoD sites maintaining this information. The DoD is aggressively deploying a defense-in-depth strategy, as discussed in the next figure, but it must still provide and support access to all NIPRNET DoD sites for the general public and those elements of the private sector with which DoD conducts e-commerce. This planned approach makes it harder to design and deploy an effective defense-in-depth approach.

The panel also noted that the GIG is really, today, the aggregation of the JWICS, SIPRNET and NIPRNET virtual private networks. These networks, together, constitute the starting point for the GIG. Consequently, one should think of the SIPRNET as the VPN that provides (secret level) secure data/information transfer from post/camp/station to the "foxhole." Thus, all service secret-level combat mission functions and their supporting computers and communications should be viewed as being integrated into the SIPRNET. Similarly, the NIPRNET VPN should be viewed as the network supporting unclassified but sensitive (UBS) combat information services such as in-the-field logistics and medical and troop deployment/movement. If this perspective is taken, a means of more fully protecting the NIPRNET is required. A suggested architecture will be provided in the section of this report entitled "What Might Be."

Page 894 of 3957

Finally, the panel notes that both the SIPRNET and JWICS provide virtually no protection against the insider threat. This issue is also addressed Chapter 4 entitled "What Might Be Done" later in this report.

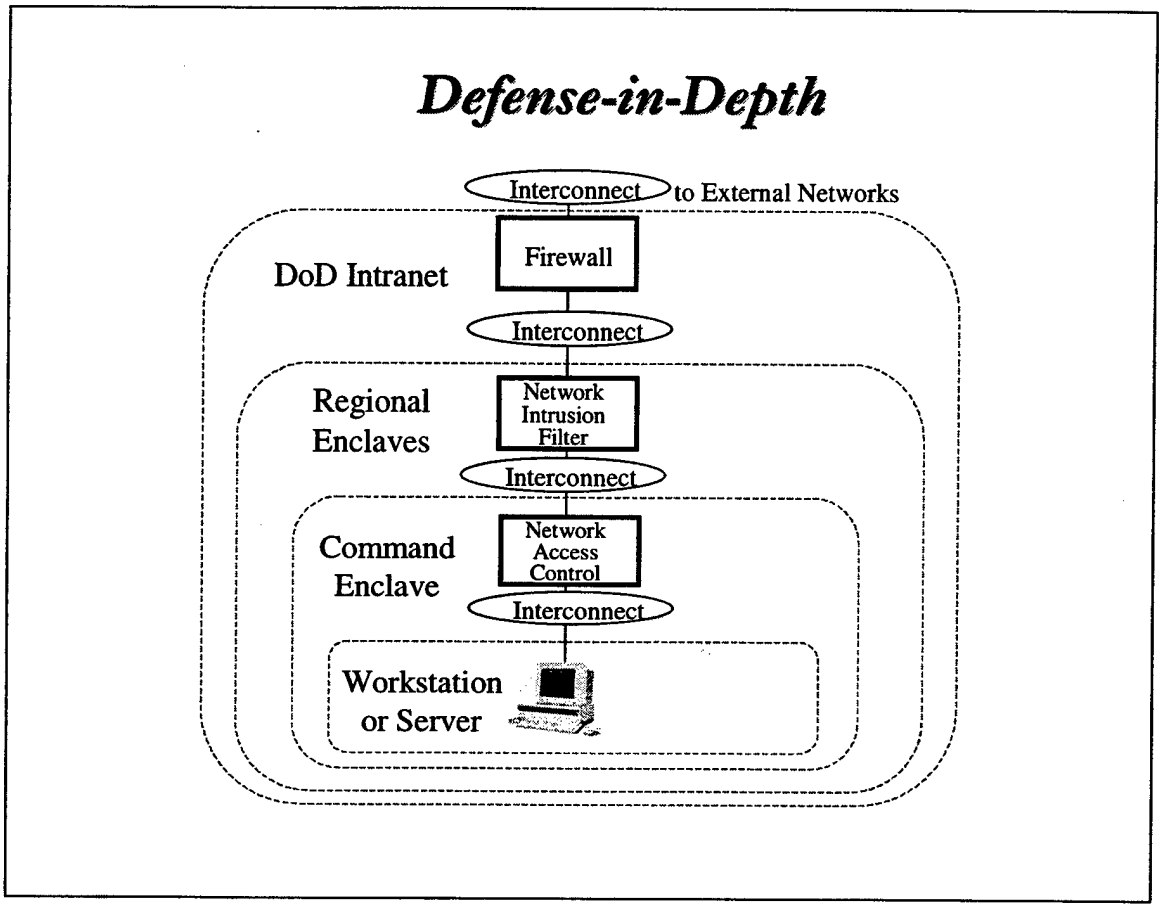


Figure 16. Defense-in-Depth

Figure 16 shows the "defense-in-depth" (DiD) strategy DoD is employing to try to protect its publicly accessed sites on the NIPRNET. The basic concept of defense-in-depth is to provide multiple layers of security mechanisms between computing elements (workstations and servers) in a particular enclave and computing elements in other enclaves, the DoD Intranet, or external networks. There are four focus areas of defense-in-depth: defend the computing environment; defend the enclave boundary; defend the network; and establish supporting infrastructures. Defending the computing environment includes properly configuring operating systems and application software, along with using host-based security services such as anti-virus software, intrusion detection, and public key cryptography. Defending the enclave boundary includes identifying all enclave boundaries, employing firewalls at these boundaries, and detecting intrusion at the enclave-level. Defending the network includes using link encryption for classified networks, firewalls, and intrusion detection. Supporting infrastructures include PKI (public key infrastructure) services and services that support network management, intrusion detection, and intrusion response.

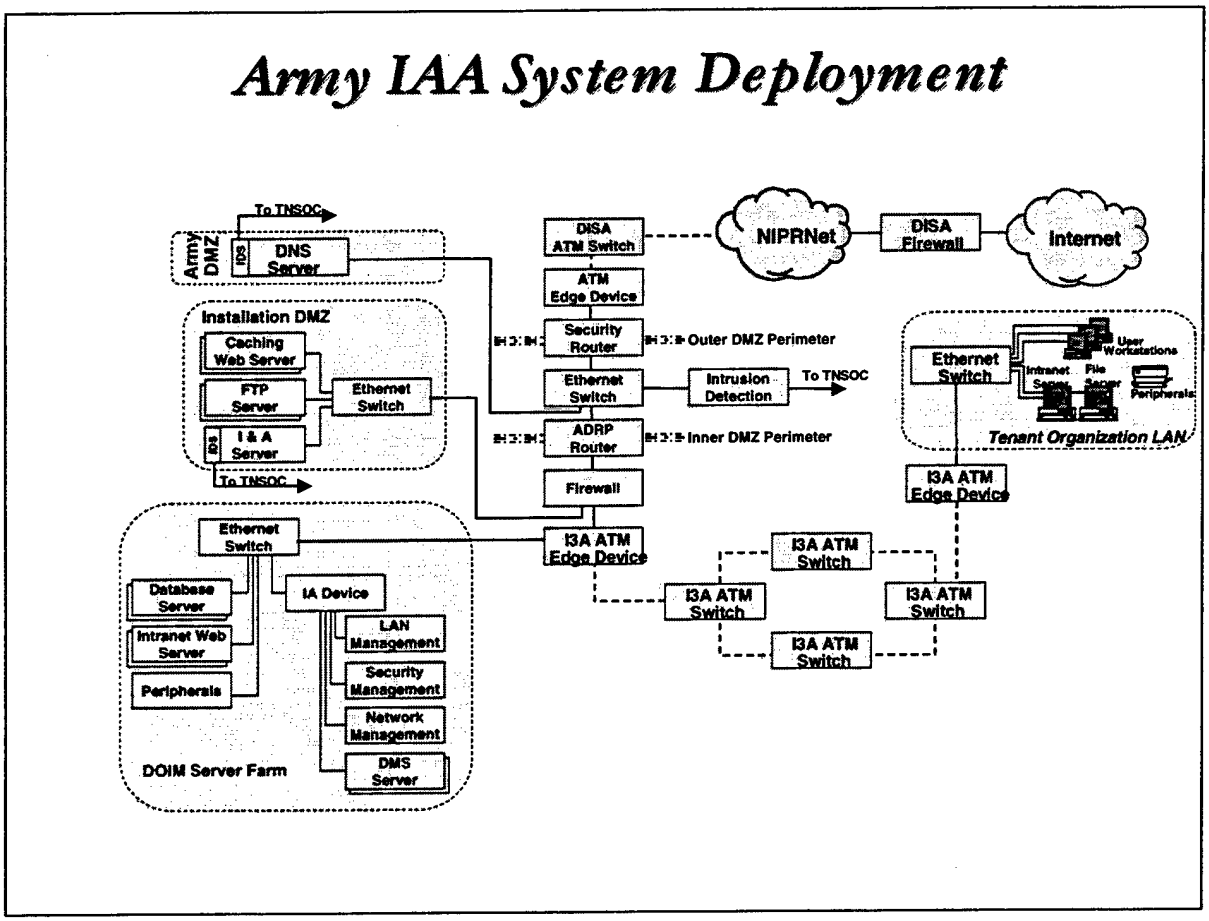


Figure 17. Army IAA System Deployment

The Army is applying a defense-in-depth (DiD) strategy to their NIPRNET post/camp/station enclaves as shown in Figure 17. In this particular system architecture, the Army is accepting that Defense Information Systems Agency (DISA) is providing asynchronous transfer mode (ATM) services to the enclave boundary. A router then provides a translation from the native ATM backbone to an IP-based network interface in the demilitarized zone (DMZ) and to an Ethernet interface within the enclave itself.

In the Army's implementation of DiD, the Army's public information servers are within the installations DMZ. All access from the WWW (public use) comes from the Internet through the NIPRNET, to the installation perimeter, then through the ATM switch, perimeter IP router and an Ethernet switch (at which point intrusion detection is conducted) to the installation servers. Thus *all* public users are funneled to the installation's DMZ for general information services.

In this implementation, there is then an additional IP router, a firewall and an ATM switch to convert from IP back to native ATM. These are then the backbone for the installation server farm and tenant organization's local area networks (LANs). This multiple conversion from ATM to IP to Ethernet to IP to ATM can cause latency and throughput problems (due to multiple protocol translations). This system architecture does provide the opportunity to use higher bandwidth (relative to existing IP network encryptors) ATM network encryptors where necessary. There

does appear to be uncertainty, however, as to why this multiple protocol translation is necessary or desirable.

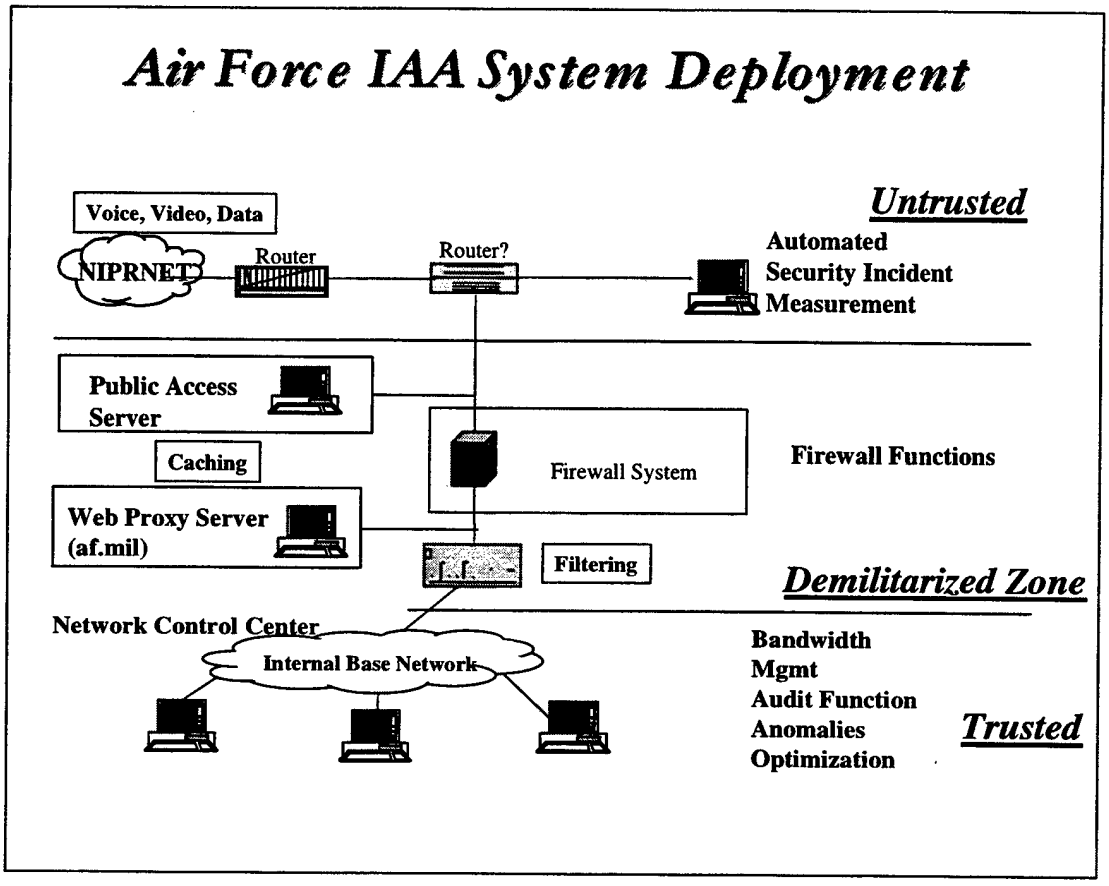


Figure 18. Air Force IAA System Deployment

The Air Force has taken an alternative approach to implementing DiD as compared to the Army. As shown in Figure 18, the Air Force is deploying different protocol translation architecture as well as different locations for performing its enclave-level intrusion detection. Furthermore, the Air Force has combined both firewall and router filtering to provide access control to their enclave infrastructure.

The Air Force implementation is, however, similar to the Army's in that they both invite the general public into their enclave DMZ's for general information services. Thus, the general public is required to transit the NIPRNET for these services; everyone on the WWW is an "insider" on the NIPRNET, with access control being levied only at the installation boundary. Malicious behavior detection for both the Army and the Air Force is conducted at the common access point to the DMZ information services and at the Army/Air Force installation (managed) services. In both cases, the general public can reach this access point as well as the access points associated with the actual installation boundaries.

The Navy's IAA is to be determined (TBD). The Navy has chosen to outsource its GIG/Intranet, including IA services. The Navy does have concepts for how to protect its enclaves, but it has decided to procure IA as an incentivized service in the acquisition. The panel was not able, therefore, to comment on the IA system architecture that the Navy will have. What is evident, however, is that each service is pursuing its own solution to the problem of providing IA for its specific GIG/Intranet component of the DoD NIPRNET VPN. Each service's solution is different and attendant interoperability issues will arise given that all components must be integrated into the NIPRNET. Intrusion Detection System (IDS) information must be readily shared as must information to dynamically set filtering in firewalls and routers given indicators and warnings of information operations against the DoD GIG. Such coordination is especially difficult in the context of diverse defense-in-depth implementation strategies.

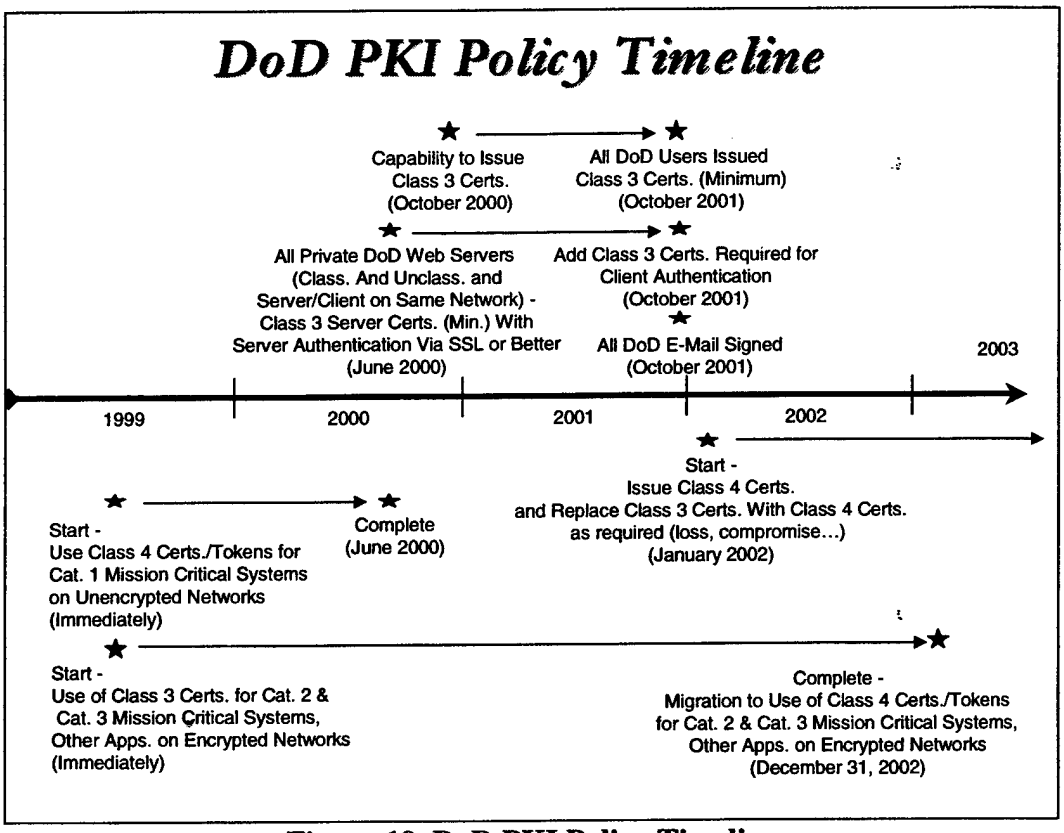


Figure 19. DoD PKI Policy Timeline

An important element of the DoD IAA system architecture is the deployment and use of commercial-based public key infrastructure (PKI). Figure 19 depicts the current DoD PKI policy timeline. This policy applies to all DoD components and provides timelines for the issuance of class 3 and class 4 PKI certificates.

Class 3 certificates are designed to protect administrative, mission support, and some mission-critical information when being transferred within a single security classification level. Class 3 certificates can be issued with a private key contained in a software token. Class 4 certificates protect sensitive but unclassified mission-critical information passing over

unencrypted networks, and the corresponding private keys are intended to be contained in hardware tokens.

The policy establishes timelines for issuing class 3 and 4 certificates to users. It also establishes the timeline for using certificates for web server access control and for email. The timeline shown above has dates that are not aligned with the Common Access Card (CAC) program. The CAC program will provide, via the Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System (DEERS/RAPIDS), the ability to issue smart cards to DoD personnel that can contain at least class 3 certificates. It is anticipated that class 4 certificates may be able to be issued via the CAC, though this policy was not yet in place at the time of this study. Because the current PKI timeline is not aligned with the CAC timeline, a new PKI policy has been drafted. Though not yet finalized, this policy is expected to move the June 2000 dates to December 2000.

3.3 OPERATIONAL ARCHITECTURE

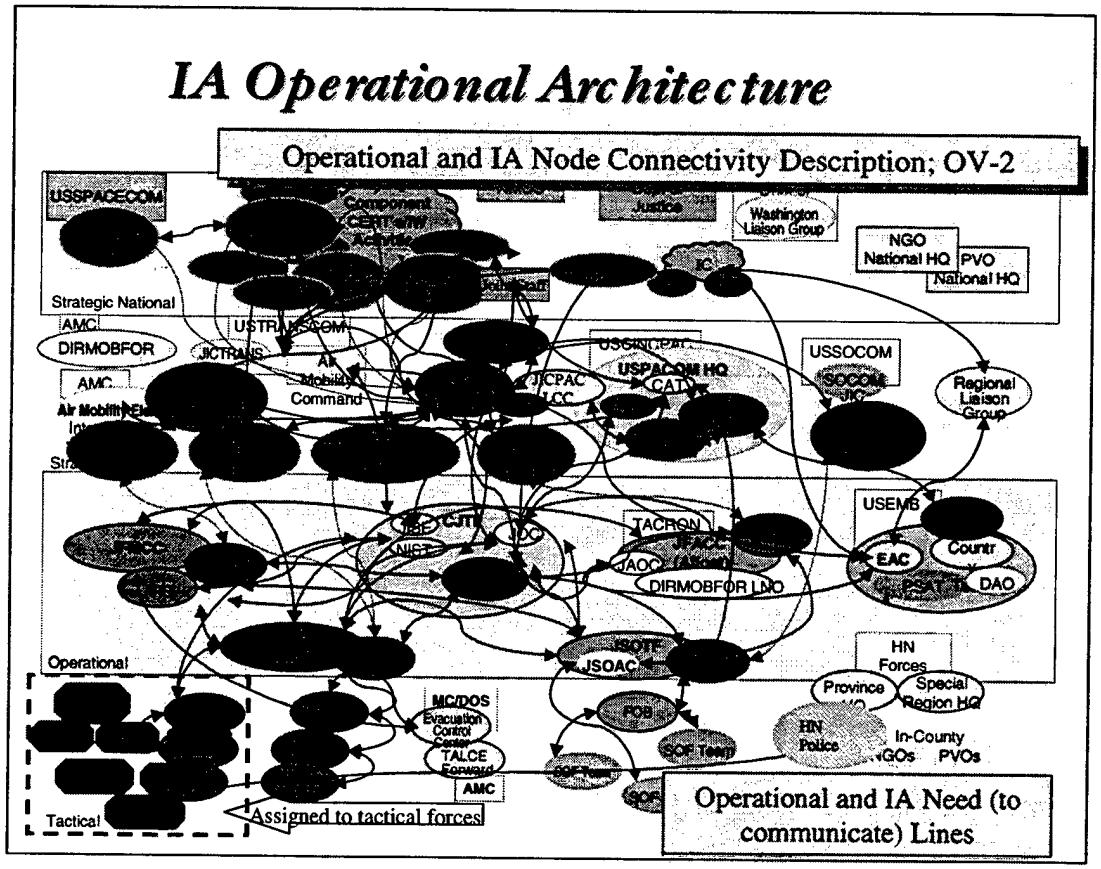


Figure 20. IA Operational Architecture

In addition to the progress made in establishing an IAA system architecture, DoD has begun the process of establishing an IAA operational architecture. Figure 20 depicts one product that has resulted from this effort to date. In this figure, operational facilities (OPFACs) that would be involved in IO processes are identified. The IAA OA has also identified the IA-related

Page 899 of 3957

information exchange requirements (IERs) between these OPFACS that is necessary to coordinate and conduct IA activities. The figure represents a limited non-combatant evacuation operation (NEO), height-of-operation, scenario in the Pacific.

As part of the operational architecture effort, information exchange metrics, activity models, and logical data models are being developed. The panel noted that this IA operational architecture effort is important and will make a critical contribution to understanding IO mission processes, responsibilities, and required information flow for specific concept of operations. Furthermore, this operational architecture will be important in helping to define how IO can/should be process-reengineered to allow for more efficient and timely response to IO missions and threats in the future.

Although establishing an IA operational architecture is a difficult and time-consuming task, the panel feels this effort will provide important insights into the mission, organization and tactics, techniques and procedures (TTPs) required to effectively execute IO. For example, the panel noted that the number of OPFACs associated with the limited scenario represented in Figure 20 implies a substantial IO coordination and information exchange overhead in support of the mission. From such "as-is" operational architecture efforts, "to-be" architectures can be investigated that would simplify the prosecution of IO missions to achieve information superiority as envisioned in JV2020. It is noted, though, that a single IA operational architecture is not sufficient. A representative set of IAA operational architectures for various types of missions and areas of responsibility should be developed in order to more fully understand the entities, processes, and supporting IERs for IA.

Page 900 of 3957

3.4 TECHNICAL ARCHITECTURE

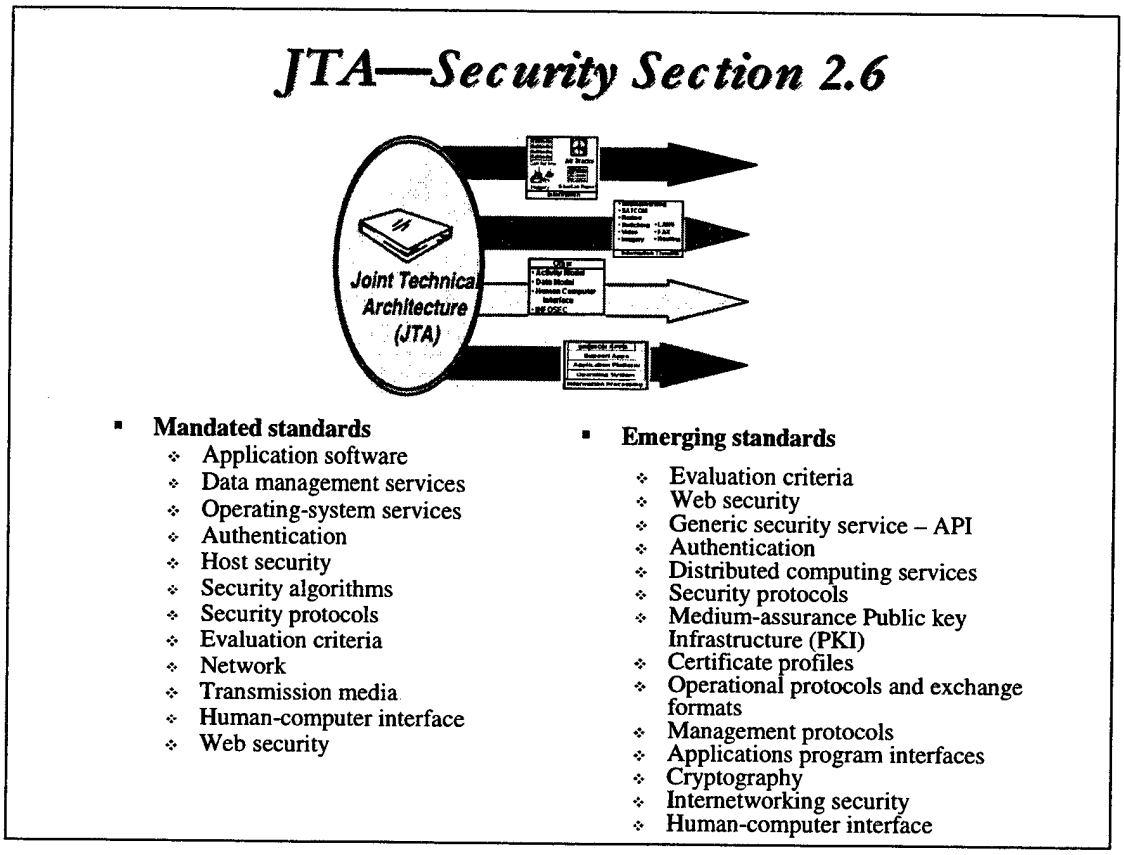


Figure 21. JTA—Security Section 2.6

The remaining component of the IA architectural framework is an associated technical architecture. This latter component is the third element of the DoD C4ISR architectural framework methodology. The set of IA architectural components, IA operational architecture (IA-OA), the IA system architecture (IA-SA), and the IA technical architecture (IA-TA), will provide the perspective to support securing and protecting the Global Information Grid.

The panel received two briefings on IA-TAs. The first was a briefing on Section 2.6 (Security) of the DoD Joint Technical Architecture (JTA). The JTA identifies the services, interfaces, standards, and their interlocations and provides the technical guidelines for implementation of information systems and services. The standards selected for the JTA are selected primarily from the private sector IT industry although some military specific (MILSPEC) standards are included where no commercial counterpart exists. Figure 21 provides a summary of the JTA security chapter.

The panel noted that the standards called out in the JTA for mandated standards are consistent with those noted in the ISO security reference model presented previously. The concept, processes, and content of the JTA, and specifically Section 2.6, are strongly endorsed by the IAA Panel.

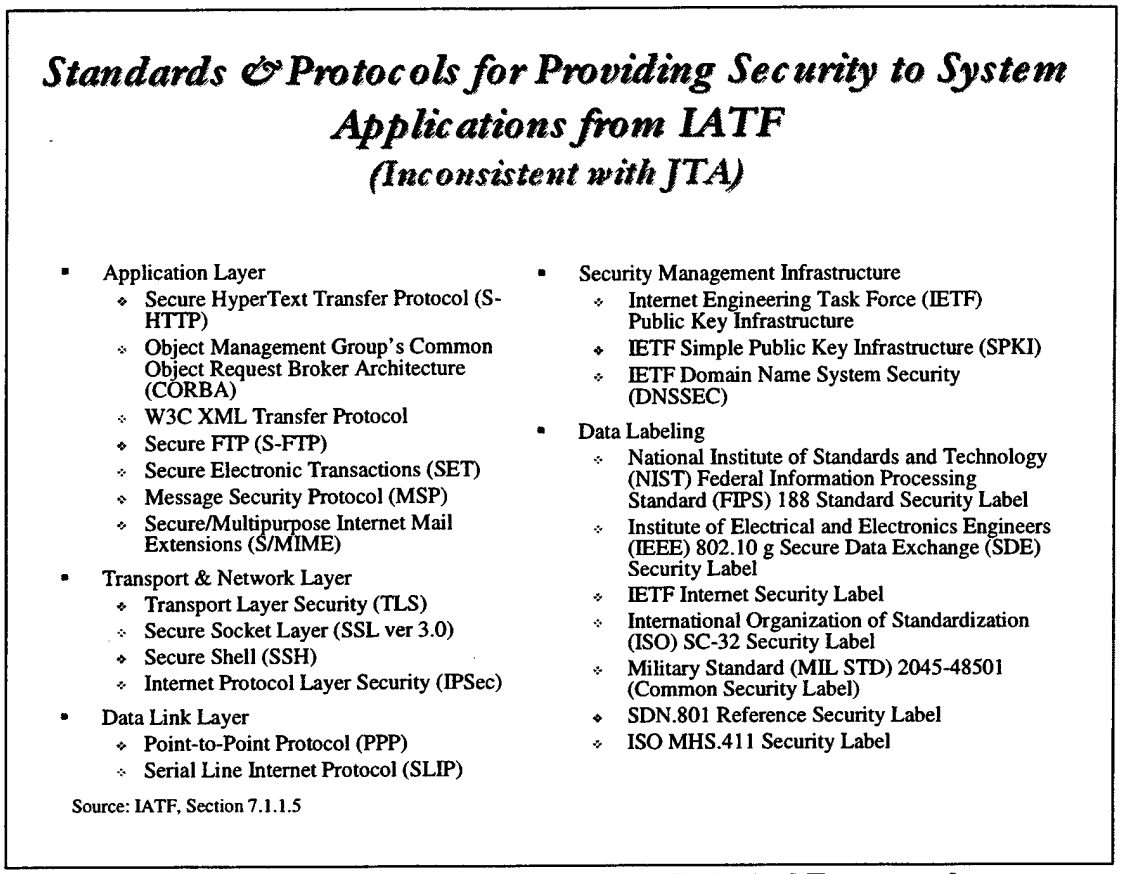


Figure 22. Information Assurance Technical Framework

The second technical architecture briefing to the panel concerned the Information Assurance Technical Framework (IATF), an excerpt of which is provided in Figure 22. The panel found this document to be a tutorial and collection of useful generic information on IA. The panel noted, however, that the section of the IATF associated with standards and protocols for providing security to system applications is incorrect and inconsistent with the JTA. The IATF, unlike the JTA, is not a standards setting or selection document. Rather, the IATF Forum has been organized to encourage participation by vendors of (largely COTS) IA products and services. The major focus of the IATF is the development of protection profiles (under common criteria) that will be used to evaluate products, i.e., under the national Information Assurance Partnership (NIAP) program operated by NIST and National Security Agency (NSA). There is no unified architectural underpinning for the IATF. This is to be expected, i.e., security evaluation criteria such as the Common Criteria (CC) (and product profiles based on the CC) tend to be architecture independent. As a result, the collection of standards cited by the IATF, as briefed to the panel, lacks architectural continuity and it is not an appropriate alternative to the work of the JTA.

Many of the security standards that are collected in the IATF are experimental or did not gain acceptance in the Internet. For example, secure hypertext transfer protocol (S-HTTP) is not implemented in any commercial browsers or servers; it lost the protocol battle to SSL/TLS. SPKI is not a standard, but rather is the experimental output of a failed IETF working group, not

Page 902 of 3957

supported in commercial products. The Public Key Infrastructure Working Group (PKIX WG) of the IETF produces standards based on X.509, which are implemented in a wide variety of products. Moreover, the other IETF security protocol working groups make use of the PKIX standards, not SPKI. The IATF referenced a wide range of security labeling standards that are a mix of redundant and/or superceded documents.

The IATF thus suffers from the same problems associated with the TAFIM; it is a collection of history and general information – not a document that can be used to implement interoperable, secured information systems for DoD.

The panel notes, with concern, that DoD policy requires that the JTA be used as the "building code" for the DoD information infrastructure. On the other hand, the recent document from the Deputy Secretary of Defense, subject "Department of Defense Chief Information Officer Guidance and Policy Memorandum no. 68510," Department of Defense Global Information Grid Information Assurance (ASD/C3I) suggests that the IATF and published Common Criteria Protection Profiles be consulted "for guidance... and IA solutions that should be considered to counter attacks."

The panel's concern is the apparent confusion these two policy statements could cause within the IA community. The IATF standards are incorrect and inconsistent with the JTA and private sector practice. The panel believes the JTA is the better reference on IA standards and protocols, and it should be referenced as such in all GIG IA policy documents.

Page 903 of 3957

3.5 METRICS

Joint Staff J6, IA Metrics

- Performance-based
- Integrated into operational readiness reporting
- CINCs report as part of JMRR process
- Example

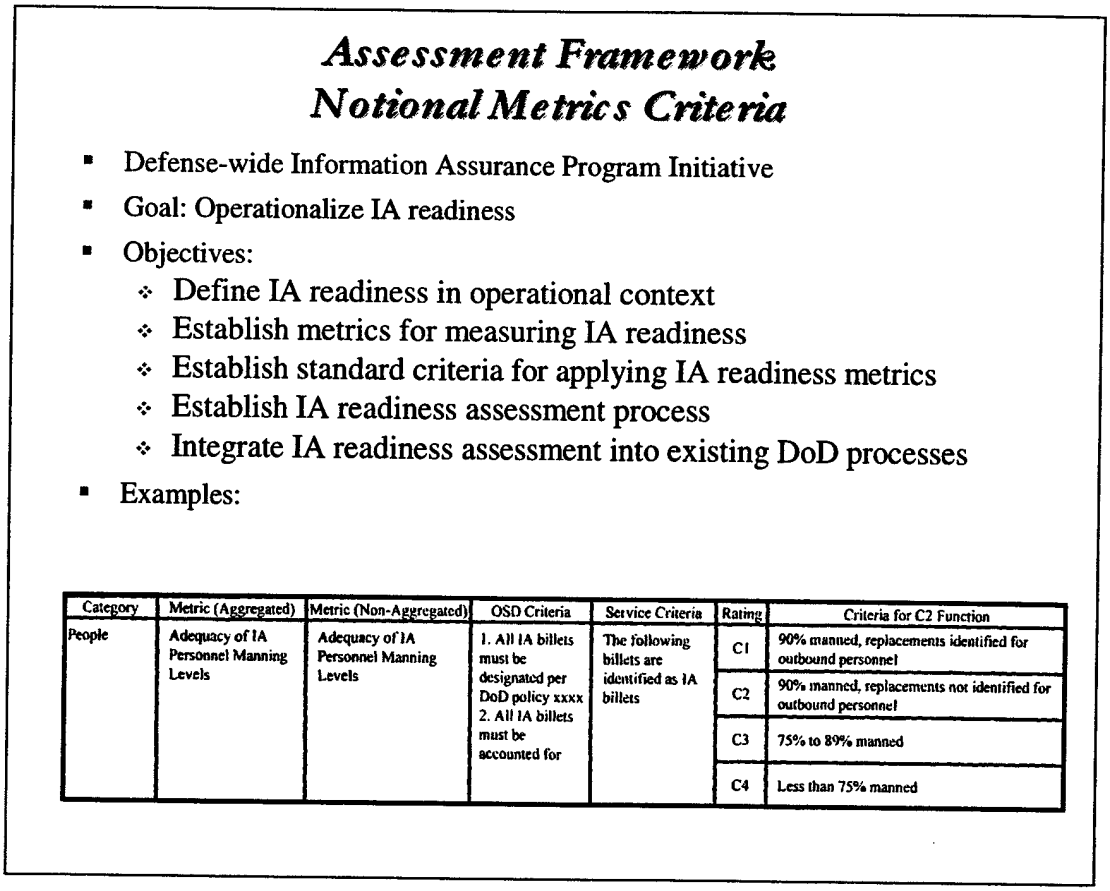
INFORMATION ASSURANCE METRICS (List 1)					
1.0	**PLANS AND OPERATIONS**				
Joint Readiness C-Level	**PLANS AND OPERATIONS ASSESSMENT**				
C-1	..... **minor** deficiencies ..... with **negligible** impact on capability to perform required missions.				
C-2	..... **some** deficiencies .... with **limited** impact on capability to perform required missions.				
C-3	..... **significant** deficiencies ... **prevent** it from performing some portions of required missions.				
C-4	.... **major** deficiencies .... that **preclude** satisfactory mission accomplishment.				
1.1	**Plans** — Planning involves both those specialized IA plans and IA portions of operations plans. IA Planning should identify necessary resources in detail.				
1.1.1	IA portion of concept of operations and operations plans; standard operating procedures (SOP), continuity of operations plan developed and effectively implemented.	C1	C2	C3	C4
1.2	**Operations** – ongoing execution of daily IA support procedures....				
1.21	Garrison Operations –IA strategy should support military operations				
1.21.1	IA integrated sufficiently in current/ongoing operations	C1	C2	C3	C4
1.2.2	**Deployed JTF operations**				

Figure 23. J6 IA Metrics

As noted in the GIG reference material (see Figure 6), metrics play an important role in architecting and deploying this infrastructure. The panel, therefore, chose to address this topic as a stand-alone topic outside of the DoD C4ISR architectural framework. Only two specific initiatives addressing IA metrics with DoD were presented to the panel. They are described next.

Figure 23 provides an overview of IA operational readiness metrics developed by the Joint Staff. These metrics are used by the CINCs to assess and report on IA readiness as part of their overall readiness assessment. The panel noted that these metrics are a good starting point to raise the awareness and importance of IA as a critical warfighting requirement. Although these metrics are difficult to measure, are not yet comprehensive in nature, and do not address the CINC's warfighting capabilities as supported or hindered by the IA capabilities, they do raise IA awareness within a CINC's organization, and they do begin to raise the importance of IA to the warfighter. The panel recognizes that this set of metrics will evolve and improve over time.

Page 904 of 3957



Category	Metric (Aggregated)	Metric (Non-Aggregated)	OSD Criteria	Service Criteria	Rating	Criteria for C2 Function
People	Adequacy of IA Personnel Manning Levels	Adequacy of IA Personnel Manning Levels	1. All IA billets must be designated per DoD policy xxxx 2. All IA billets must be accounted for	The following billets are identified as IA billets	C1	90% manned, replacements identified for outbound personnel
					C2	90% manned, replacements not identified for outbound personnel
					C3	75% to 89% manned
					C4	Less than 75% manned

Figure 24. Assessment Framework

The second initiative on establishing IA metrics is being conducted under the auspices of the Defense-wide Information Awareness Program (DIAP). A team has been established and is tasked to develop an IA readiness assessment framework and associated metrics. The team has begun the process of defining quantifiable IA metrics and associated ratings, as indicated by the example in Figure 24. The panel noted that the metrics presented by the speaker overlapped to some degree with those presented by the J6 briefer. The panel understood that the J6 metrics are intended to be integrated with the DIAP metrics in a process that will provide a DoD-wide IA readiness assessment.

Based on the two briefings, however, the panel felt that greater coordination is necessary between the two efforts. The message conveyed by the speakers tended to leave the impression that these efforts were not tightly coordinated, could lead to duplication of effort, and, of greatest concern, could lead to confusion within the user organizations that are being assessed.

The panel felt that a single DoD IA effort should exist that addresses the spectrum of IA metrics that are necessary. This spectrum is much greater than the sets of metrics presented by the J6 and DIAP. For example, IA technology and system-architecture related IA metrics should also be developed and used to assess progress and residual vulnerabilities in the GIG as it is deployed and improved over time. The panel could identify no specific, focused initiative on developing such technical metrics. The panel's suggestions regarding metrics are provided in the next section of this report.

3.6 WIRELESS

The panel noted that wireless-infrastructure IA issues were not raised in any of the briefings it received. Although wireless data communications over military owned/operated systems is well understood and IA is typically provided through transmission security (TRANSEC) at the physical layers and communication security (COMSEC) at the application layer, the private sector wireless infrastructure that today is embedded in the GIG was not addressed as an area of concern within DoD. The panel notes that private sector wireless media can be used as a means to gain access and control of the "wired" part of the commercial infrastructure (at network management layers). This wireless segment of the infrastructure must be carefully protected. As a result, this issue is addressed in greater depth in the next section of this report.

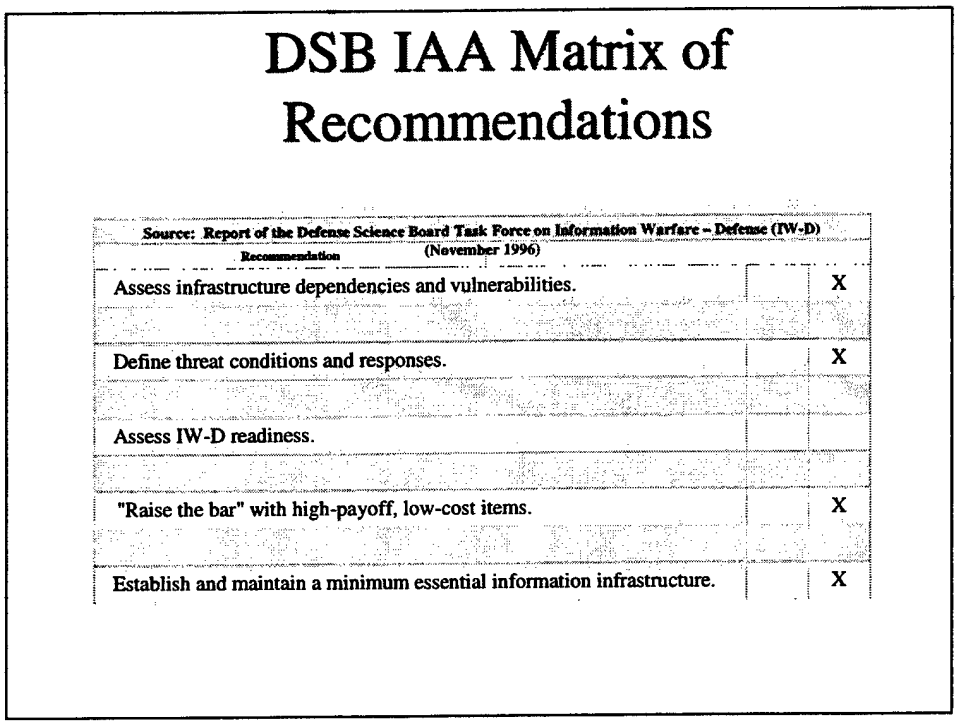


Figure 25. DSB IAA Matrix of Recommendations

3.7 SUMMARY OF FINDINGS

As part of our findings, the panel notes that the 1996 DSB Summer Study made four overarching recommendations related to IAA. These recommendations are listed in Figure 25. From the preceding discussion, the panel makes the following observations.

Recommendation 1: Assess infrastructure dependencies and vulnerabilities. The DoD today is relying primarily on the private sector to assess NIPRNET infrastructure dependencies and vulnerabilities. As vulnerabilities are identified, the DoD implements the associated fixes within the NIPRNET (software patches, virus filtering, IDS templates) using DiD as the basis for its system architecture. However, the panel notes that there is currently no methodology for "engineering" DiD. There are processes for implementing DiD updates, but there is no engineering discipline that allows for the design of a DiD solution with confidence in the security

it offers in the face of various threats. The premise underlying DiD is that an acceptable level of protection can be achieved through layering of defenses, even though each defensive technology is known to be imperfect, i.e., each one is known to have residual vulnerabilities or functional shortcomings. Also, central to the DiD premise is the assumption that each layer of defense exhibits functional deficiencies or vulnerabilities that are independent (ideally orthogonal), and thus the ability to penetrate one defensive layer dos not imply the ability to penetrate other layers (by the same means). However, to the extent that many of these defenses are built upon COTS operating systems (OS) that are known to be vulnerable, but for which not all residual vulnerabilities are known, this premise is questionable. Moreover, not all the flaws in each defense mechanism are likely to be known because they are COTS products with low to medium assurance. Thus it is not possible to estimate the extent to which such layered defenses increase the work factor for an attacker, above and beyond the OS problem cited above. (Nonetheless, there is reason to believe that the work factor is increased, at least for low-grade threats.) None of these observations implies that DoD should not pursue DiD. Rather, they suggest that additional effort is needed to develop a suitable methodology that will support DiD engineering and deployment. They also suggest that prospective users of a DiD strategy should be apprised of the uncertainty associated with both the strategy and its implementation.

Recommendation 2: Define threat conditions and responses. The DoD information condition (INFOCON) policy and procedures are well established, promulgated and understood. The panel does not believe, however, that DoD has experience in understanding (how consistent and timely the responses will be executed throughout DoD) upon INFOCON status changes. Furthermore, the panel believes that experience is lacking in assessing how effective the INFOCON procedures will be in thwarting an attack. Gaining this experience, through continuous exercises and the assessment of INFOCON responses to varying red-tem attacks, is an important process to establish.

Recommendation 3: "Raise the Bar" with high-payoff, low-cost IA Initiatives. The panel notes that a great deal of progress has occurred here as well. DoD has established an IAA framework, it has selected a systems architecture, and it is deploying DiD solutions; it has increased user/community awareness of the IA problem. The panel does note, however, that work remains to be done. Simple but strict IA configuration management practices at all DoD information sites is still a critical issue; closing all NIPRNET connections to the public Internet (other than through the 8-11 DoD gateways) remains an unresolved issue; and the insider threat on the SIPRNET and JWICS remains an open issue although suitable IA technologies and processes to mitigate this risk are available.

Recommendation 4: Establish and maintain a minimum essential infrastructure. The panel did not receive any indication that this recommendation was being pursued by DoD. In fact, DoD has focused on deploying a GIG with integrated IA services. The panel does support the goal of deploying and securing the GIG, but notes the following: the GIG is being deployed based on a security strategy referred to as "risk management," not one aimed at achieving an impenetratable minimum essential in infrastructure. It has been suggested that, in the past, security experts focused on achieving "perfect" security, which can be viewed as a "risk avoidance" strategy. In fact security experts have long acknowledged that perfect security is unattainable. Risk management argues for explicitly making a decision to accept a certain level of risk as a condition of deploying a system. This is a fine principle, but it is based in part on the

premise that one can evaluate (and quantify) the residual risks associated with a system composed of components that are known to be imperfect. This is a questionable assumption. First, although one might be aware of some set of residual vulnerabilities in the system components, it also is likely that these components contain other, unknown vulnerabilities of undetermined severity. Second, there is no algebra that allows the computing of the risk associated with deploying a system composed of components with known vulnerabilities, much less a system in which the components have unknown vulnerabilities. Thus it seems certain that risks of unknown magnitude are being accepted when the phrase "risk management" is part of the security design and accreditation process. This issue can, at this time, only be addressed through empirical means whereby a representative segment of the deployed GIG is subjected to a comprehensive and continuous IA vulnerability assessment process. A "testbed" concept will be proposed in the next section as a means to address this need.

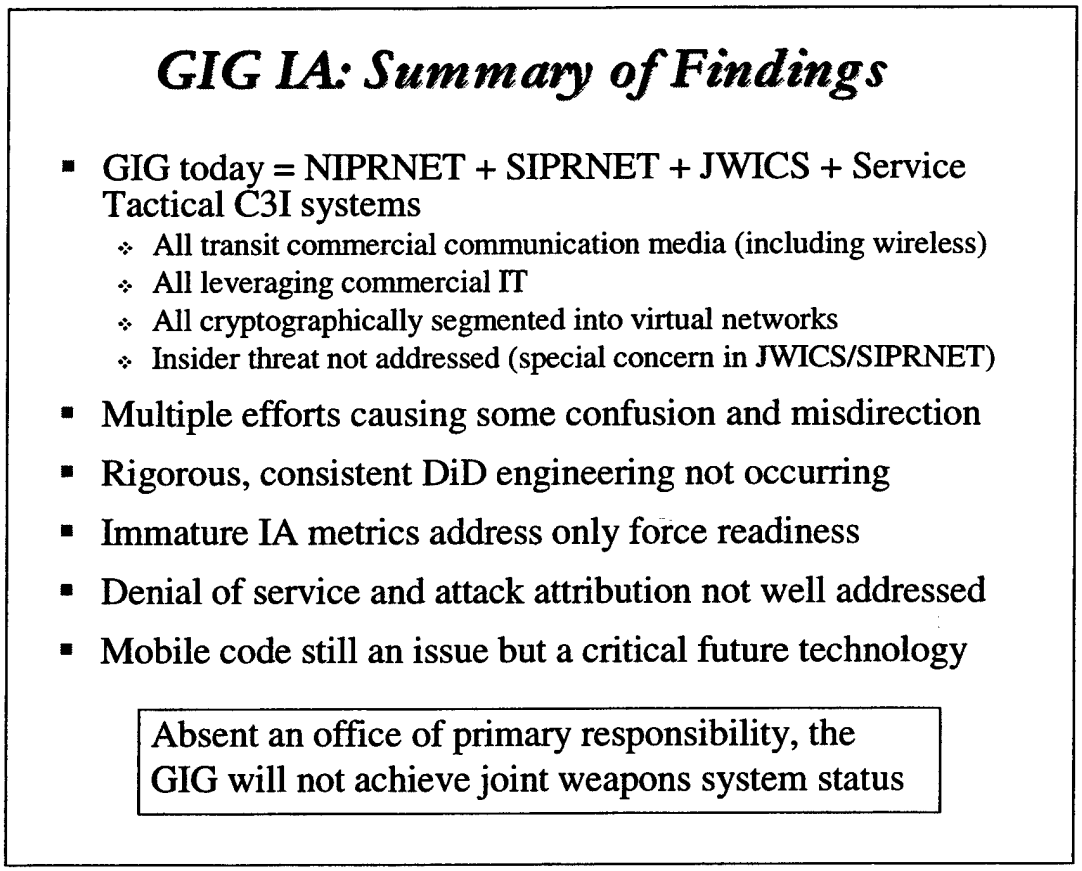


Figure 26. GIG IA Summary of Findings

In closing this section of our report on panel findings, Figure 26 provides a summary of our observations. The Global Information Grid does comprise multiple virtual worldwide data networks, the NIPRNET, SIPRNET, JWICS and service tactical C3I systems. These networks use shared commercial communications media and commercial information technologies. In addition, all are cryptographically segmented into virtual networks. However, the panel noted that there is virtually no protection against the insider threat, especially for the classified networks. All services are adopting a Defense-in-Depth (DiD) strategy, with different

implementations. For example, the Air Force is employing a different strategy from the Army: a different protocol translation architecture; a different location for performing enclave level intrusion; and different measures for enclave access control. The panel notes that while there is a general framework for implementing DiD, there is no engineering discipline that allows for design of a DiD solution that provides confidence in security against a variety of attacks.

The current emphasis on information assurance metrics is focused on readiness and is not addressing the metrics needed to assess and measure mission, system or technical level performance. In addition, denial-of-service measures and attack attribution metrics are not well addressed.

Finally, the panel believes that today's DoD organizational structure is inadequate to deliver a GIG. Although both the DoD Chief Information Officer (CIO) Executive Panel and the Military Communications and Electronics Board (MCEB) are working on defining and providing guidance for the GIG, the panel feels that a new organizational structure, with a centralized primary point of responsibility, will be required to develop a GIG worthy of weapons system status.

Specifically, the current charter of the DoD CIO Executive Board is contained in the DepSecDef Memo Subj: DoD Chief Information Officer Executive Board, 31 March 2000. This charter states that the Council is the principal forum to advise the DoD CIO on the full range of matters pertaining to the Clinger-Cohen Act (CCA) of 1996 and the Global Information Grid. Additionally, the board also coordinates implementation of activities under the CCA, and exchanges pertinent information and discusses issues regarding the GIG, including DoD information management (IM) and information technology (IT). The primary mission of the board is to "advance the DoD's goals in the areas of IM, information interoperability and information security between and among Defense Components." The Board also coordinates with the IC CIO Executive Council on matters of mutual interest pertaining to the GIG. Its management oversight includes recommending, reviewing, and advising the DoD CIO on overall DoD IM policy, processes, procedures and standards, as well as overseeing all aspects of the GIG to support the DoD's and IC's mission and business applications. This includes the collaborative development of IT architectures and related compliance reviews; management of the information infrastructure resources as a portfolio of investments; collaborative development of planning guidance for the operation and use of the GIG; and identification of opportunities for cross-functional and/or cross-component cooperation in IM and in using IT. The board's architecture management responsibilities include ensuring the collaborative development of architectures as specified in the CCA, and ensuring that processes are in place to enforce their standardized use, management and control, as well as aligning IT portfolios with the GIG. Although the board has budgetary review authority for IT investments, and can make recommendations, it has no direct budgetary authority. It also has no authority, either review or management oversight, over the warrior components of the GIG. The membership of the DoD CIO Executive Board includes:

- Chair: DoD CIO (ASD (C3I))
- Members: CIOs of the Military Departments
  - CIO, Joint Staff

  - USD (AT&L)
  - USD (P) (Policy)
  - USD (C) (Comptroller)
  - USD (P&R) (Personnel and Readiness)
  - ASD (C3I) (usually the Deputy CIO)
  - Director PA&E (Program Analysis and Evaluation)
  - J6, Joint Staff
  - OPNAV N6
- Director, Communications and Information, USAF, AF/SC
  - IC CIO
  - CIO, JFCOM (Joint Forces Command)
- Security Advisor: Director, National Security Agency (DIRNSA)
- Technical Advisor: Director, DISA
- Legal Advisor: DoD General Counsel

The charter of the MCEB is contained within DoD Directive 5100.35 dated 10 Mar 1998. The MCEB considers those military communications-electronic matters, including those associated with national security systems (NSS) referred to it by the SecDef, CJCS, the DoD CIO, secretaries of the military departments, and heads of DoD components. The mission of the MCEB is to obtain coordination among the DoD components, between the Department of Defense and other governmental departments and agencies, and between the DoD and representatives of foreign nations on matters under the MCEB jurisdiction. The MCEB provides guidance and direction to the DoD components and advice and assistance as requested. The membership, as listed below, is primarily composed of those in charge of the communications activities in the listed components, which have little, if any, authority over IT issues in other portions of their component. The MCEB has no budgetary review or execution authority over any component, nor is there any mechanism within the MCEB structure for enforcement of non-compliance with decisions. The relationship between the MCEB and CIO Executive Board is still being discussed, but in effect, the MCEB is a subordinate activity under the direction of the CIO Executive Board and its recommendations are referred to that Board for final decision. Membership of the MCEB includes:

- Chair: Joint Staff, J6
- Members: Vice, J6
  - DISC4, U.S. Army
  - OPNAV, N6
  - HQ USAF, SC
  - HQMC, C4
  - USCG, Assistant Commandant for Systems
  - Director, DISA

Page 910 of 3957

- Director, NSA
- Director, DIA

Thus, neither the DoD CIO Executive Board nor the MCEB has the membership or authority over budgets and execution activities that the panel believes are necessary to ensure the GIG is built and managed as intended by the IAA Panel. Without that level of authority over all elements of the GIG, the architecture is subject to interpretation by each component based on its needs, rather than the needs of the entire DoD enterprise. There is also little incentive to address crosscutting issues in a coherent fashion when the funding for these programs is provided via Title 10 channels without some mechanism to encourage cooperation. Because of the Title 10 and DoD versus intelligence community issues, the only level of management senior enough to cross this bridge is at the DepSecDef level. Additionally, neither of these two boards has a direct oversight responsibility over any specific office or organization that carries out its direction.

Page 911 of 3957

CHAPTER 4. "WHAT MIGHT BE DONE" PANEL SUGGESTIONS

4.1 THE GIG IS A WEAPON SYSTEM

The GIG is a Weapon System

- It leads to information/decision superiority, therefore it will be attacked by our adversaries
- Built unlike a traditional weapons system
  - Critical elements not owned by the DoD
  - A platform shared by all DoD users
  - Built primarily from COTS components
  - Components evolve very rapidly
- Attacked more readily
  - Low "cost of entry" for attackers
  - Easy to deny service globally
  - Attacks escalate rapidly (compressed Observe, Orient, Decide, Act [OODA] loop)
  - Attack attribution is difficult
  - Forensics processes & technology are immature

Figure 27. The GIG is a Weapon System

Information superiority is the pacing item in realizing the goals of JV2020, and the Global Information Grid is the underlying information superiority infrastructure. The panel argues, in Figure 27, that because of its importance, the GIG should be viewed as a weapons system, one that will present a lucrative target for our adversaries. However, unlike traditional weapons systems, the critical elements of the GIG are not owned or controlled by the DoD. Furthermore, the GIG is shared by all DoD users and is built primarily from COTS components, which are rapidly evolving.

A significant weakness of the GIG is that it can be more readily attacked than traditional systems, which are far less ubiquitous and have limited interfaces and stricter controls. This is due to several factors, but first and foremost is the low capital cost of entry for attackers. A few people with personal computers and Internet access have demonstrated the capability to deny

Page 912 of 3957

service and penetrate DoD systems. Attacks have a non-linear characteristic in that they can escalate rapidly, as evidenced by the recent distributed denial-of-service attacks. Unfortunately, attacker attribution is difficult if not impossible today. The attacker enters third party machines and uses those facilities to launch attacks. Current processes and forensics for identifying and tracing attackers are primitive and do not provide adequate support for attribution.

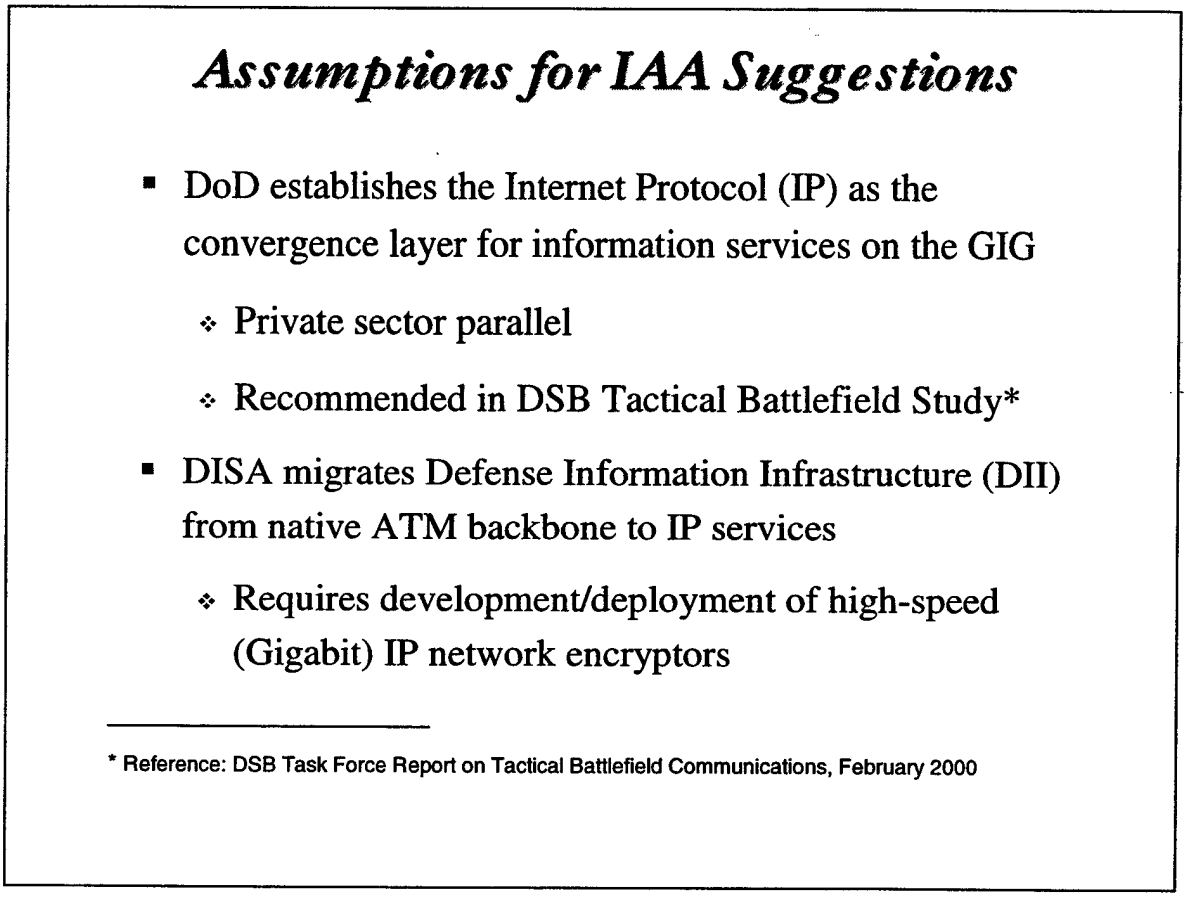


Figure 28. Assumptions for IAA Suggestions

Figure 28 provides the assumptions that are the foundation of the panel's IAA suggestions. These assumptions are based on the following. In the private sector, a trend is underway to develop a single infrastructure providing integrated voice, video and data services. This trend to a common, shared infrastructure for all multimedia services is termed "convergence." The convergence is facilitated by and expected to occur through a common, ubiquitous protocol – IP. This protocol is an open standard supported worldwide by the data telecommunications industry; it is rapidly becoming the convergence layer for all information services on the Internet.

The common IP layer separates the task of telecommunications (transport) from the tasks of service types, information types, and application development. Network engineers concentrate on moving IP packets from one place to another, independent of their content. Application and service developers concentrate on applications and count on the IP layer to provide requested telecommunications services.

The present version of the IP, designated Internet Protocol Version 4 (IPv4), does not yet support QoS-based dynamic resource allocation, a capability needed to support real-time, stream-oriented information flow (i.e., real-time voice and video). In the near term, this limitation is being addressed through higher-layer protocols such as the Real-Time Protocol (RTP), and the Resource Reservation Protocol (RSVP) and via tag switching. In addition, extensions to IPv4, to include a minimum level of QoS, are being investigated by the Internet Engineering Task Force (IETF). The IETF is also working on the next generation of IP, called IPv6, which will include QoS (called differentiated services) and a much larger IP address space, permitting the integration into the Internet of embedded processors (sensors) and many more addressed devices as users.

Today IP is used over many dissimilar networks including: ATM, Ethernet, wireless 802.11, Cellular Digital Packet Data (CDPD) and the like. IP was designed to be the mechanism for transparently moving bits across such networks. Thus, IP is the mechanism that permits the integration of these many types of networks into a network-of-networks – that is, the Internet.

The panel noted that a prior DSB study made a strong recommendation that DoD establish IP as its convergence layer for the GIG.[6] In our discussions with DISA, the briefer observed that he was strongly in favor of migrating the Defense Information Infrastructure (DII) to an IP service infrastructure, resulting in IP being the standard interface to the DISA-supplied point of presence (POP) at all DoD sites supported on the DII. This migration would place DII in the mainstream of the private-sector migration toward a converged infrastructure. Thus, DoD, through DISA services, could fully take advantage of private sector IT.

It was noted that to support this migration, DISA would need high-speed, Type 1, IP network encryption technology. Today DISA uses ATM encryptors developed by DoD, given that DISA provides ATM service to POPs. The panel noted that DoD is supporting the development of equivalent IP devices.

Thus, the panel assumes, in what follows, that DoD will migrate to IP as its convergence layer for the GIG. By doing so the DoD benefits significantly not only in leveraging commercial IT transport technology and services, but also from the perspective of leveraging emerging private-sector IA and IAA technologies, protocols and services.

---

[6] Reference: Defense Science Board Task Force Report on Tactical Battlefield Communications, February 2000

Page 914 of 3957

4.2 ARCHITECTURE SUGGESTIONS

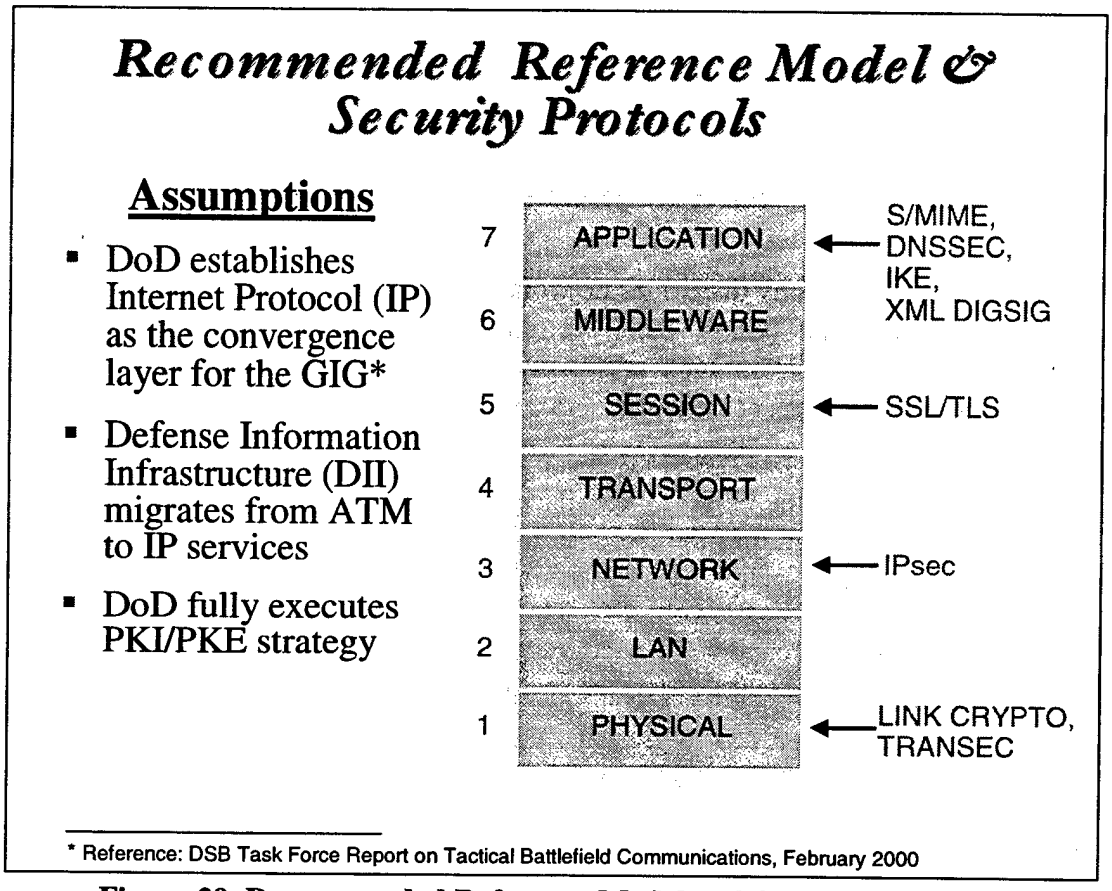


Figure 29. Recommended Reference Model and Security Protocols

The panel's suggested IA reference model is shown in Figure 29. This protocol stack assumes the use of internet protocols in a wide range of environments, including both tactical and strategic. It parallels the ISO reference model (ISO 7498), with the substitution of a "middleware" layer in lieu of the presentation layer, and is consistent with the TCP/IP protocol suite. (This substitution seems appropriate because modern systems do not make use of separate presentation layer functions; these functions are assumed by applications.)

Physical layer protection is afforded via link crystographic systems (i.e., KG 84, KG 189,etc.) on a hop-by-hop basis, where warranted by threat concerns. No data link security; i.e., LAN security protocols such as IEEE 802.10, is recommended. This technology has not been adopted by product vendors and is generally not warranted in switched LANs, when higher layer security protocols are employed. IPsec is recommended for end-to-end, enclave-to-enclave, or end-to-enclave protection. No transport (i.e., TCP) layer security protocol is recommended because there are no widely used standards yet available, and because the services provided at the IP and session layers obviate the need for transport layer security.

Page 915 of 3957

Although the Internet protocol stack does not include a session layer per se, the introduction of SSL, SSH, and analogous security protocols has created one. SSL is widely deployed and DoD policy calls for its use for secure web access. We recommend its use with client (not just server) certificates, for high quality user authentication and access control, with transition to TLS (the IETF standard) as it becomes more widely available.

The panel has inserted a "middleware" layer to accommodate systems such as Common Object Request Broker Architecture (CORBA), distributed computing environment (DCE), or Enterprise Java Beans (EJB). However, such systems are not universally required and there is no clear appropriate choice among these competing middleware technologies at this time. Finally, several critical protocols exist at the application layer, and more may emerge. For secure e-mail, S/MIME (v3 with enhanced security services) is the preferred protocol, and it is widely available in COTS products. Secure DNS is an essential infrastructure security component requiring DISA as well as base-level support. Internet Key Exchange (IKE) is the key management protocol used by IPsec. As the extensible markup language (XML) becomes more common, the digital signature standards developed for it will become critical elements of more sophisticated web security designs, supplementing, but not supplanting, SSL/TLS.

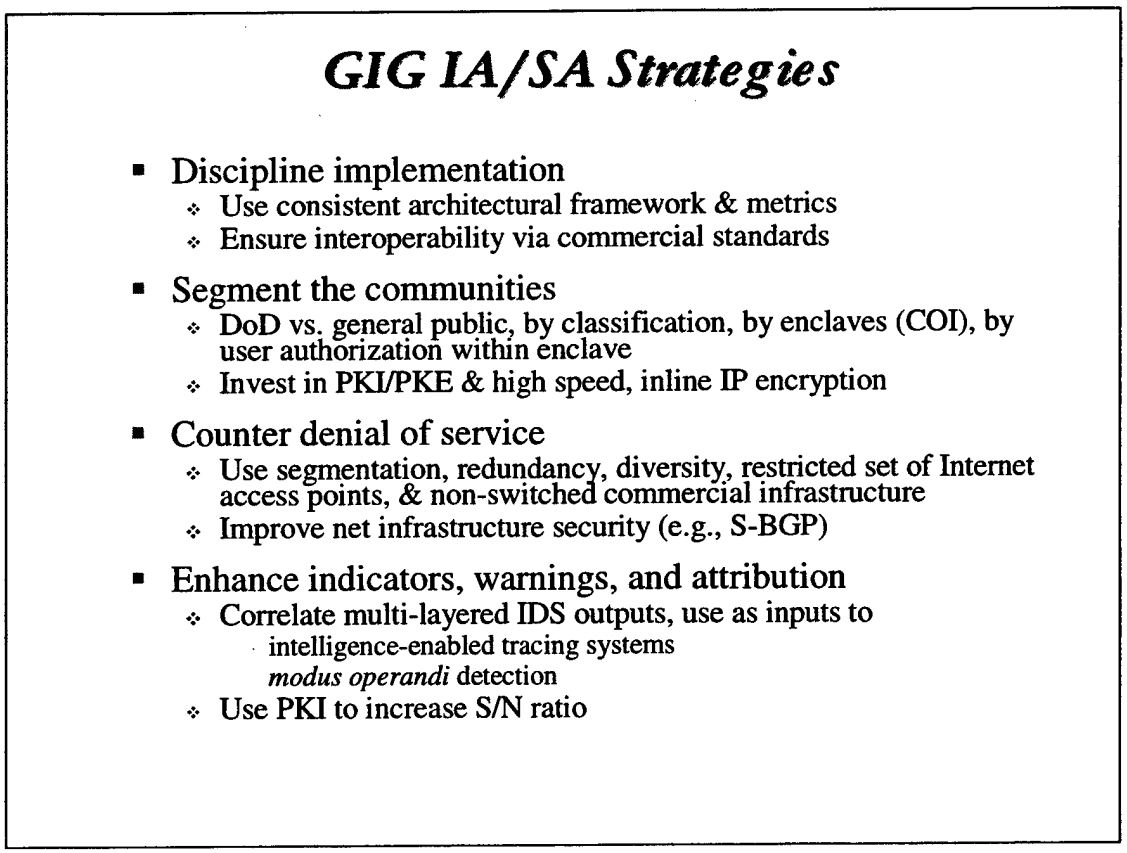


Figure 30. GIG IA Strategies

Figures 30 and 31 outline the GIG IA system architecture strategies recommended by the panel, representing the underlying themes that are embodied in the later recommendations. The first strategy is to use a consistent architectural framework and metrics across the entire DoD

GIG. This strategy lies in contrast to the current divergence of approaches between the services. It is important to foster interoperability via commercial standards, so that commercial and government off-the-shelf technology can be employed throughout the system. The defense-in-depth approach leads to the strategy of segmentation. Segmentation is recommended between the DoD and the general public Internet, between levels of classification, by enclaves (COI), and by individual user within an enclave. In order to support segmentation, investment will be needed in high-speed in-line IP encryption devices, and in large scale PKI and PKE.

Segmentation, redundancy, diversity, a restricted set of Internet access points, non-switched commercial infrastructure, and improved overall net infrastructure security, such as S-BGP (Secure Boundary Gateway Protocol), used in concert can partially mitigate the denial-of-service threat.

Another important element of the strategy is to enhance indicators and warnings and attack attribution. By correlating multi-layered IDS outputs, one can detect patterns of behavior that may indicate a modus operandi. This can be useful in tracing the sources of unwanted behavior. The correlated outputs of host- and network-based IDS at various levels can also be used to direct attention to potential threats. Resources such as human system administrators and various intelligence assets can be directed in this way. The use of a PKI and PK-enabled applications can greatly reduce the noise level of amateur attacks coming into the GIG, and thus increase the signal to noise ratio of the existing indicators and warnings in the GIG.

Fine-grained access control (FGAC) is the principle that allows access to computing and communication resources to be shared, in a safe manner, among a large number of users and user communities. Technology is available to enforce FGAC with an acceptable level of computational overhead, but tools must be available to enable local administrators and users to efficiently manage FGAC for WANs, LANs, and individual hosts and servers.

Accountability is supportive of FGAC and acts as a deterrent to inside attacks. Fine-grained identification and authentication, i.e., via use of level-4 PKI, provides the inputs needed to make FGAC decisions. Intrusion detection mechanisms help detect attacks that have eluded access controls, or activities that represent inappropriate use of resources by authorized personnel.

Page 917 of 3957

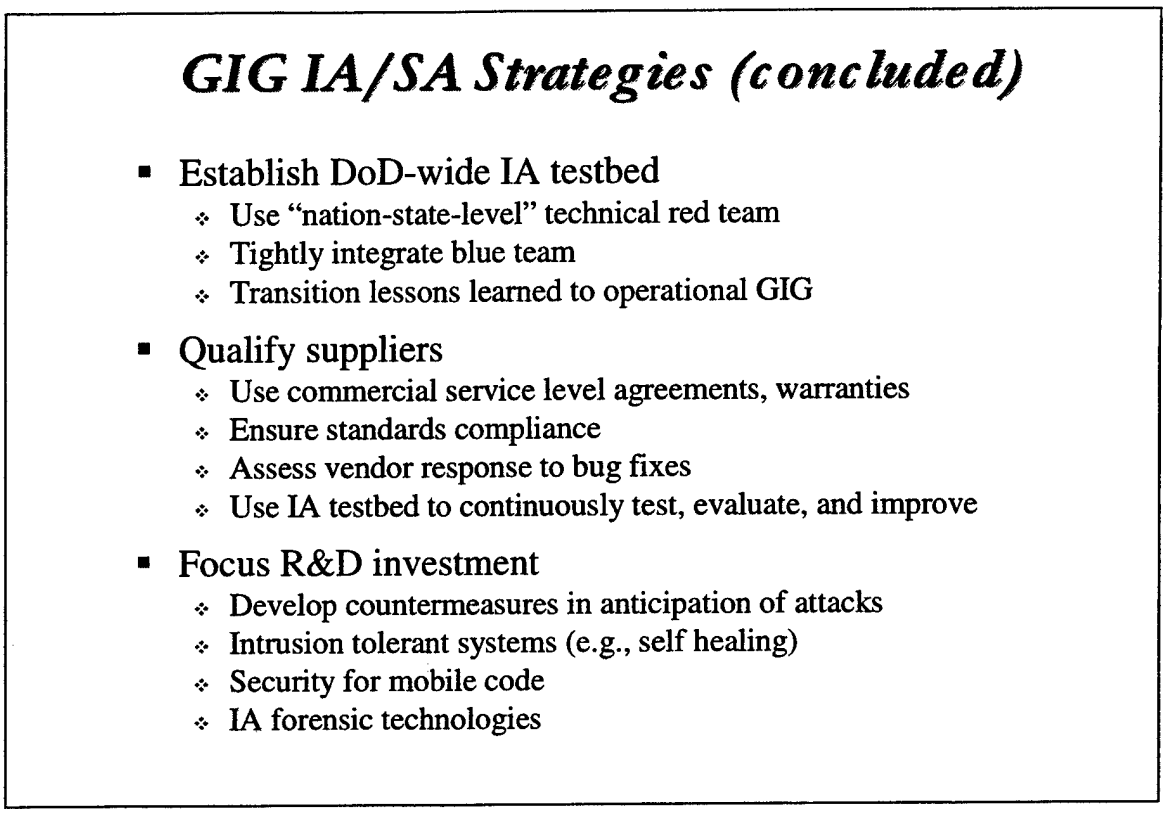


Figure 31. GIG IA Strategies Concluded

The fifth strategy is to establish a DoD-wide GIG IA testbed. This testbed would draw blue team members and current configuration information from GIG operations, and employ a nation-state-level technical red team. The lessons learned through these exercises should be used to upgrade the IA properties of the testbed, and if successful in defense, should be transitioned to the operational GIG. Building an IA testbed avoids the costs and other issues inherent in red-teaming the live operational GIG.

A sixth strategy is to more stringently qualify suppliers of GIG IA technologies than is current practice in government procurement. It is imperative that the DoD becomes a smart buyer of commercial information and information assurance technology and services. Commercial information services can often be bought with service level agreements (SLAs) and/or warranties. SLAs can cover a variety of service aspects. For example, an SLA for a communications service might cover: 1) communication speed, 2) link availability, and 3) notifying the customer within certain timelines of problems. In the future, we expect that SLAs may also address security issues.

It is also important to assess suppliers' conformance with applicable standards. There are numerous organizations that measure and certify compliance with a wide range of standards, such as Underwriter's Laboratory. In the information security area, conformance with the Common Criteria, evaluated under the auspices of the National Information Assurance Partnership (NIAP) is particularly important. The NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The NIAP encourages the development of commercial products with security features as specified in

the Common Criteria, and certifies commercial laboratories to evaluate products against the criteria under NIST's National Voluntary Laboratory Accreditation Program (NVLAP). In implementing the GIG, strong preference should be given to products evaluated under the NIAP.

Another way to qualify suppliers is to gauge their commitment to fixing security-related flaws found in their systems. There are numerous organizations that compile information about vulnerabilities in commercial systems, among them the CERT at Carnegie-Mellon University (www.cert.org), the SANS Institute (www.sans.org), Security Focus (SecurityFocus.com), and NTBugtraq (www.ntbugtraq.com). In implementing the GIG, strong preference should be given to suppliers who have a track record of quickly fixing reported flaws. Furthermore, preference should be given to products that are compatible with the Common Vulnerabilities and Exposures (CVE) list. CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools with a "common enumeration."

Furthermore, while the vulnerabilities of commercial technology need to be understood, the impact on the overall GIG architecture of adding the technology needs to be weighed before employment. We recommend that the GIG IA testbed be used to address this issue. As mentioned above, there is a great deal of publicly available information about technology and product vulnerabilities. The testbed should use this information as a starting point for developing a knowledge base of technology and product benefits and vulnerabilities.

The DoD should develop a deep understanding of how commercial services are provided, so that they can be properly specified when purchased. For example, buying communication lines from multiple suppliers in order to gain redundancy and diversity may not yield the desired results, if each supplier's fiber goes through the same physical switch or runs over the same physical bridge. Instead, when buying a second communication line, DoD should specify that the line share no physical components or transit mechanisms with the first communication line.

The final strategy recommended is to adequately resource a focused GIG IA R&D program. Current DoD IA R&D does not adequately address the IA needs of the GIG. Countermeasures must be developed in anticipation of attacks. The GIG IA testbed the panel recommends can be used to experiment with potential fixes before any form of specific attacks are found live on the GIG. The development of self-healing systems that are intrusion-tolerant and fault-tolerant is an important step in deploying a reliable GIG infrastructure. Self-healing, recovery, and reconstitution of GIG components could provide continuity of operation throughout and after significant attacks. Clear commercial trends point toward mobile code as an increasingly important software distribution and maintenance mechanism. Current practices in some networks of stripping mobile code out of incoming e-mail and disabling Java and JavaScript are stopgap maneuvers. Significant focused research is called for to contain and verify mobile code, to discover new methods of utilizing mobile code to defend against attacks (i.e., throttling incoming traffic at the routers during a denial-of-service attack), and to automatically install 'good' viruses that upgrade system survivability. R&D focused on forensics, tagging, and traceback could provide GIG administrators with the tools necessary to trace attacks back to their source. Non-repudiable identification of malicious attackers and wayward insiders can provide a level of deterrence not currently in evidence.

Page 919 of 3957

4.3 DEFENSE-IN-DEPTH

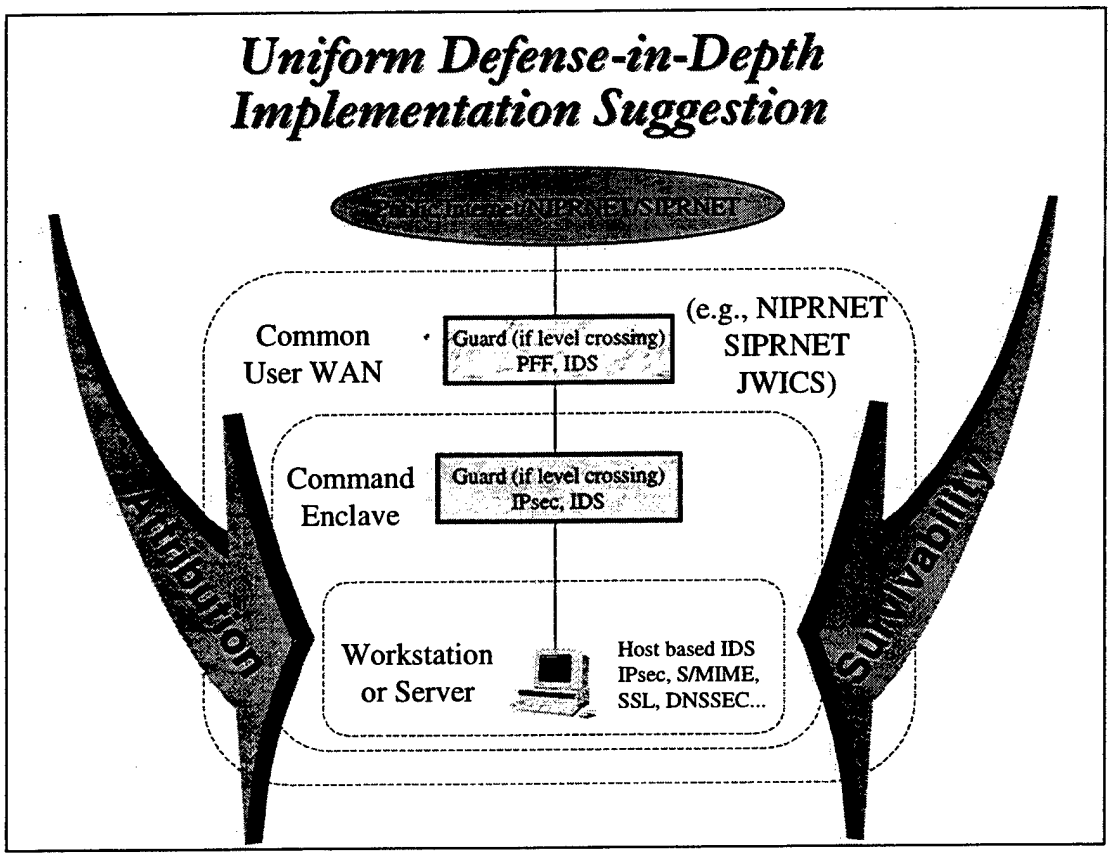


Figure 32. Uniform Defense-in-Depth Implementation

Figure 32 provides an example of layered defense, or defense-in-depth, from a traffic flow perspective. *All* DoD common user networks, SIPRNET and JWICS as well as NIPRNET, should reflect this architecture. This is a departure from current practice in which the classified networks do not provide significant barriers to attacks launched from sites in the same community, i.e., other subscribers to the same common user network.

The outer perimeter represents an interface between a single-level, common user WAN, i.e., NIPRNET, SIPRNET, or JWICS, and a less sensitive WAN, i.e., the public Internet. (If a sensitivity level is crossed, i.e., from SIPRNET to NIPRNET, then a guard is employed.) This perimeter is protected by the use of a (stateful) packet filtering firewall (PFF) and an IDS. Non-IPsec or SSL protected traffic, i.e., e-mail, DNS, and web traffic, is screened via the PFF, and restricted to destinations inside the WAN that are well-defined web servers, e-mail servers, etc. The IDS here is used to screen traffic (at very high data rates) to detect patterns of attacks against multiple sites on the WAN, through correlation of analytic data from each of these IDS systems. Virus scanning might even be applied to (non-encrypted) e-mail attachments at this point, via the use of implicit mail relays.

Page 920 of 3957

At the enclave boundary, IPsec is the primary defense mechanism, preventing unauthenticated connectivity to external sources. A PFF is used for traffic that would not be afforded IPsec protection, i.e., e-mail and DNS services. (As illustrated in later discussion, web data designed to be available for public access will be maintained outside of the enclave boundary.) The enclave IDS has access to some plaintext data (except when IPsec or SSL is used all the way to a workstation or server) and thus can perform more analysis than the WAN IDS. Virus scanning can be applied to (non-encrypted) e-mail attachments at this point, if it is not applied at the WAN boundary.

Each workstation or server is equipped with an IDS, which is monitored by the enclave security administrator. IPsec, SSL, and S/MIME are available for end-to-end cryptographic security, including authentication, integrity, confidentiality, and access control. A secure DNS resolver interacts with secure DNS servers.

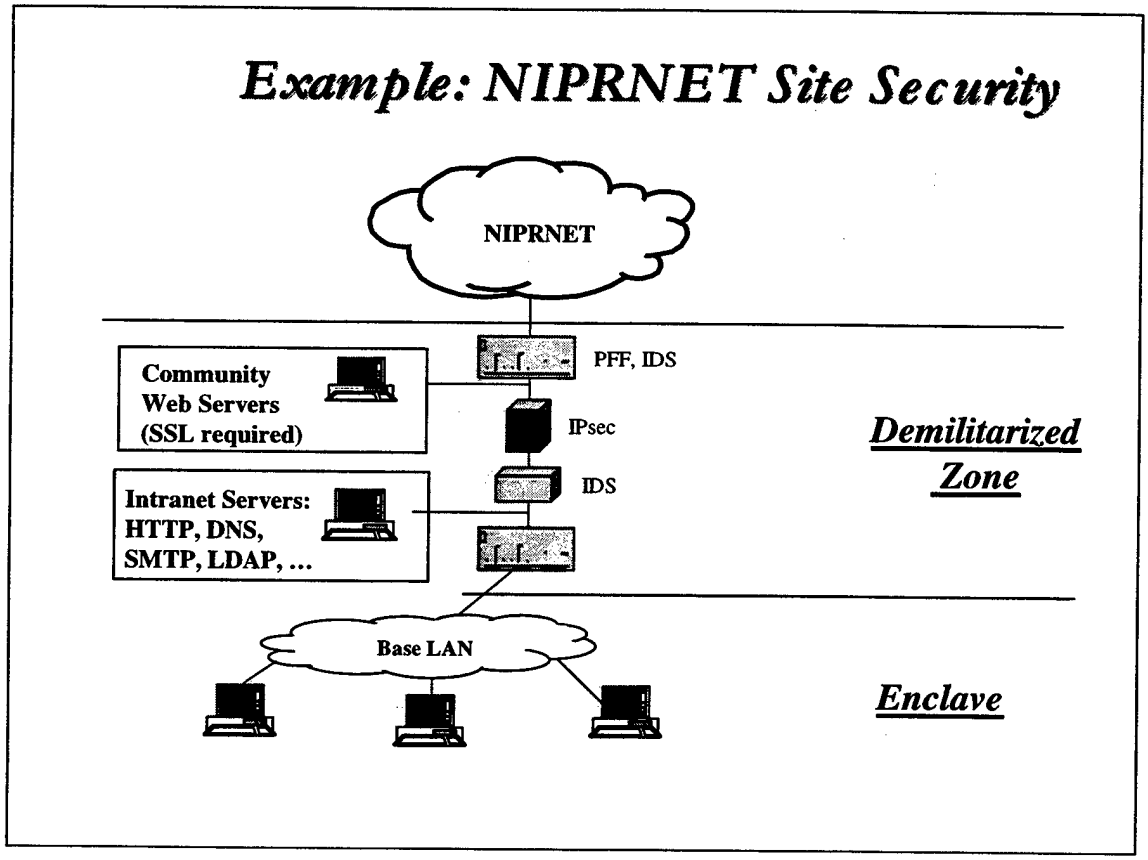


Figure 33. Example: NIPRNET Site Security

Figure 33 illustrates the IA components that would be employed at the interface to a typical NIPRNET site to implement the panel's suggested defense-in-depth architecture. The Packet Filter Firewall (PFF) at the attachment point to the NIPRNET filters out traffic that should never access the web server. The IPsec device in the DMZ is the primary access control mechanism. It implements a basic PFF, as required by the IPsec specifications (RFC 2401). This device, or one immediately behind it, incorporates an IDS that focuses on non-encrypted traffic that traverses

Page 921 of 3957

the IPsec device. Examples of such traffic include transport mode IPsec or SSL traffic destined for machines on the base LAN. (Note, S/MIME protected mail cannot be scanned for viruses at the SMTP server, but any e-mail with viral attachments can be tracked to its sender when S/MIME has been used. This provides reliable attribution of such e-mail, which acts as a deterrent and provides excellent forensics. The host-based IDS will examine incoming e-mail attachments for malicious code upon receipt and decryption.)

The DMZ IDS monitors traffic that bypasses the IPsec device (i.e., DNS traffic or SMTP traffic from the Internet) as well as decrypted traffic from other NIPRNET sites and from contractor sites. (A LAN-based approach may also be employed if technology permits.)

The servers behind the IPsec device are accessed via a mix of plaintext and crypto-protected traffic streams. For example, DNSSEC and e-mail protection is at the application layer, whereas LDAP traffic may be unauthenticated or may be SSL/TLS protected. The latter will be required for access to sensitive directory entries and for all infrastructure management functions.

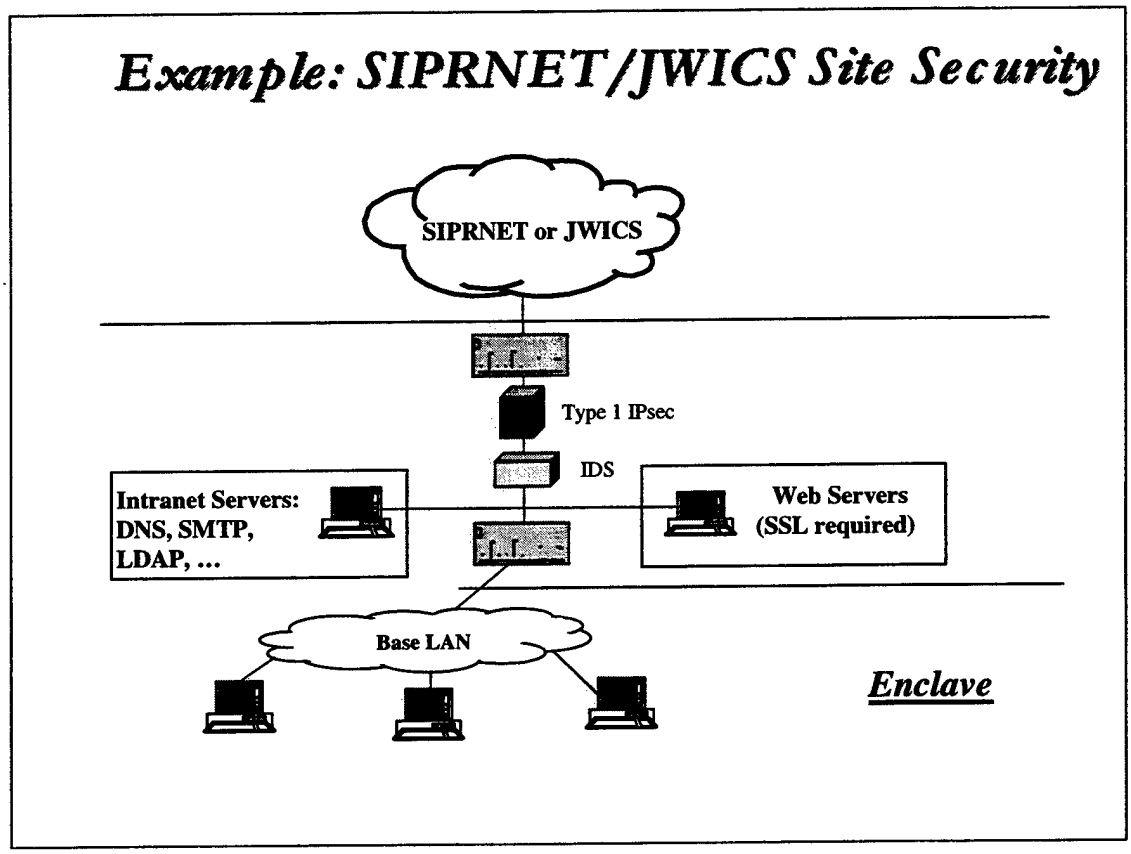


Figure 34. Example: SIPRNET/JWICS Site Security

Figure 34 is similar to the NIPRNET example. Note that there are no DMZ community servers, because all traffic is IPsec protected. This approach is feasible because there is no direct communication with sites not on the same, common user WAN. All sites on SIPRNET or JWICS will be equipped with Type 1 IPsec devices and thus all traffic entering or leaving a site is protected and subject to access controls.

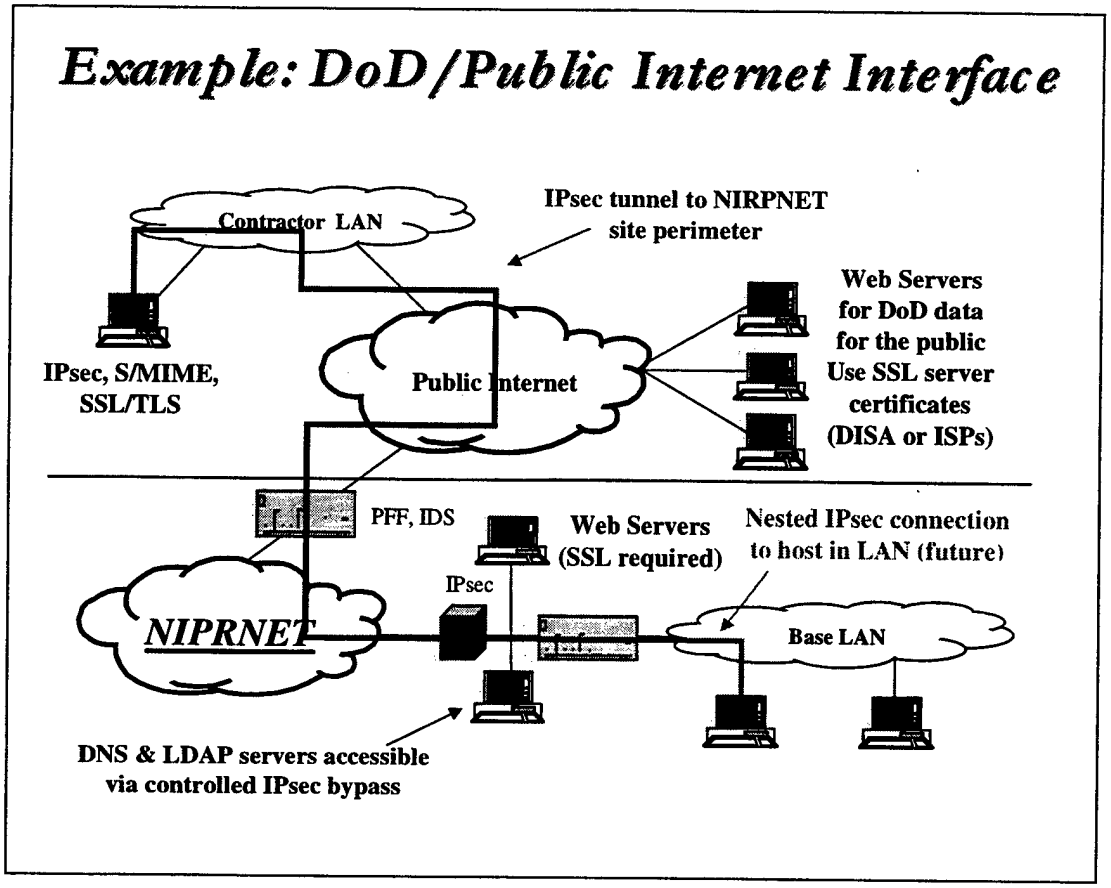


Figure 35. DoD/Public Internet Interface

Figure 35 illustrates the suggested interface between NIPRNET sites and the public Internet. In this approach, all DoD data that is releasable to the general public should be housed on web servers that *are outside of* NIPRNET. This segregation keeps traffic associated with this data off of NIPRNET, avoiding potential congestion on NIPRNET due to "legitimate" access. It also minimizes opportunities for denial-of-service attacks against NIPRNET that masquerade as legitimate access to public Web pages. The web servers holding this data could be operated by DISA on behalf of all DoD activities, or could be outsourced to commercial providers, i.e., ISPs.

Contractors, universities performing DoD sponsored R&D, and other users authorized to access resources on NIPRNET must use secure protocols and employ individual certificates. For example, access to a web server at a NIPRNET site will requires SSL/TLS, with client certificates. E-mail will be protected using S/MIME. The assumption is that each organization will establish a PKI and issue certificates to its employees in order to support these security protocols.

These requirements seem quite feasible. SSL/TLS is integrated into freely available browsers. IPsec is built into Windows 2000 and should soon be available in Sun OS and Linux. (After-market IPsec implementations are available for Windows 95 and 98.) Access to web servers behind the enclave IPsec device makes use of SSL, which is bypassed by the IPsec device (when the destination is one of a set of selected web sever at the site). Most IPsec traffic to a site will terminate at the IPsec device, which enables local IDS examination of the traffic. However, a site

may authorize nested IPsec traffic for true end-to-end security where appropriate. S/MIME e-mail (with triple wrapping) from approved sources is protected all the way to the recipient, while other e-mail is subject to scrutiny at the SMTP server, i.e., attachments will be scanned for viruses and some types of attachments may be prohibited.

Many organizations have, or have plans to establish their own PKIs. Small scale CAs are either free, i.e., Windows 2000, or inexpensive, i.e., the Netscape Certificate Server (which costs about $1,000). The major costs of instituting an organizational (local) PKI are administrative, not capital. Thus it does not seem unreasonable to mandate that organizations doing business with the DoD establish a PKI for secure communication purposes. (The DFAR might explicitly authorize some of the costs of PKI establishment and maintenance as chargeable to DoD contracts.)

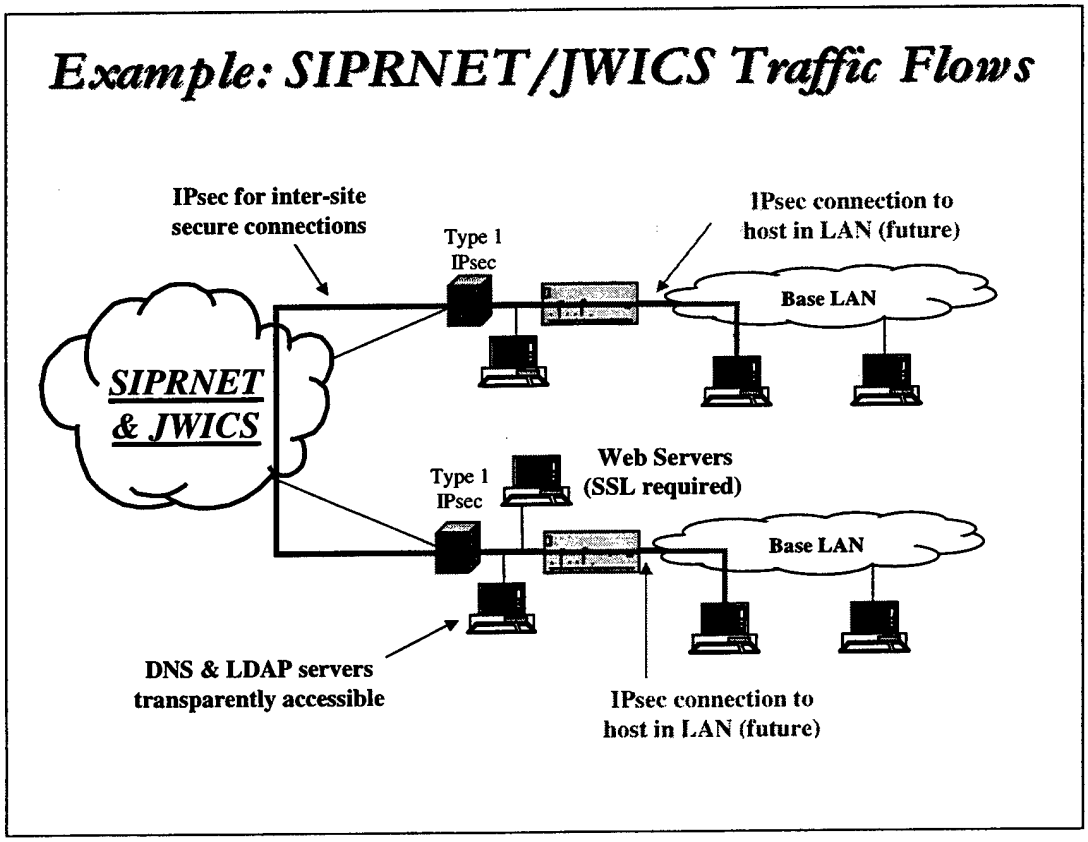


Figure 36. SIRPNET/JWICS Traffic Flows

Figure 36 illustrates connections between users or between a user and server at two SIPRNET or JWICS sites. The Type 1 IPsec devices at the perimeter of each enclave provide confidentiality, authentication, integrity, and access control for all traffic, transparently. Because all inter-enclave traffic is protected by these devices there is not need to bypass traffic. (Special provisions may be required for dual-homed enclaves that need to exchange BGP traffic with routers in the SIPRNET or JWICS backbone.) Thus all servers, including e-mail, DNS, and web servers are "behind" these devices. Each site is responsible for managing the access control lists in the Type 1 IPsec device(s) at its enclave boundary.

When a user in one enclave needs to send or receive data to or from a computer in another enclave, if further protection is required (in support of FGAC), IPsec, SSL/TLS, or S/MIME is employed. For example, all web server access is SSL/TLS protected. S/MIME is used to protect all e-mail. IPsec is employed when accessing other systems where SSL/TLS is not appropriate, i.e., where UDP (vs. TCP) is employed for transport.

Guards, which provide controlled upgrade/downgrade connectivity to networks at different sensitivity levels, are located in enclaves, and thus communication with them follows this same paradigm.

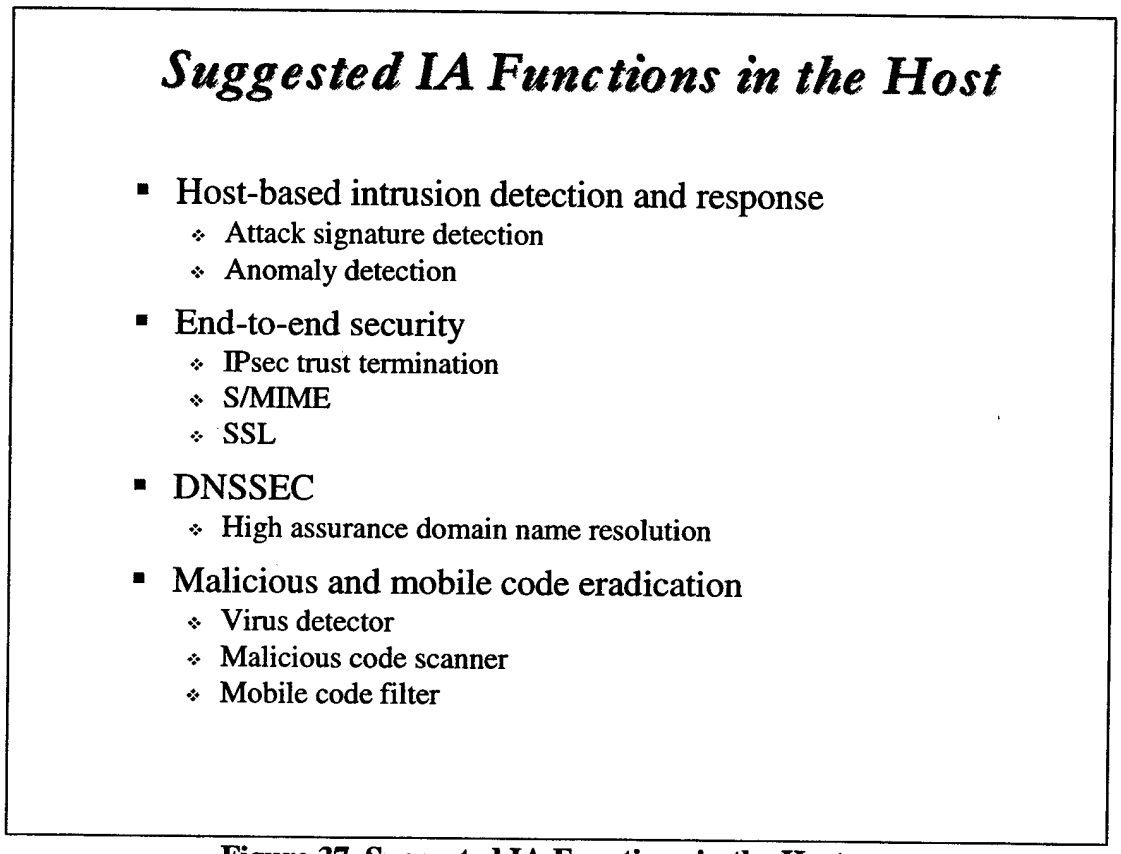


Figure 37. Suggested IA Functions in the Host

In addition to boundary protection provided by the DiD architecture, there are a variety of functions that should be employed to defend the hosts in the GIG. The panel suggests that these be used in all DoD common-user networks, including NIPRNET, SIPRNET, and JWICS.

IPsec, SSL, and S/MIME should be used for end-to-end cryptographic services such as confidentiality, authentication, nonrepudiation, integrity, and access control. A secure DNS resolver should be deployed with secure DNS servers to provide high assurance that a domain name is resolved correctly. A virus scanner, malicious code detector, and mobile code filter should be used to strip any attachments or content violating mobile code policies established within an enclave.

In keeping with the defense-in-depth strategy, host-based intrusion detection and anomaly detection tools should also be deployed. When IPsec is used all the way to the host, the host has the only opportunity to apply serious IDS scrutiny to incoming packets. Since the hosts will experience relatively small data rates, the IDS can be tuned to high levels of sensitivity. The host-based IDS should communicate alert information to other enclave IDS services which can correlate data from network IDS and other host-based IDS deployed in the enclave to obtain a more accurate enclave-wide view of intrusive and other network activity. Signature-based IDS should be kept up-to-date and output monitored by the enclave security administrator.

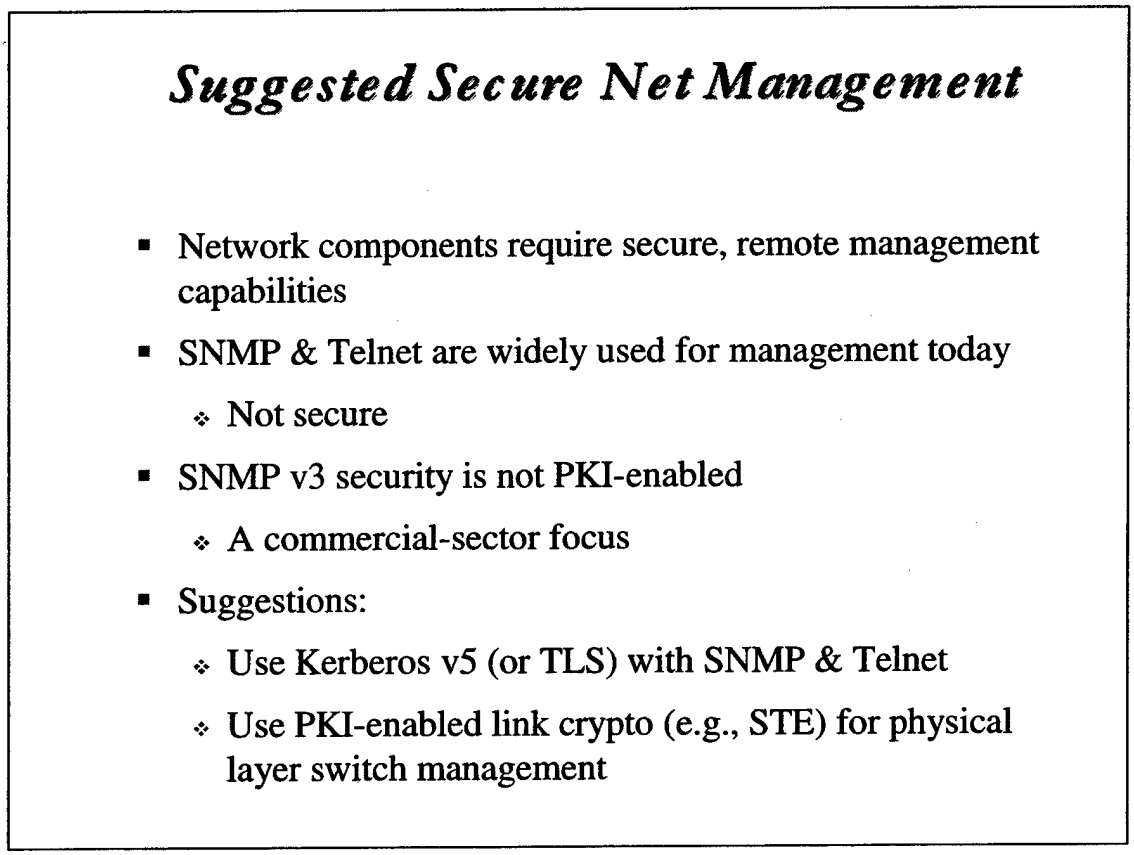


Figure 38. Suggested Secure Net Management

Today, most layer 3 and above network components are managed remotely using a mix of SNMP and Telnet, although some offer web interfaces as well. Simple Network Management Protocol (SNMP) v1 offered no security, and so was used only for getting information from managed devices (for reading MIBs, but not for modifying them). Telnet, even if used with plaintext, reused passwords, was often employed. SNMP v2 had static, symmetric key cryptographic security added, but was not commercially successful. SNMP v3 has improved security services, but still uses manually distributed, symmetric keys. This is not consistent with our proposed use of PKI for user authentication and authorization everywhere else in the GIG. The use of Kerberos for SNMP v3 security has recently been proposed. Version 5 of Kerberos supports X.509 certificates and thus may provide a means of PKI-enabling SNMP v3.

Telnet, secured by Kerberos, is available and used today in some products for secure SETs, and web interfaces for management can make direct use of SSL/TLS. Telnet can also be secured using SSL/TLS.

For the most part, the GIG will not own or directly manage circuits, but when it does, the circuit switches, SONET switches, and the like often require or offer out-of-band management interfaces, i.e., via the PSTN. These interfaces should be secured via link crypto devices that make use of PKI technology, to provide authenticated, integrity-protected, and confidentiality-secure channels. Some such devices are commercially available, and one can use STU-IIIs (or, preferably, the next generation technology, STEs) in this fashion as well.

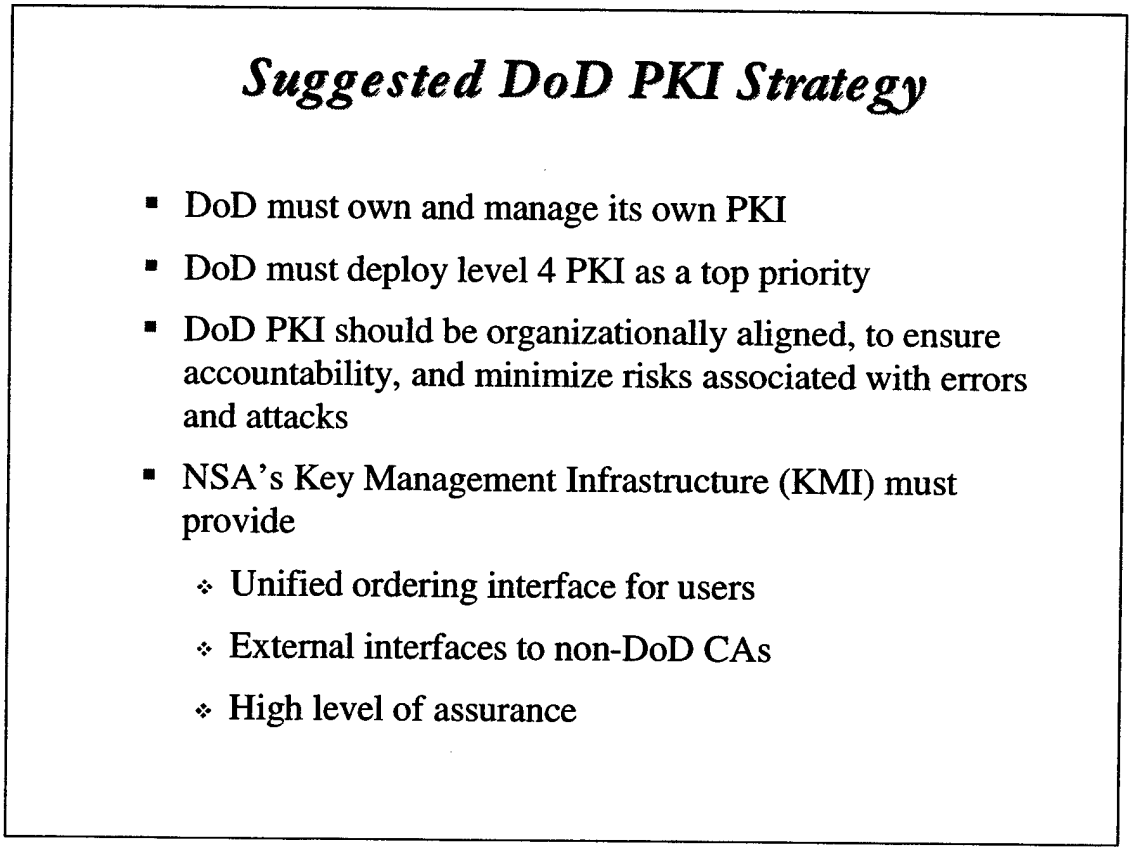


Figure 39. Suggested DoD PKI Strategy

As suggested in Figure 39, DoD should focus on deployment of level 4 PKI. If this requires delaying Common Access Card (CAC) deployment that delay should be tolerated. A PKI is a central element of system security and subversion of a PKI can undermine most layers of a defense-in-depth scheme. Thus it is critical that DoD take responsibility for its own PKIs. The DoD should *not* make use of commercial CAs, although the DoD PKIs must interoperate with commercial PKIs, i.e., to support authentication of DoD contractors.

The DoD PKI should be aligned with organizational boundaries and should use alternate (subject/issuer) name extensions to incorporate DNS names and RFC822 names in order to facilitate native support of security protocols such as S/MIME, IPsec, and SSL/TLS. The NSA

key management infrastructure (KMI) could provide a suitable infrastructure for these requirements. It is critical that certificates be issued along organizational boundaries, to constrain the damage that might result from local security compromises. For example, it must not be possible for an Army CA to issue a certificate that purports to be for an Air Force employee. Current plans for the KMI do not necessarily adhere to this principle and should be modified accordingly. Also troubling is the so-called "bridge CA" concept, developed for inter-organizational cross certification in the federal PKI. Several important PKI security features do not operate properly when a bridge CA is part of a certification path. A bridge CA should be used *only* to facilitate acquisition of public key certificates of other organizations, so that local security administrators can issue cross certificates directly to the other organizations with which they need to interoperate.

DNSSEC is a PKI-like system that provides secure name/address translation support for most Internet protocols. The DNS is global in scope and thus the DoD should encourage widespread adoption of DNSSEC. Within the DoD, high assurance (cryptographic) technology should be employed to protect DoD domains, i.e., the DoD should implement DNSSEC for the .mil and .sml domain and sub-domains.

Directories are essential for widespread deployment of e-mail security (S/MIME), because a sender must retrieve the certificate for a recipient prior to encrypting a message. IPsec and TLS do not rely on directories, except for certificate revocation status information. LDAP is the current, commercial directory interface standard; it is a rapidly evolving standard, of growing complexity. Security for directory access, i.e., via TLS, is improving, but implementations will probably remain significantly vulnerable for some time. The DoD must ensure that the directory systems it deploys make use of the best available load sharing, replication, and security.

Page 928 of 3957

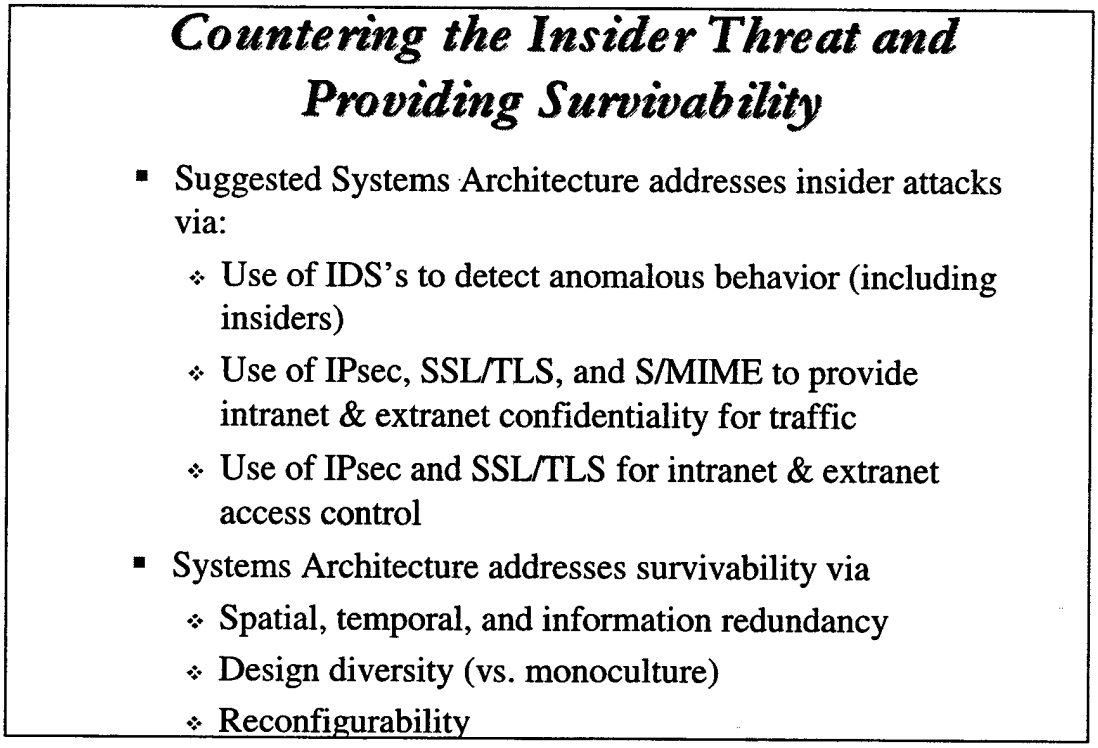


Figure 40. Countering the Insider Threat and Providing Survivability

The panel's suggested system architecture and DiD address the insider threat previously discussed. Intrusion detection systems deployed in enclaves, on user workstations servers and other devices, monitor activity to detect inappropriate (i.e., suspicious) behavior by authorized personnel, as well as attacks by outsiders, which should provide a deterrent to some class of insiders, as well as aid counter-intelligence efforts.

The security protocols cited above (IPsec, SSL/TLS, and S/MIME, level-4 PKI) support fine-grained access control to information in storage on servers and in transit. This fine-grained access control helps prevent a subverted insider from eavesdropping on communications inside enclaves and helps prevent insiders from gaining access to servers or to other enclaves without explicit authorization. Because all of these protocols make use of PKI technology for authentication, the resulting audit trails also help to detect and deter insider misuse.

Survivability is addressed through the use of redundant servers, access lines, and local interfaces (i.e., multi-homing), and via dynamic routing in common user WANs.

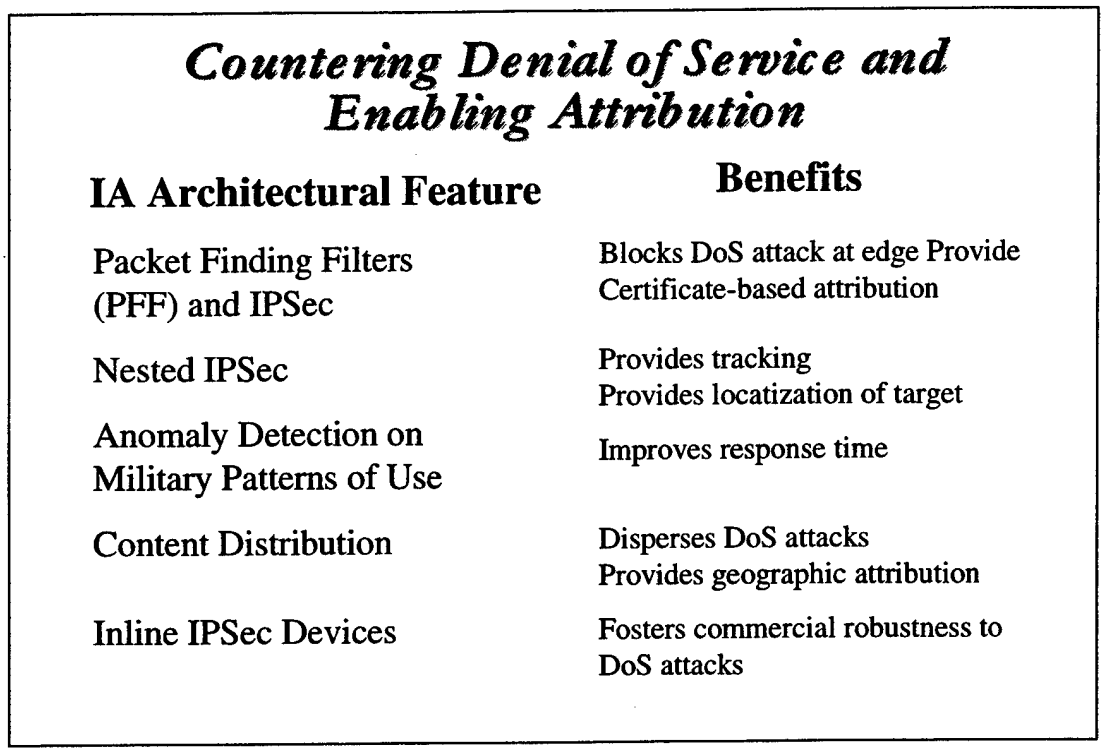


Figure 41. Countering Denial of Service and Enabling Attribution

In Figure 41, the panel suggests architectural elements that counter denial-of-service and provide partial ability to attribute attacks back toward their origins. The stateful packet-filtering firewalls installed at the boundaries should be configured to reject Internet Control Message Protocol (ICMP) echo and reply messages, and to throttle SYN messages to limit the number of half-open connections. Smurf attacks depend on ICMP echo reply (as well as other questionable mechanisms) that can easily be stopped at firewalls. Synchronization (SYN) floods depend on overflowing the fixed-length queues of TCP, so by throttling the number of SYNs allowed into a network, perhaps contingent on the completion of connections, one can limit the DoS potential at the firewalls.

There is a potential performance penalty associated with such throttling, but this can be managed. In the Feb 2000 distributed denial-of-service attacks, approximately 80% of the attacks were Smurf, and 15% were SYN floods. Thus approximately 95% of Feb-2000-style DoS attacks would be mitigated by present and suggested firewalls at the enclave boundaries.

The panel recommends the use of IPsec, which prevents denial-of-service within the enclaves. Further, future nested-IPsec implementations can counter denial-of-service and assist attribution by target localization and path tracking. The panel recommends research and development of networked IDS visualization tools for semi-automated sysadmin response, which would improve the time to response to a DoS attack. (It took days for sysadmins to identify the first DoS attack for what it was.) The panel also recommendation to employ anomaly detection can be configured to exploit known military patterns of use, and can trigger responses perhaps including dynamic user reauthorization. Content distribution networks, such as those run commercially by Akamai and Digital Island, provide additional mechanisms to counter DoS attacks. The static content of public DoD web sites can be replicated in a similar way. For public

Page 930 of 3957

DoD web sites using SSL server certificates to prevent web site defacement the current commercial offerings are inappropriate. Some content-distribution approaches provide a partial geographic attribution. Finally, the panel recommendation to support development of high-speed inline IP cryptographic device could foster widespread commercial IPsec use, initially in large multinational corporations. Together, the panel recommendations partially address denial-of-service attacks on the GIG and provide initial attribution capabilities.

4.4 METRIC SUGGESTIONS

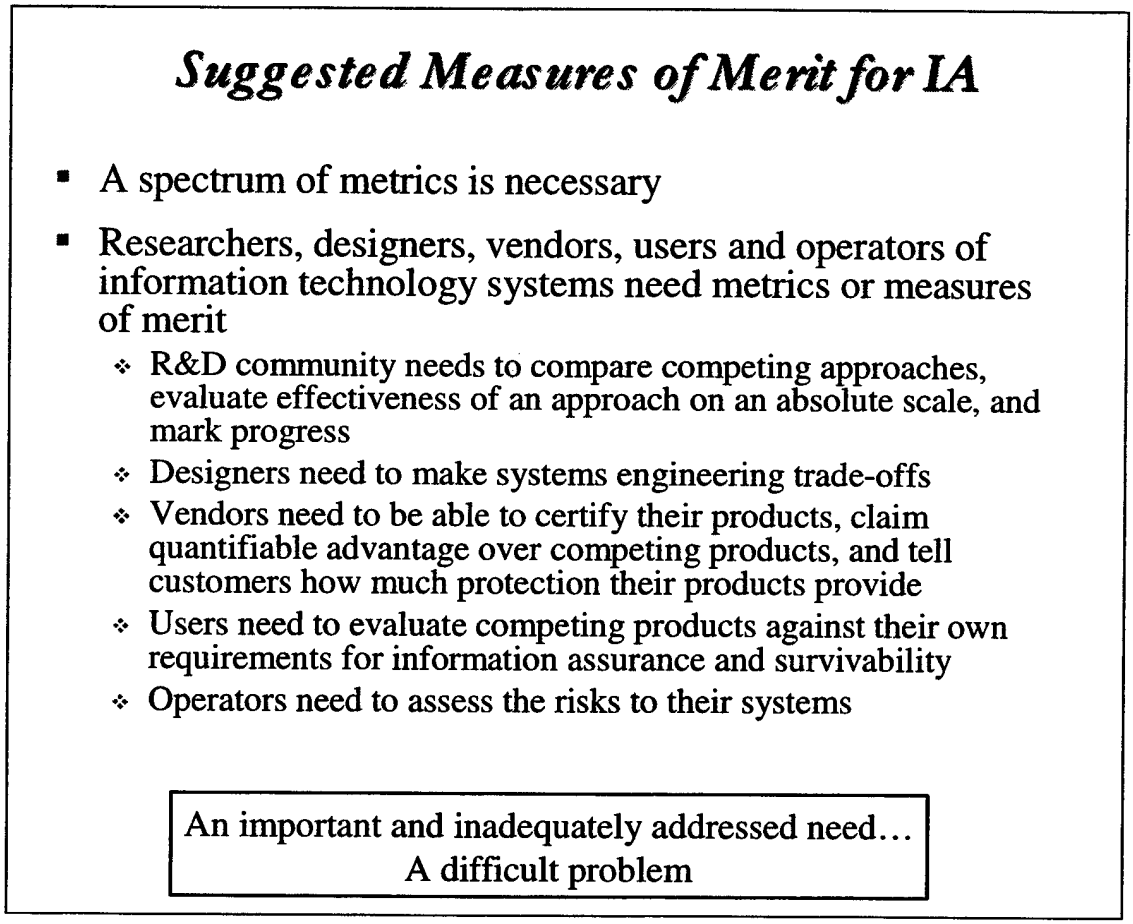


Figure 42. Suggested Measures of Merit for IA

Metrics for information assurance and surveillance architectures are an important and inadequately addressed need. Researchers, designers, vendors, and operators of information systems need a broad spectrum of metrics to achieve their respective objectives. From a systems perspective there is a need to develop metrics for technical-, system-, and mission-level evaluation. This development will require collaboration amongst technical, evaluation, and operator communities. A testbed is required to provide a means for measurement of system performance given different scenarios and related information traffic. The defense-in-depth systems architecture and metrics-measuring capability facilitate new capabilities for indications

and warning. Figures 42 and 43 provide a few examples of how the metrics may be utilized by different communities at different stages of the lifecycle of a system.

The research and development community must compare competing approaches, evaluate effectiveness of an approach on an absolute scale, and mark progress as a function of time. This paradigm of common metrics, validated training, and test data has proven to be extremely successful in areas such as speech, speaker, and language recognition.

Designers need to make systems engineering trade-offs. This is particularly true when attempting to trade complexity for performance.

Vendors need to certify products, claim quantifiable advantage over competing products, and tell customers how much protection their products provide. Metrics enable an Underwriters Laboratory (UL) approach to evaluating commercial products, i.e., common data, measurements and analysis. There has been progress on this front over the last 17 years, starting with the Trusted Computer System Evaluation Criteria (TCSEC) "Orange Book," progressing to the Information Technology Security Evaluation Criteria (ITSEC), and now the Common Criteria (CC) version 2. However, there are still questions about the viability of such security evaluation criteria, as noted in the recent National Research Council report, "Trust in Cyberspace."[7] Thus one should not expect that component evaluation will, by itself, "solve" the problems we face in engineering secure systems. Thus the approach described below, which emphasizes development of IA metrics for fielded systems, is critical.

Users need to evaluate competing products against their own requirements for information assurance and survivability. Operators need to assess the risks to their systems. Measures of merit or metrics for information assurance and survivable architectures is an important and inadequately addressed need.

---

[7] Trust in Cyberspace, Committee on Information Systems Trustworthiness, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press, Washington, DC 1999, Fred B. Schneider, Editor

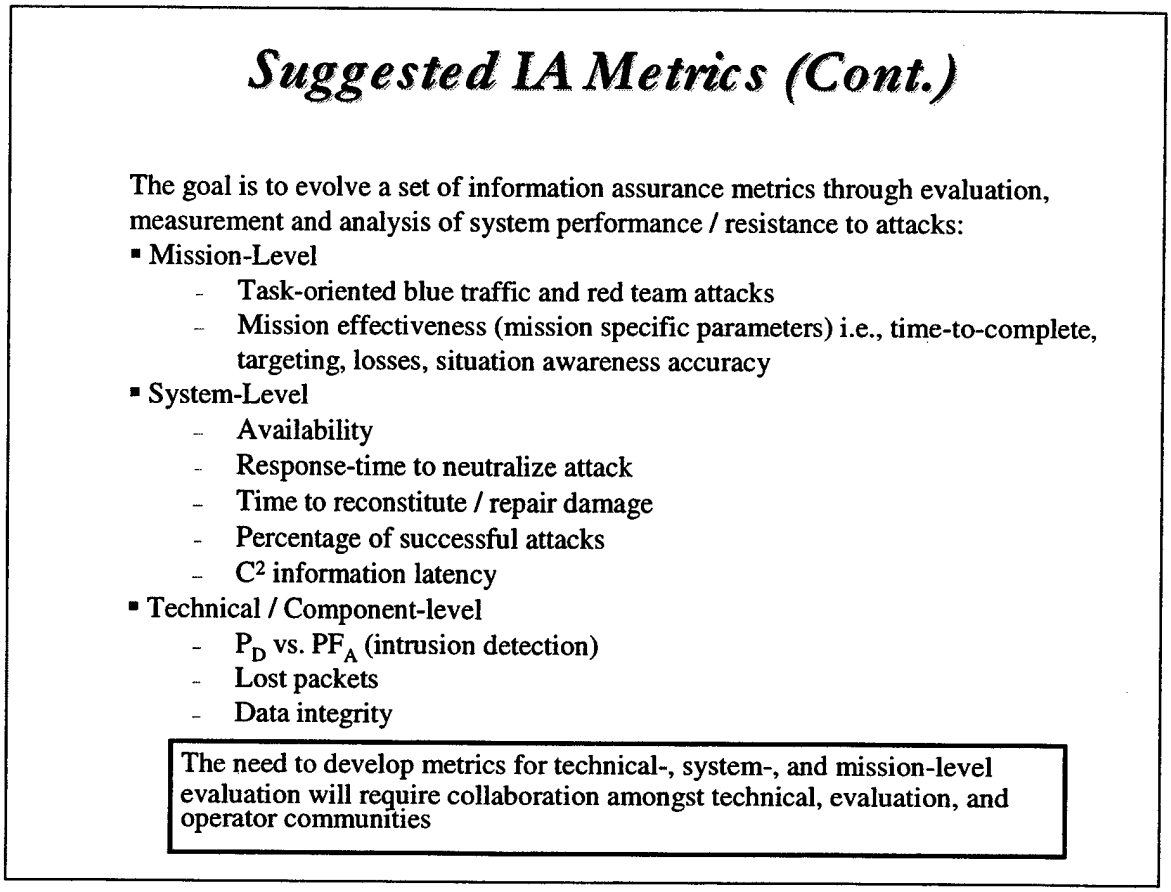


Figure 43. Suggested IA Metrics

The overall challenge, based on the architectural environment and an evolutionary experiment, evaluation, and analysis process, is to develop a set of information assurance metrics to measure system performance in the face of a wide-ranging set of attacks. At the mission-level, the metrics will involve task-oriented blue team operations and traffic and red team attacks to evaluate overall mission effectiveness. Mission level metrics would cover such topics as time-to-complete, targeting success, losses, situation awareness, timelines and accuracy, etc. Systems-level metrics are related to mission-level metrics but are finer grained and would cover overall system availability; response time to neutralize attacks, reconstitute and repair damage; percentage of successful attacks; and C2 information latency. At the technical and component level, suggested metrics include specific measurements of probability of intrusion detection vs. false alarms, to provide a basis for performance quantification. In addition, measurements of packet loss and data integrity and losses will provide a means for evaluating the overall performance of information systems. The relationship of measurements and performance at all levels will require collaboration amongst the technical, evaluation and operator communities.

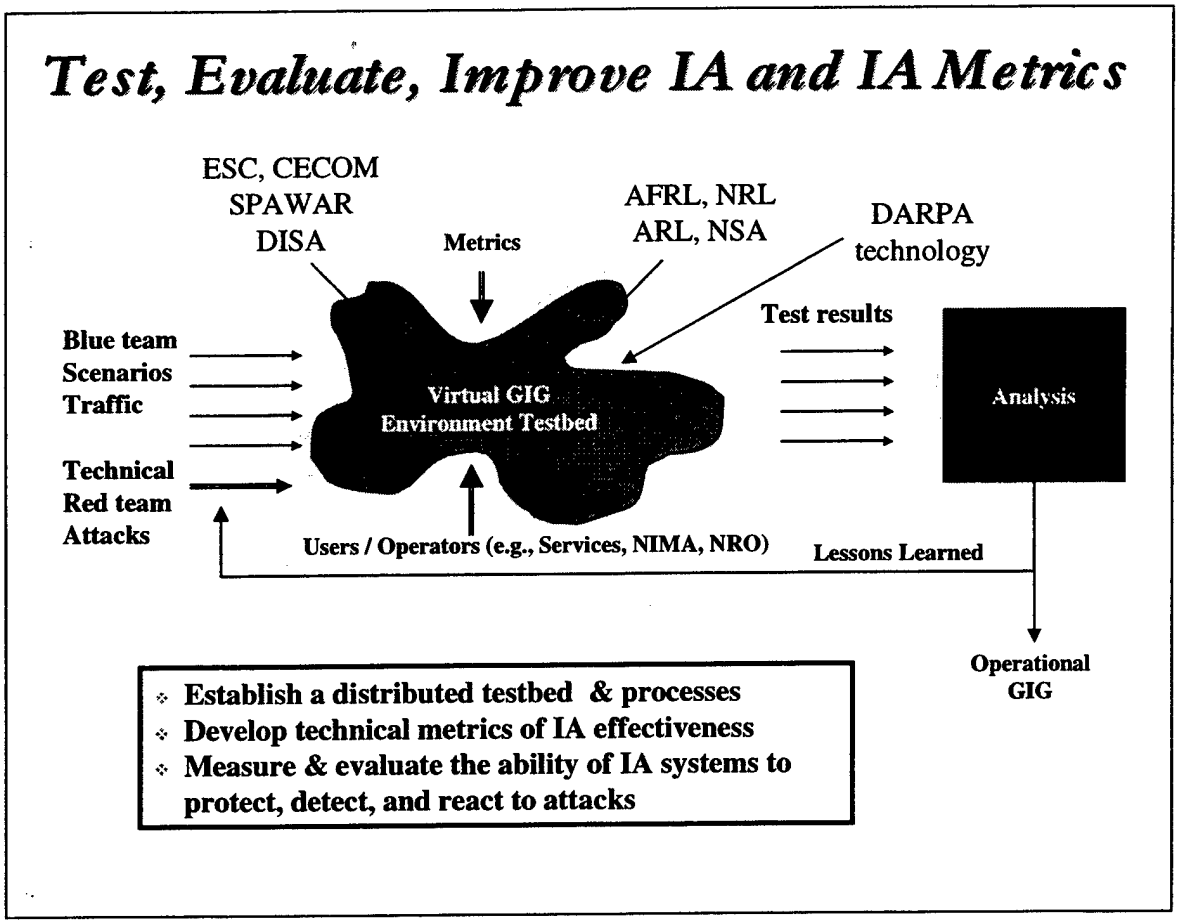


Figure 44. Test, Evaluate, Improve IA

The goal of information assurance metrics is to evaluate the ability of information assurance systems to protect, detect and react to attacks. As noted in Figure 44, to achieve this goal it will be necessary to establish a distributed testbed and processes for developing information assurance effectiveness metrics. Testbed nodes should be located at the U.S. Air Force Electronic Systems Center (ESC), U.S. Army Communications Electronics Command (CECOM), Space and Naval Warfare Systems Command (SPAWAR), Air Force Research Laboratory (AFRL), NSA, etc. The participants in the evaluation process will include research and development, evaluation, and operational communities (services and agencies). The testbed will provide a means for measurement of system performance in the face of red team attacks on blue team scenarios and related information traffic. The testbed will also serve as a primary means for DARPA information assurance technology insertion and evaluation. The metrics and measurements will evolve as results are analyzed and lessons learned are derived from the data. Lessons learned will be fed back to red and blue teams to refine and update strategies and will be used by developers to improve system defenses. Lessons learned will also be made available to the GIG architects and system engineers to improve IA.

This evolutionary process is essential to achieving a commonly accepted basis for measuring effectiveness of information assurance systems. The overall process represents a journey rather than a destination. Change is inevitable for offense, defense, infrastructure and particularly for COTS components. Measurement and evaluation of the ability of information assurance systems

to protect, detect, and react to attacks by adversaries must track these changes to achieve continued protection.

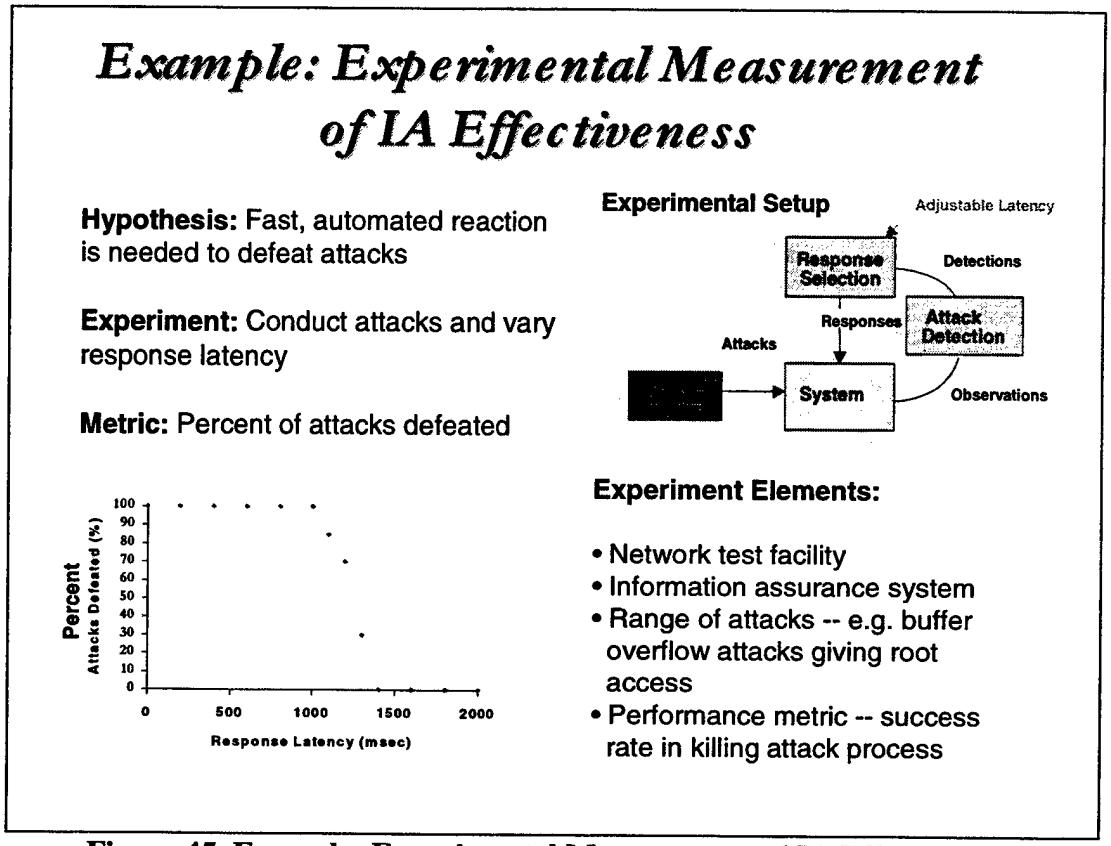


Figure 45. Example: Experimental Measurement of IA Effectiveness

Figure 45 is an example of a recent experiment to measure information assurance effectiveness. In this case, an experiment team including information assurance systems developers, and attack developers, was assembled to measure the effectiveness of an Information Assurance System response to detected attacks. The IA system has the capability to detect attacks and to respond in a variety of ways, i.e., by killing the attack process and removing attack scripts that may have been planted by an attacker. The latency of response time is an experimental variable – by waiting longer to respond, the IA system learns more about the attack, but might be too late to defeat the attack. The example set of attacks is built around "buffer overflow" attacks, where the attacker exploits weaknesses in the operating system to become "root," or "superuser."

An example of the experimental results is shown, where it is seen that a fast response (< 1 sec) defeats all attacks, while a slower response (>1.5 sec) fails to defeat any attacks. The experiment metric – percent of attacks defeated – is simple, but the experiment design, the team required, and the scenario development, illustrate the major components required for experimental measurement of information assurance effectiveness.

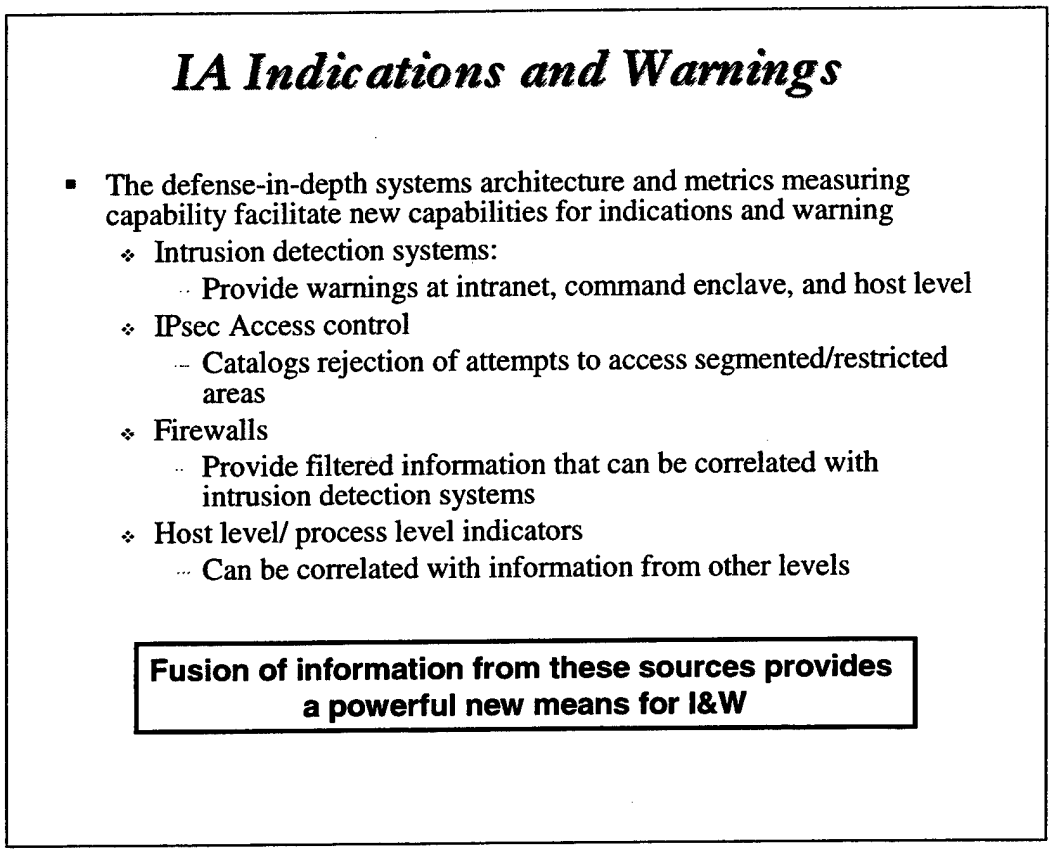


Figure 46. IA Indications and Warnings

As stated earlier, metrics for information assurance and survivable architectures are essential to achieving the broad spectrum of objectives of researchers, designers, vendors and operators of information systems. By implementing the defense-in-depth system architecture previously described, not only is system performance significantly improved, but a new set of system data (metrics) becomes available for indications and warning, as noted in Figure 46. The indications and warning data derive from a number of sources: 1) intrusion detection systems provide warnings at intranet, command enclave and host levels; 2) IPsec access controls provide data on illegal attempts to access segmented and restricted areas; 3) firewalls provide filtering information which can be correlated with data from intrusion detection systems; and 4) host-level and process-level indicators can be correlated with data from all of the above sources. The net result is that this multilevel, highly filtered data can be fused together to provide a powerful new means for facilitating indications and warning at multiple levels of the defense-in-depth architecture.

4.5 WIRELESS SUGGESTIONS

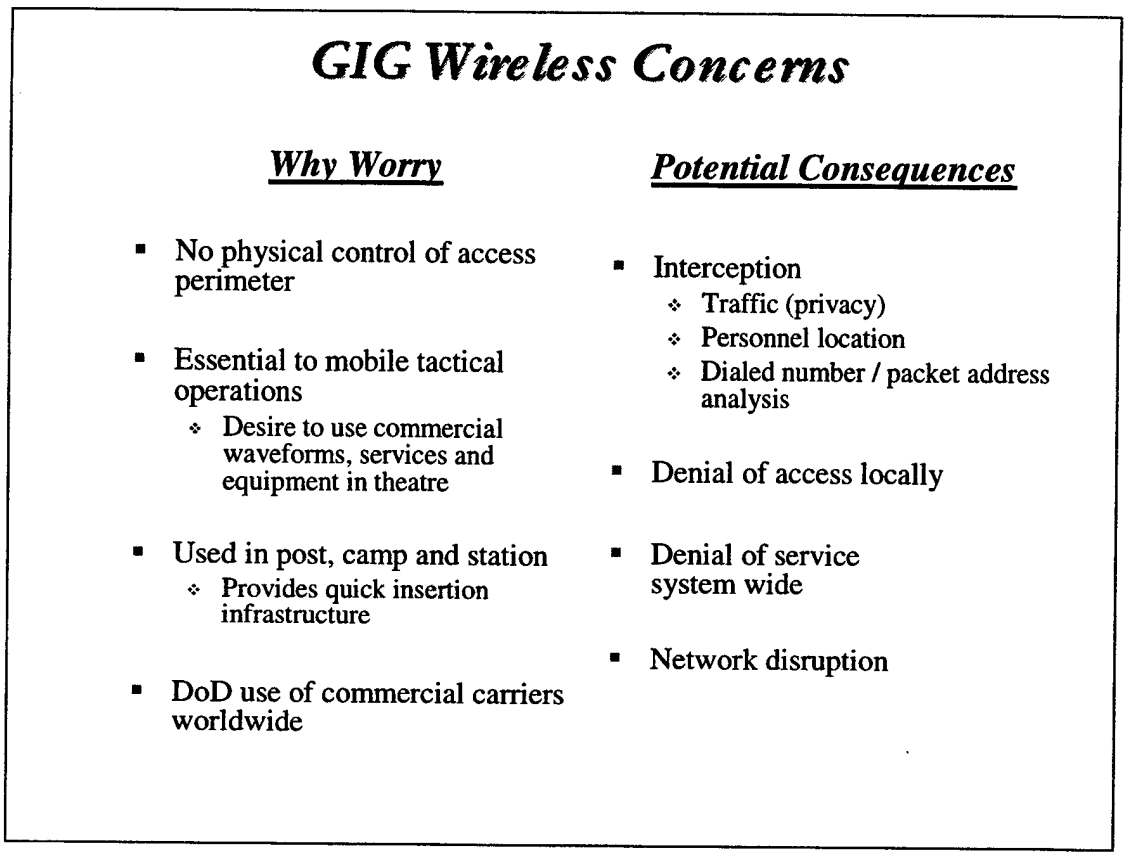


Figure 47. GIG Wireless Concerns

Since before WWII, wireless facilities have been part of military operations. They have been used in radio trunking throughout the upper echelons of the force and in tactical radio nets in the lower echelons of the force. From an information assurance perspective, wireless links merit special consideration, as noted in Figure 47, because they are not confined to a physical perimeter and can be observed from as far off as space.

Recognition of wireless observability and the Soviet radio electronic combat doctrine caused these links to be both encrypted and protected against jamming. In the last twenty-five years the tactical forces have procured a wide variety of secure radio systems. Wireless facilities will continue to enable mobile military operations. Recently, efforts to "digitize" the battlespace have demanded an increased bandwidth. Increased bandwidth systems will typically have shorter ranges and thus require "ad hoc" networks to move the data around the battlefield. As a result, networked communications will move further forward in the tactical area.

Projections indicate that data will be an ever-increasing part of mobile military operations, while the level of voice information will be relatively static. Consequently it can be expected that voice and data services will ultimately be provided above a common wireless/wired tactical Internet (the GIG). Thus the security of the wireless networking is essential to the performance of

the system. In the civilian world, the use of wireless has been rapidly exploding. Mobile personal communications systems, such as terrestrial cellular services and satellite-based services, represent large economic investments. They provide ubiquitous, near-global access to the public switched telephone network from small, inexpensive user devices.

JV2020 envisions similar universal, on-the-move, information access for the military. Similarly, there are a number of emerging fixed wireless systems in use for wideband data and video access to the home. These systems are commercially attractive because they can provide service with a minimal infrastructure. For the military they can also provide "instant infrastructure" in existing and deployed post, camp and station facilities. While the use of these commercial capabilities in the GIG is attractive, these systems will be subjected to attack and, if compromised, could have system-wide impact.

Passive interception and observation of links can provide information on user location, traffic content, called party, and pattern of use. Commercial providers are incorporating some forms of privacy in their systems to prevent well publicized eavesdropping and fraud. However, network signaling information is generally available and can be used to deduce information or attack the system.

Active intervention in a wireless system, either by jamming or the use of equipment to render a system "busy," can deny access to communications service in a geographic area. More sophisticated attacks can deny particular users, or user communities, use of wireless facilities. All mobile systems depend on some system level database to allow calls to find a user. Attacks on these databases, either outright or through exploitation of fraud prevention safeguards, can disable use of worldwide wireless facilities.

Finally, as discussed subsequently the exploitation of network control structure can cause failure of the entire network. There have been examples of such failures in commercial networks due to software defects, and similar scenarios can occur due to either induced misbehavior or the use of wireless links to introduce false control signals into the network.

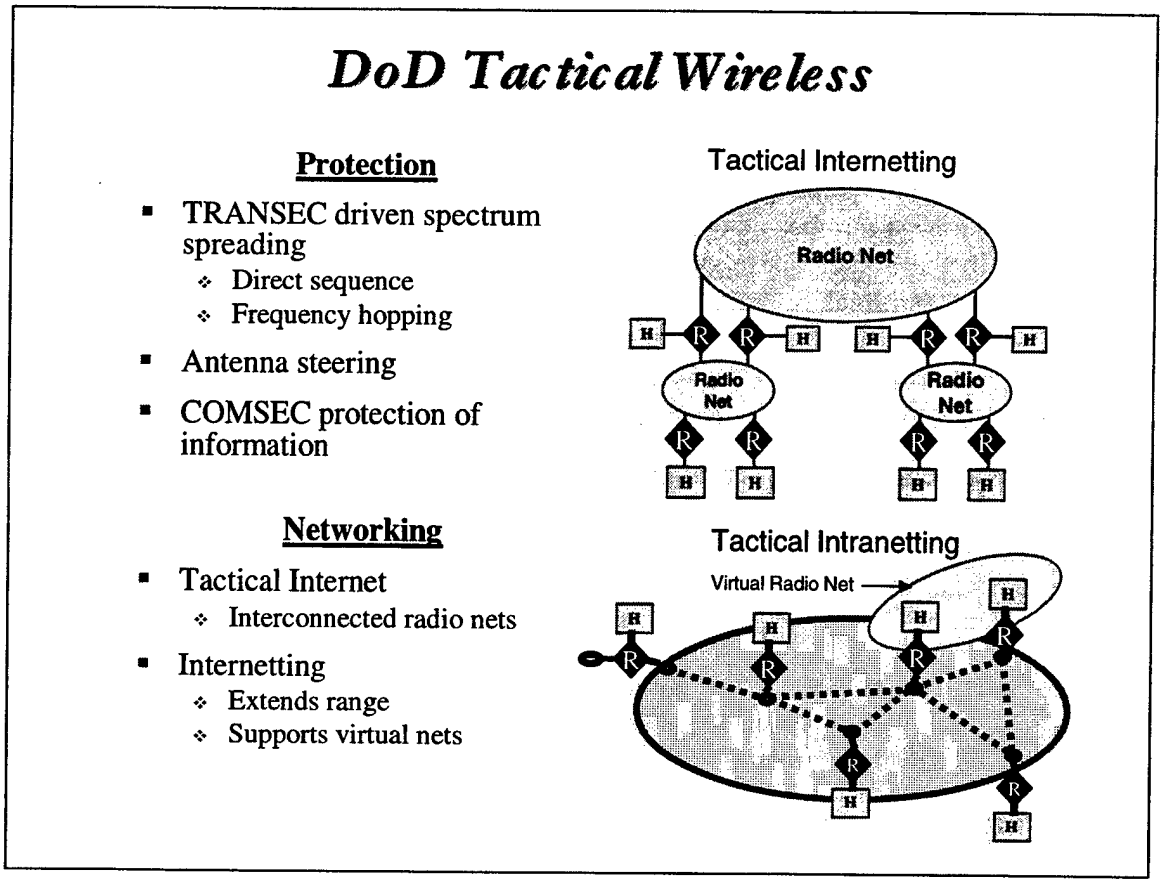


Figure 48. DoD Tactical Wireless

The DoD has led the technology development of a wide range of countermeasures to physical level attack on wireless links. These techniques may be employed individually or in concert. As noted in Figure 48, the standard technique for countering jamming is the use of spread spectrum techniques, which can be carried out with either frequency hopping or direct sequence spreading or a combination of both. The basic strategy common to both is to spread the information across a wide range of frequencies so that the jammer has to dissipate his power over the whole spectrum, while the desired user can exploit his private spectrum access information to reject the jamming signal. Adaptive antenna arrays have also been used to spatially reject a jammer. On most tactical radio links today the information is protected by COMSEC, typically embedded in the radio.

In the forward tactical area, radio nets have traditionally served single organizations. Recently there has been a desire to move digital information across multiple radio networks to achieve wide area connectivity and coordination. Initially this has been accomplished by using routers to interconnect secured radio nets, with the routers operating on decrypted traffic (system high). The Army's interconnected system is referred to as a Tactical Internet. Various exercises have shown that the routers are vulnerable to intrusion.

With a demand for higher bandwidth and robust connectivity, the emerging system concept is to separate the radio resource from the application. In this model the radios form an intranet where each radio handles all traffic in its area. The organizational communications are then achieved as a "virtual" net – above the radio infrastructure.

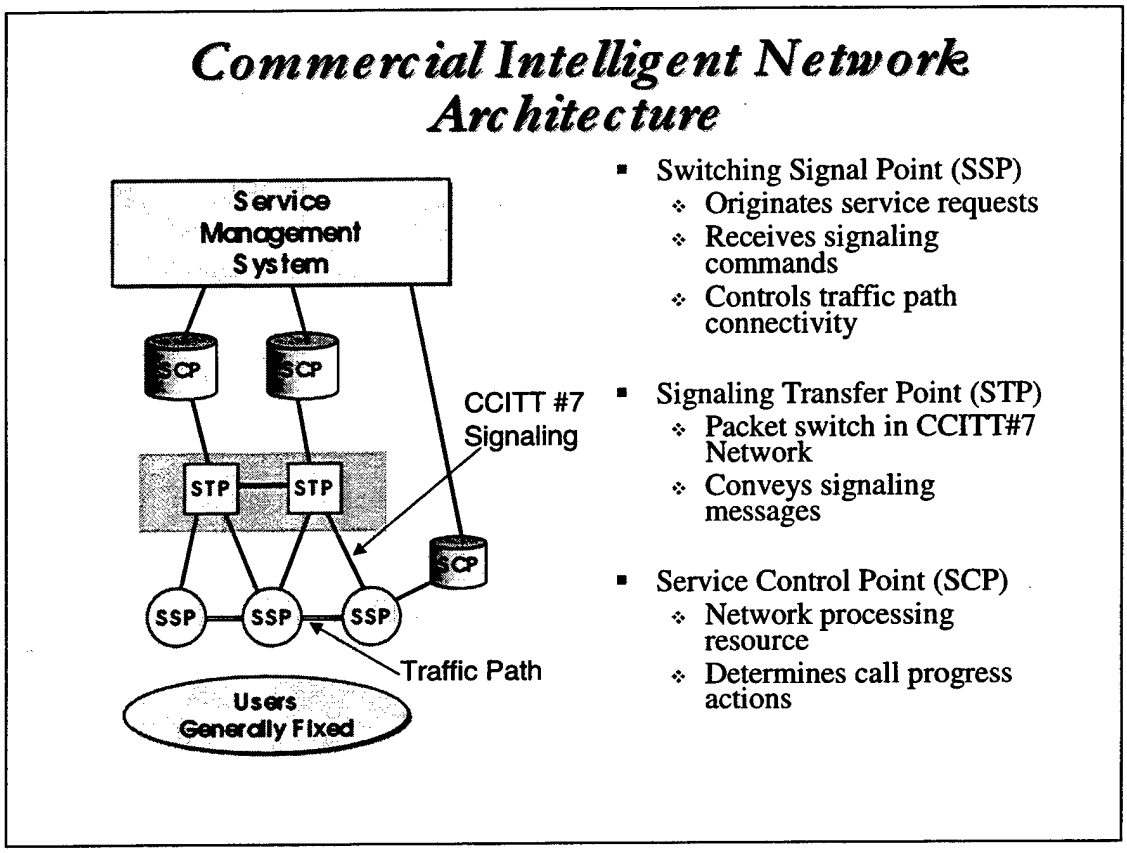


Figure 49. Commercial Intelligent Network Architecture

The GIG will use communications links in the Public Switched Telecommunications Network (PSTN). In the 80's, telecommunications providers developed and deployed a system architecture termed the "Intelligent Network" (IN) noted in Figure 49. This system architecture separated the signaling and control portions of the network from the interconnection process, so that advanced, revenue-producing, call-handling services could be provided. In this system model, a Service Switching Point (SSP) takes a subscriber's request for service and forwards messages through a network of Signal Transfer Points (STP). STPs are packet switches deployed throughout the telecommunications network. The originating SSP uses these messages to request information from Service Control Points (SCP) on how to respond to the service requests. Service Control Points (SCP) contains system-level data and processing services. In response to these requests, messages are sent to all switching points required to complete the response to the call request. The suite of protocols used to communicate these control operations has been standardized by the CCITT international standards body and is referred to as Signaling System #7 (SS7).

Access to the Signal Switching point is across an access facility. Traditionally this point has been twisted pair and considerable effort has been made to move ever-increasing data rates across this copper plant. In the 1980s, Integrated Service Digital Network (ISDN) was deployed to provide144 kbps to subscribers. More recently, higher rates have been made available through Digital Subscriber Line (DSL) technology.

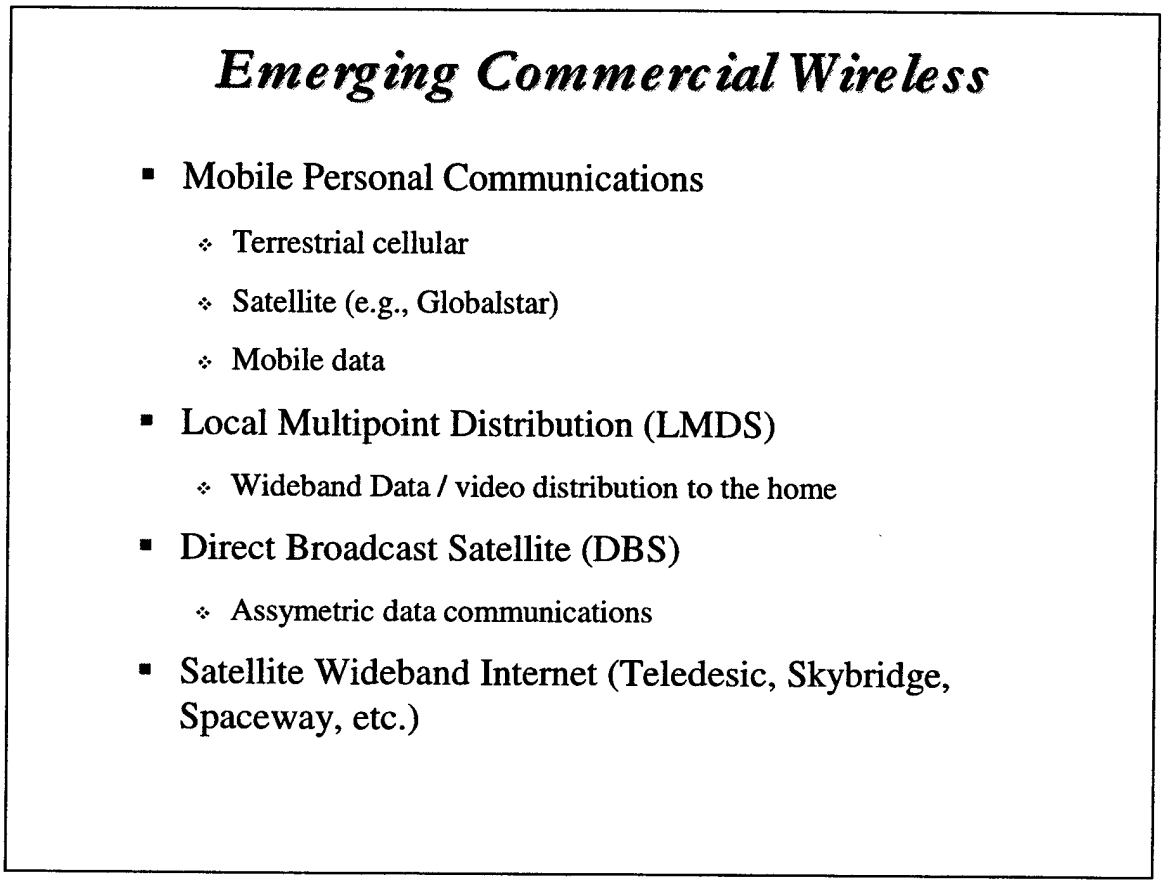


Figure 50. Emerging Commercial Wireless

The majority of the recent wireless explosion has been in the area of wireless access to fixed infrastructure. Cellular and personal communications systems (PCS) technologies, for example, use wireless access to deliver mobile users both switched voice services and narrowband data services. Low earth-orbiting satellite systems are in the early stages of deployment. These systems allow a user access to the fixed infrastructure across a wider roaming area where terrestrial base stations may not be available. In addition, as shown in Figure 50, there are high-speed wireless access technologies, such as the Multichannel Multipoint Distribution System (MMDS) and Local Multipoint Distribution System (LMDS), whose services are based on high-bandwidth radio segments in the spectrum at the 20 GHz frequency range. Emerging wireless access methods include Direct Broadcast Satellite (DBS), which employs Ka band satellite technology to distribute entertainment programming. DBS systems also offer asymmetric, two-way data transmission supporting high-speed data transmission to the user (from the satellite system) and low-speed data reception from the user.

Wireless wide area transport systems are planned to provide low-cost, high-bandwidth data and voice service to remote areas. These systems operate from either low earth orbit (Teledesic and Skybridge) or geostationary orbit (Spaceway). Most of these systems use the 20-30 GHz band, where wide bandwidths and small antenna apertures are possible.

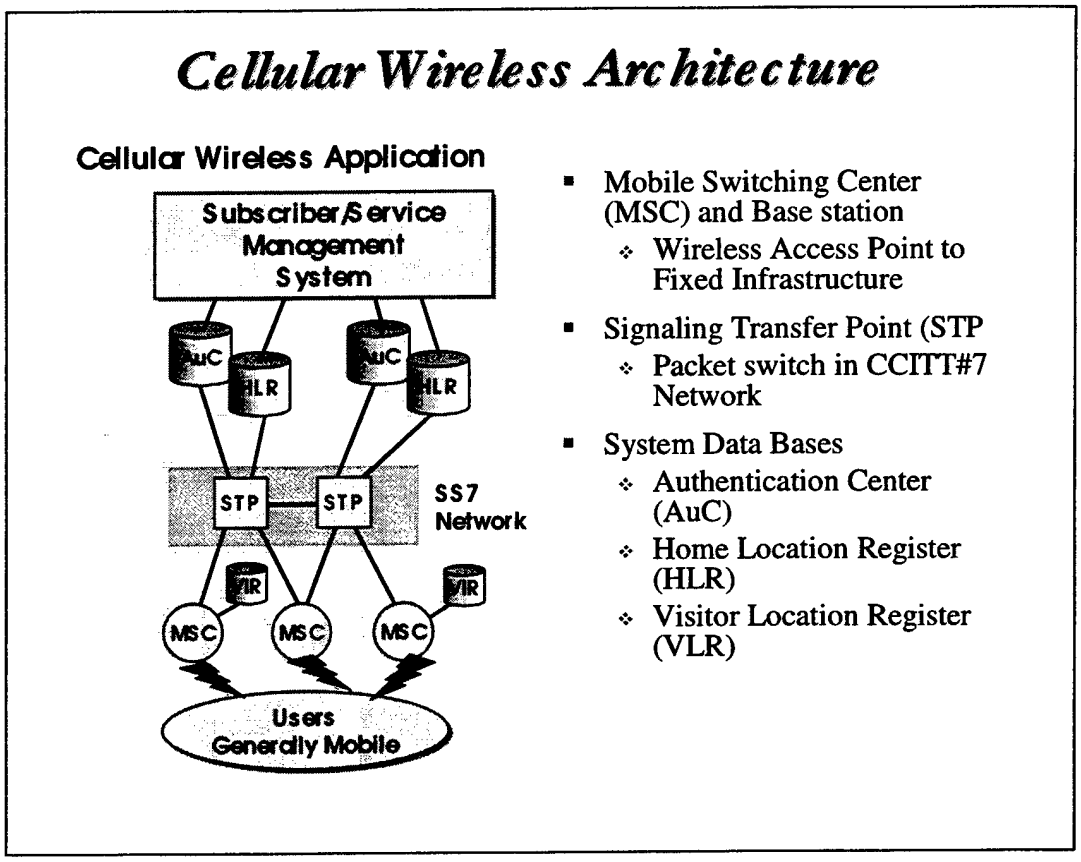


Figure 51. Cellular Wireless Architecture

The widest deployment of commercial wireless is in the mobile cellular system for which the system model is shown in Figure 51. Commercial mobile wireless services are furnished largely within the context of the Intelligent Network Architecture. The figure shows the standard wireless model. In the case of the cellular wireless application, the Mobile Switching Center serves the role of the Service Switching Point. The Mobile Switching Center and its associated Base Stations receive call requests from the mobile subscriber population. Call handling information is then requested from several key system databases, via the CC7 network. Messages are space-based on the (ANSI)-41 standard protocol suite.

These databases are: 1) the Home Location Register (HLR) which contains all of the information about the user and his current location within the system; 2) the Visitor Location Register (VLR) which contains information about all subscribers within an area served by a Mobile Switching Center (MSC); and 3) an Authentication center which validates the billing validity of the subscriber and accumulates the billing information. There may also be an Equipment Identity Center that holds information on particular devices in use within the system.

In the future, other processing resources are anticipated for new wireless-based services. One is a group of voice-controlled services, i.e., voice-controlled dialing, that allows the wireless user to control features and services through spoken commands. Another is a suite of services offering incoming-call options, where the subscriber can customize call-forwarding or call-blocking instructions for different types of incoming calls or receive calling name identification.

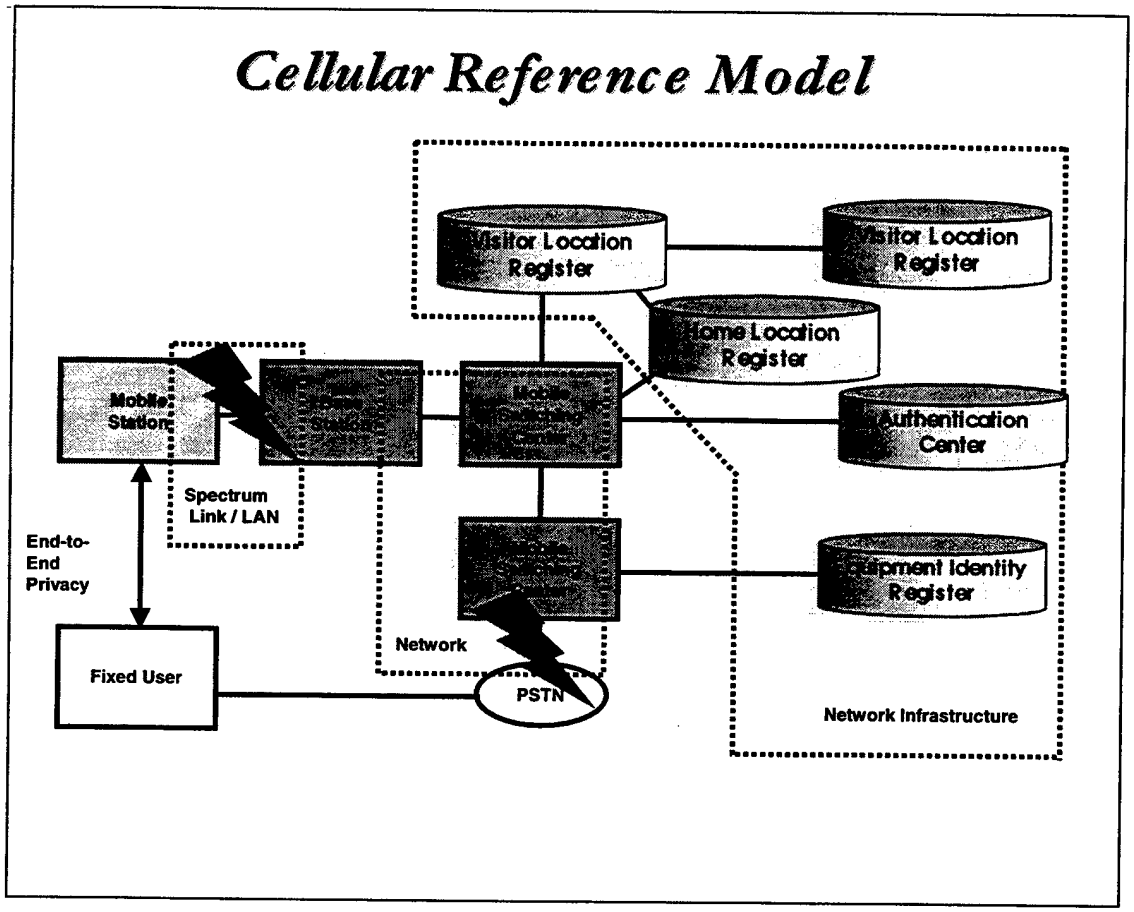


Figure 52. Cellular Reference Model

The next level of detail in the cellular communications systems model is presented in the cellular reference model shown in Figure 52. This figure illustrates the Base Station and Mobile Station that provide the subscriber access to the system. Base stations are sometimes split into one or more Base Transmission Systems (BTS) at a cell site and a Base Switching Center (BSC). Multiple BTS's can be served by a single BSC and a single Mobile Switching Center (MSC) can serve multiple BSCs.

There are several potential attack points in this system. The first is an attack on the cell spectrum or a wireless point-to-point link between a BTS and a BSC or a BSC and an MSC. The information that is accessible at this point primarily pertains to subscribers currently within the serving area of an MSC and thus has a more localized effect. Wider ranging network attacks can be mounted against wireless point-to-point links that move signaling and traffic information between system nodes, either SS7 messages to system databases or internal information such as

cell handoffs. Finally, classical cyber attacks can be mounted against any of the infrastructure databases, which are available through the SS7 network or increasingly through the Internet. While some protection mechanisms are in place, they likely will yield to a determined attack.

The key point to note is that while commercial wireless services may give the appearance of infrastructure independence, they are in truth a vulnerable extension of a vulnerable infrastructure.

Utilization of Countermeasures

Threatened Area	Available Countermeasure	Military	Commercial
Spectrum Access	Waveform TRANSEC Spatial filtering	AJ LPI LPD Strong TRANSEC	Multiple Access Objective uses Weak TRANSEC Some Spatial filtering
Link	COMSEC	COMSEC – Type 1	GSM Weak
Network	IPSEC Intrusion Detection	Link Protection Only	Minimal
Infrastructure	Encryption Access Contol Intrusion Detection	Access Control	Access Control
End-to-End Privacy	ETE COMSEC	Selectively	CONDOR

Figure 53. Utilization of Countermeasures

A number of countermeasures are classically available to attacks mounted at different points in the composite system, as indicated in Figure 53. Attacks in the radio frequency spectrum are the most familiar threat to the military user, and there are a variety of techniques for countering them such as random waveforms driven by high quality Transmission Security (TRANSEC) and spatial filtering of jammers by adaptive antennas. Although commercial wireless systems employ similar waveforms (GSM uses frequency hopping and IS-95 uses spread spectrum), they are designed to combat interference from other users and provide no margin against jamming. Additionally, these systems are designed for easy access.

Tactical military systems also typically protect each link with strong encryption, but only some commercial wireless systems employ any encryption, and that encryption is weak. Above the link level neither system has much protection. The tactical internet operates its routers at system high security level, while commercial systems employ rudimentary protection if any.

End-to-end Type 1 confidentiality is being provided through the NSA CONDOR program that is making commercial wireless available with embedded strong encryption.

4.6 GIG IA SUMMARY

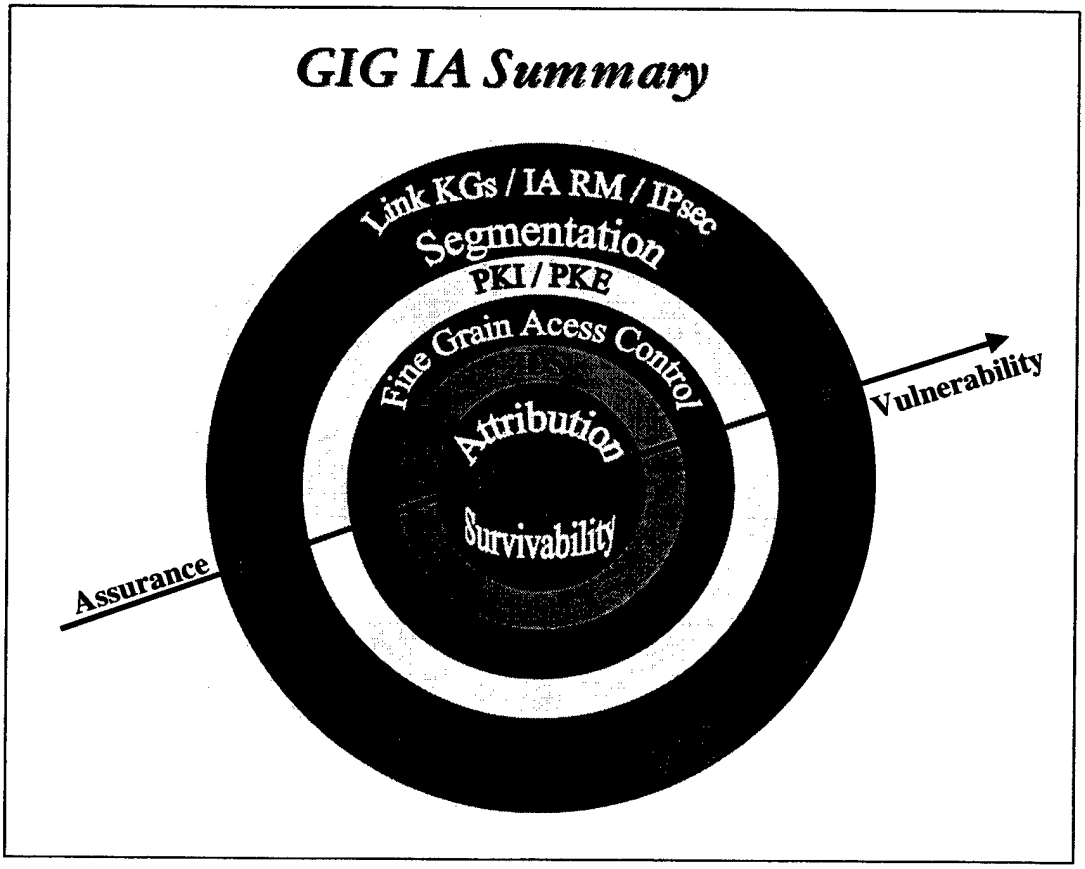


Figure 54. GIG IA Summary

Figure 54 provides a summary of the panel's suggestions for GIG IA. As we noted, the Global Information Grid is the underlying infrastructure to support information superiority for JV2020. The implementation of the GIG is one of the significant events that occurs once every decade or two. The architecture that is designed today will impact the DoD in the next decade or more. To meet this challenge, the panel has identified a layered architectural approach for providing information assurance to the GIG by pursing a disciplined architectural approach:

- Link encryption at the physical layer
- ISO-like reference model with commercial protocols, i.e., IPsec for end to end protection

- Segmentation of DoD from Internet, and segment by classification and enclaves
- Adopt PKI/PKE
- Use fine-grained access control of computers and communication resources

In addition to the architectural layers, the approach also includes use of correlated multi-layered IDS data (i.e., at common user, command and host levels) as inputs to intelligence-enabled tracing systems and modus operandi detectors. Attribution is facilitated by highly filtered data for signal-to-noise enhancement and IPsec for path tracing and target localization. The approach of the layered defense, combined with measurement, rapid response, and attribution, results in significantly reduced vulnerability and dramatically improved GIG information assurance.

Page 947 of 3957

CHAPTER 5. RECOMMENDATIONS

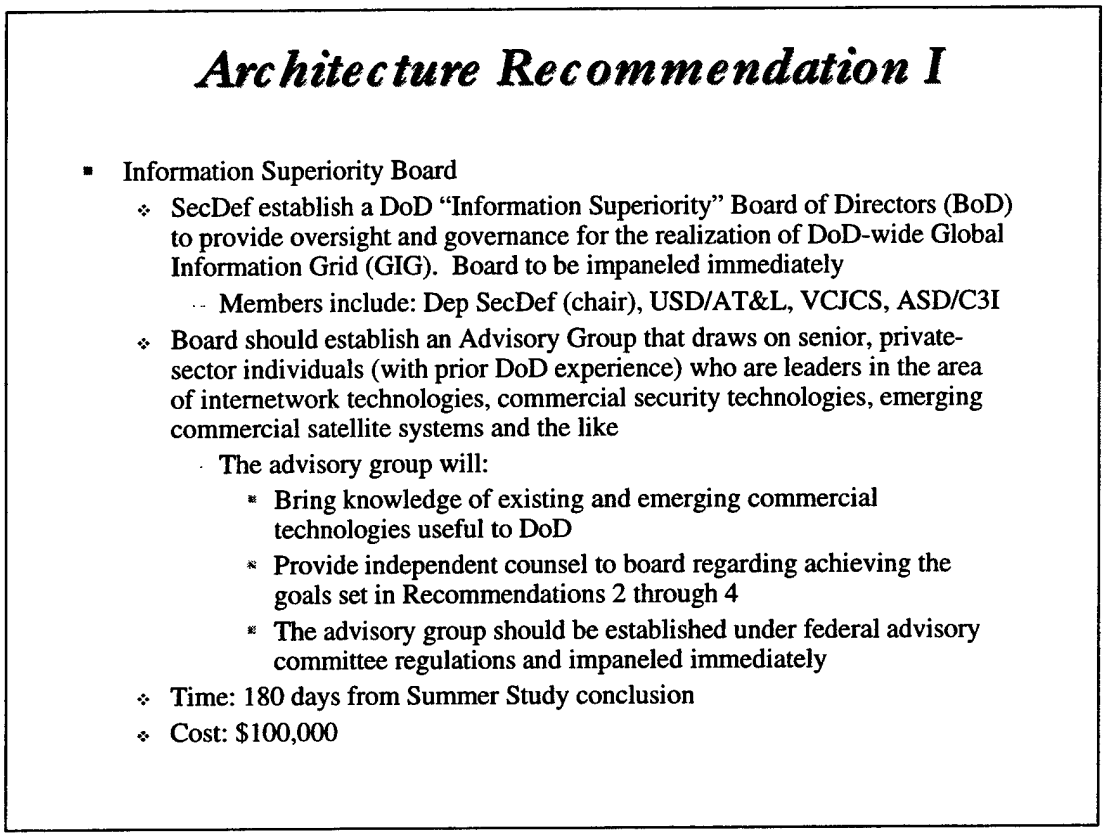


Figure 55. Recommendation I—Information Superiority Board

Consistent with its findings that under current organization (see discussion specifically associated with Figure 25), methods, and procedures the DoD is unlikely to realize a measured, consistent, and effective approach to creation of a Global Information Grid (GIG), the panel recommends the formation of a *DoD Board of Directors for Information Superiority.*

The Secretary of Defense should impanel the Information Superiority Board immediately, with membership consisting of the Deputy Secretary of Defense (as chair), the Undersecretary of Defense (Acquisition Technology and Logistics), the Vice-Chair of the Joint Chiefs of Staff, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director of Central Intelligence.[8]

It is further recommended that the Information Superiority Board create an advisory group under Federal Advisory Committee regulations (or as a permanent DSB Panel) consisting of senior private sector IT leaders. The Advisory Group's purpose would be to provide the board with up-to-date knowledge of current and emerging commercial information systems, services,

[8] Reference: Defense Science Board Report on *Tactical Battlefield Communications*, February 2000

Page 948 of 3957

and network technology of potential use to the DoD in the realization of its Global Information Grid. It would also offer experience-based advice from industry as to the best technical and management methods for creating such an infrastructure.

The advisory group should consist of recognized industry experts in inter-networking technologies, commercial information and network security technologies, emerging information transfer technologies and systems, and other commercial activities such as standards development, infrastructure development, and the like. The advisory group charter should also ensure that the group provides independent assessments and counsel to the Information Superiority Board concerning the achievement of the goals and objectives set forth in panel recommendations that follow.

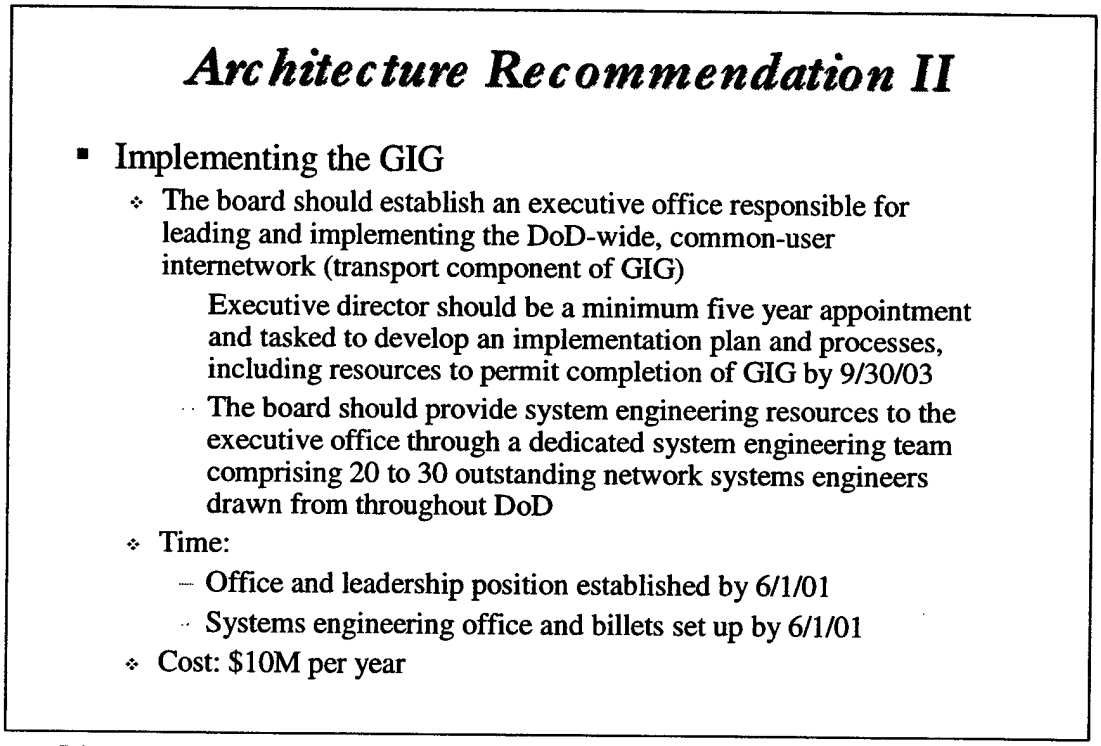


Figure 56. Recommendation II—Executive Director and GIG Implementation Process[9]

Placing the proper emphasis on GIG implementation and ensuring adherence to the policies established in accordance with the previous recommendations requires continuous oversight. It is therefore recommended that the Board of Directors for Information Superiority create, by 1 June 2001, an executive office responsible for leading the implementation of the DoD-wide common user internetwork on behalf of the board. The executive office director should be a senior DoD leader appointed for a minimum of five years. The executive director should be provided programmatic oversight for all DoD C4ISR systems acquisitions (including those procured by the services) and through this oversight ensure that all such systems are

[9] Reference: Defense Science Board Report on *Tactical Battlefield Communications*, February 2000

interoperable within and as part of the GIG. It would be the executive director's primary responsibility to deliver the GIG.

Several additional, more specific actions needed to accomplish the GIG objectives follow:

1. The executive director should be tasked to develop a GIG implementation plan, to include technical milestones, measurable interim goals, and an estimate of the resources necessary to complete transition and realization of the GIG by 30 September 2003.
2. The board of directors should provide manpower billets for a system engineering team to support the Executive Director. A cadre of 20 to 30 outstanding system engineers with backgrounds in Internet telecommunications and security technologies should be selected from throughout DoD. These individuals must be deep technically and visionary in their system engineering skills. This system engineering team would provide independent technical inputs to the executive director regarding the many responsibilities this individual will be given, as noted in the next paragraph.
3. The executive director should immediately establish a process to transform DoD information infrastructure systems from their present stovepipe configurations into a global DoD-wide common-user virtual intranet, the GIG. This transformation must embody the current and evolving commercial IT standards, protocols, and technology, with the goal of reducing inefficiency in spectrum usage and the costs of information transport, storage, retrieval, and management. Most important, this transition should enable new operational flexibility that can be leveraged by warfighters.

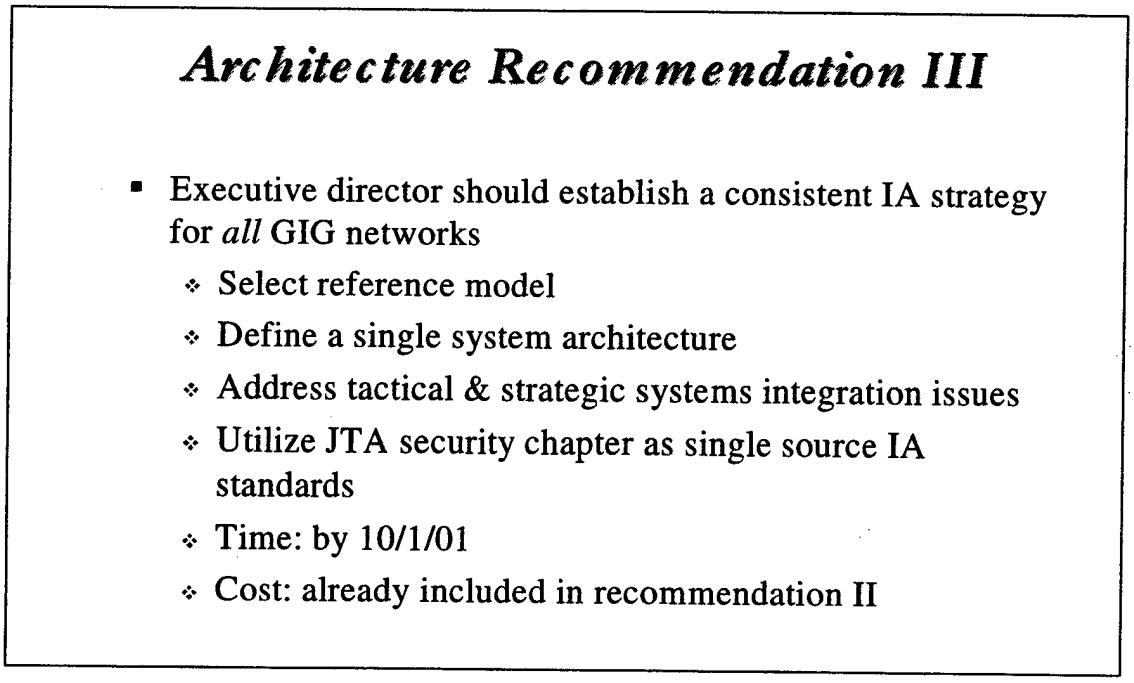


Figure 57. Recommendation III—Architecture

The GIG executive director should immediately set policy and guidance for GIG IAA. Specifically, ambiguities regarding an IA reference model, system architecture, and technical architecture (as noted in the body of the IAA report) should be clarified. The executive director should establish this unified strategy and framework no later than October 2001.

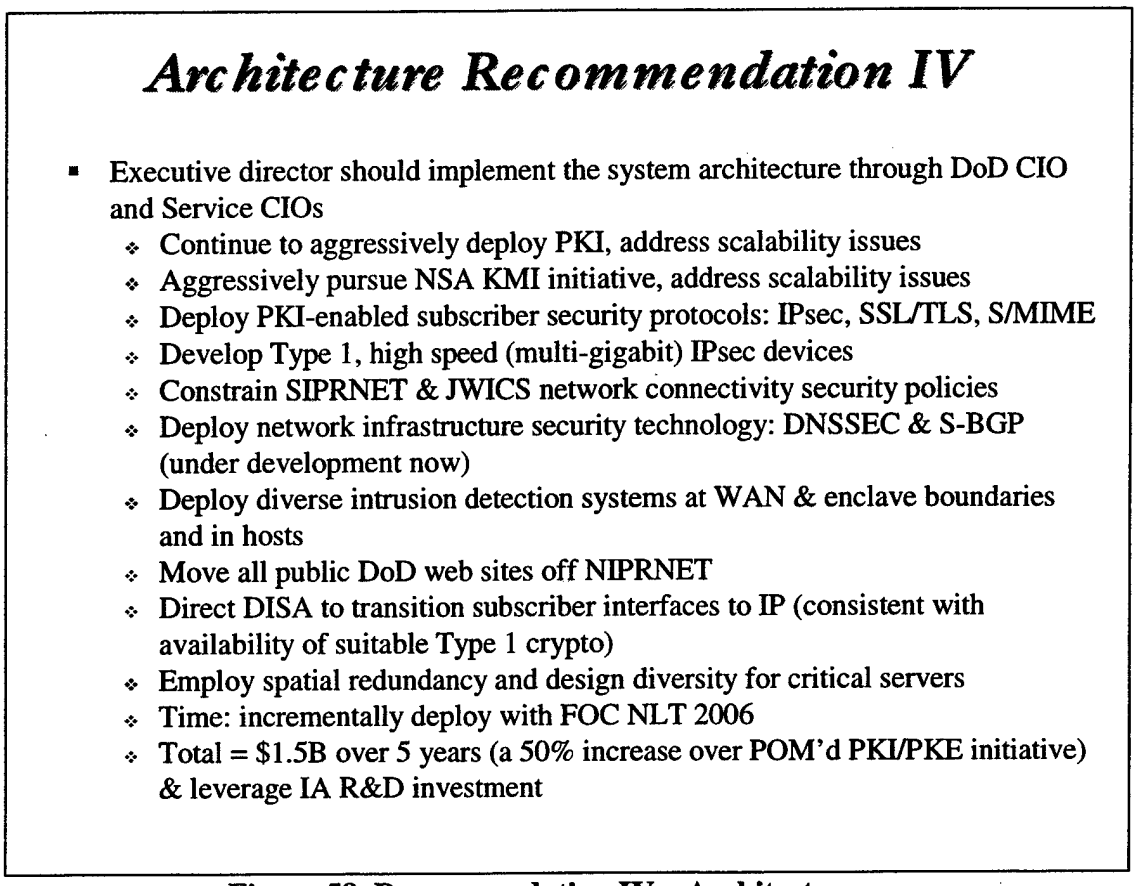


Figure 58. Recommendation IV—Architecture

Finally, the GIG executive director should work through the CIO Executive Panel and the MCEB to implement the GIG system architecture. Specific system architecture and implementation issues that need immediate attention are noted in Figure 58. These include:

- Continuing to aggressively deploy PKI, and addressing scalability issues
- Aggressively pursuing NSA KMI initiative, addressing scalability issues
- Deploying PKI-enabled subscriber security protocols: IPsec, SSL/TLS, S/MIME
- Developing Type 1, high speed (multi-gigabit) IPsec devices
- Constraining SIPRNET and JWICS network connectivity security policies
- Deploying network infrastructure security technology: DNSSEC and S-BGP (under development now)
- Deploying diverse intrusion detection systems at WAN and enclave boundaries and in hosts
- Moving all public DoD web sites of NIPRNET
- Directing DISA to transition subscriber interfaces to IP (consistent with availability of suitable Type 1 crypto)
- Employing spatial redundancy and design diversity for critical servers

To support GIG implementation and to accelerate the DoD PKI/PKE strategy, the panel recommends an increase in budget of 50% over what is presently planned. This increase should not only accelerate the strategy, but also fund the development of Type 1 high-speed IPsec devices. This funding increase should be complemented and supported by the IA S&T investments called for in the companion report of the IA Technology Panel of the Defensive Information Operations summer study.

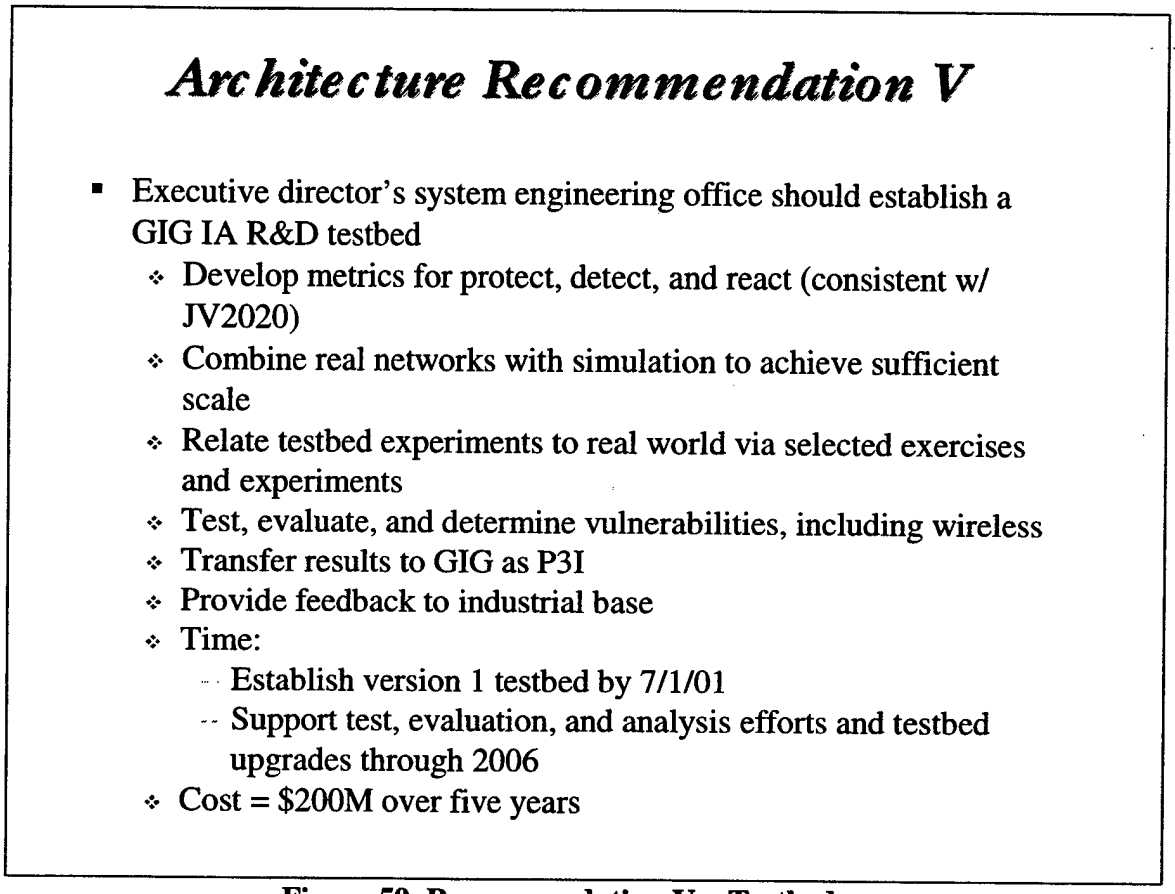


Figure 59. Recommendation V—Testbed

The panel recommends that the executive director's system engineering office establish a GIG IA research and development testbed. The testbed nodes should be located at ESC, CECOM, SPAWAR, AFRL, NSA, etc. The participants in the evaluation process will include research and development, evaluation, and operational communities (services and agencies). The testbed will provide a means for measurement of system performance in the face of red team attacks on blue team scenarios and related information traffic. The testbed will also serve as a primary means for DARPA Information Assurance technology insertion and evaluation. The metrics and measurements will evolve as results are analyzed and lessons learned are derived from the data. Lessons learned will be fed back to red and blue teams to refine and update strategies and will be used by developers to improve system defenses. Lessons learned will also be made available to the GIG architects and system engineers to improve IA for the deployed system.

Finally, the testbed should be used to engineer, evaluate, and update defense-in-depth (DID) strategies and technologies. The testbed will provide the means to understand residual DiD (and GIG) vulnerabilities and thus facilitate cost/benefit analysis for GIG IA investments. As noted in the panel's findings, no rigorous means for evaluating DiD systems, architectures, or technologies exist today.

The testbed should be implemented no later than July 2001, and augmented to support GIG IA technology, architecture, and metric evaluation over a five-year period.

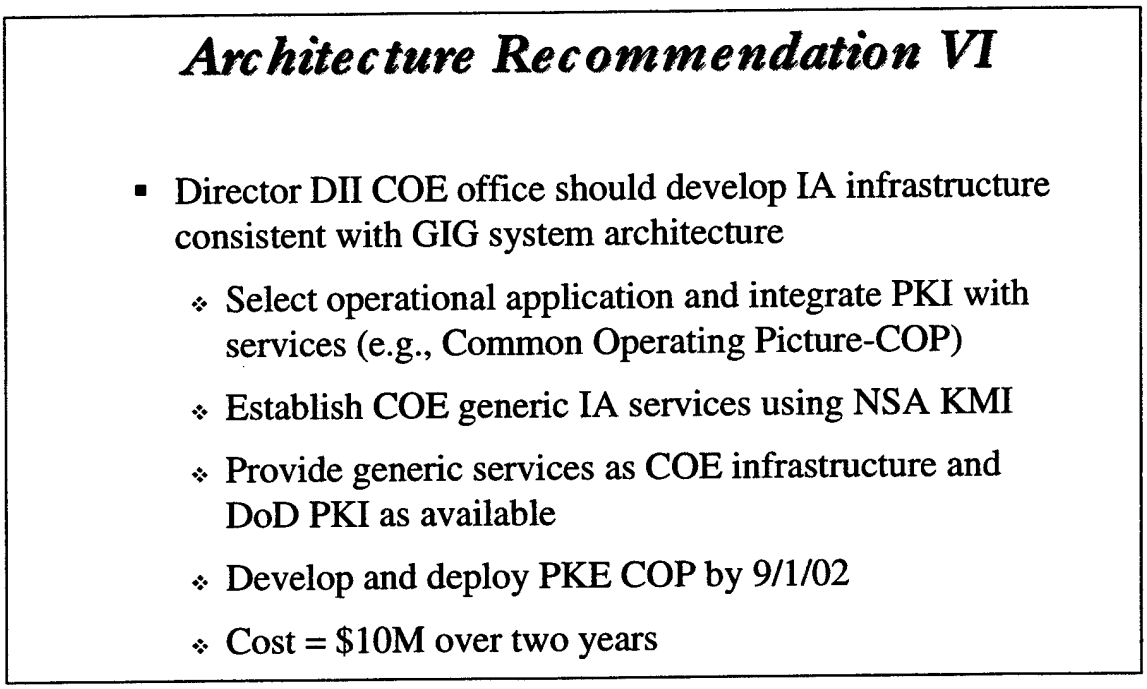


Figure 60. Recommendation VI—IA Infrastructure

The panel recommends that the DoD begin the process of incorporating IA, and specifically PKI/PKE into the DII COE. In discussing alternatives with representatives from DISA, it was noted that the Common Operating Picture (COP) application is critical to CINC and services Joint-Task-Force-mission success. For a modest investment focused on PKE of this application, an acceleration of PKI into the COE, as generic, run-time utilities, can be accomplished. In addition to gaining important experience with PKE in battlefield applications, PKI could be integrated into the COE setting software standards and infrastructure for use in other service and CINC C4ISR systems.

Although IA infrastructure is planned to be incorporated into the COE "sometime in the future," the panel feels that accelerating this process is critical to ensure consistent PKE with tactical C4ISR systems. Experience gained sooner rather than later is key to effectively deploying an IA-enabled COE for the GIG.

Page 955 of 3957

APPENDIX A. TERMS OF REFERENCE

Page 956 of 3957

Page 957 of 3957

ACQUISITION AND TECHNOLOGY

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

JAN 0 4 2000

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board Task Force on Information Warfare - Defense

You are requested to form a Defense Science Board (DSB) Task Force to review and evaluate DoD's ability to provide information assurance to carry out Joint Vision 2010 in the face of information warfare attack.

Tasks to be accomplished:

Using the "1996 DSB report on Information Warfare – Defense" as the departure point, address the following:

- What is the status of action on the recommendations?
- Where there are shortfalls, what are the barriers to action and what should be done?
- What important aspects did the 1996 Task Force miss that should have been addressed?
- Assess the recommendations of other important reports that have addressed information assurance issues.

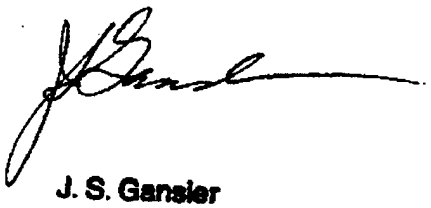
The Information Warfare - Defense Task Force will determine:

- Adequacy of the process toward the information assurance goals needed to carry out Joint Vision 2010.
- Adequacy of the Department's readiness to project and sustain power in the face of information warfare attacks.
- The appropriate role(s) and capability of DoD to provide information assurance in support of Homeland Defense and in support of Critical Infrastructure Protection.
- Recommendations for research and development which are uniquely in DoD's interest, and thus not likely to be accomplished by the private sector in the time required to meet DoD's Information Warfare - Defense objectives.
- Areas in which DoD should seek strong partnering relationships outside DoD, such as with the Critical Infrastructure Assurance Office (CIAO).
- The Task Force should provide an interim report by June 30, 2000.

Page 958 of 3957

The study will be co-sponsored by the Under Secretary of Defense (Acquisition, Technology and Logistics) and Assistant Secretary of Defense for C3I. Mr. Larry Wright will serve as the Task Force Chairman; Colonel Gregory Frick will serve as the Executive Secretary;and Major Tony Yang, USAF, will serve as the Defense Science Board Secretariat Representative.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5104.5, "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, United States Code, nor will it cause any member to be placed in the position of acting as a procurement official.



J. S. Gansler

APPENDIX B. BIOS

Page 960 of 3957

Page 961 of 3957

DR. MICHAEL S. FRANKEL (Chair) is vice president and director of SRI International's Information, Telecommunications, and Automation Division. Dr. Frankel's expertise is in survivable command, control, and communication system design and implementation, radio frequency systems design and analysis, remote sensing, and data acquisition, reduction and analysis. Dr. Frankel is a Fellow of the IEEE and a member of the Cosmos Club, AFCEA, ADPA, Sigma XI and Tau Beta Pi. He received his B.S., M.S., and Ph.D. degrees in electrical engineering from Stanford University, California in 1968, 1970 and 1973, respectively. He was a member of the Army Science Board from 1992 through 1998, and served as its chair from 1996-98. When he left the Army Science Board, the U.S. Army awarded Dr. Michael Frankel the Distinguished Civilian Service Award. This award is the highest commendation that can be given to a civilian providing volunteer services to the Army and can only be bestowed by the Secretary of the Army. Dr. Frankel is presently a member of the Defense Science Board. He is the author or co-author of seventy SRI technical reports, over twenty publications in technical journals, and two textbook manuscripts. Dr. Frankel holds patent disclosures on passive satellite systems, a passive frequency-steerable microwave repeater system, an emitter location system, as well as one on the TeleEducation concept and a passive, high gain, frequency-steerable satellite repeater.

DR. STEPHEN THOMAS KENT is Chief Scientist- Information Security, BBN Technologies, Director- Security Practice Center, GTE Internetworking, and Chief Technical Officer, CyberTrust Solutions. Dr. Kent holds the following degrees: Ph.D, Computer Science, Massachusetts Institute of Technology, September, 1980; E.E., Electrical Engineering and Computer Science, Massachusetts Institute of Technology, February, 1978; S.M., Electrical Engineering and Computer Science, Massachusetts Institute of Technology, May, 1976; B.S., Mathematics, summa cum laude, Loyola University of New Orleans, 1973.

In his role as Chief Scientist, Dr. Kent oversees information security activities within BBN Technology, and works with government and commercial clients, consulting on system security architecture issues. In this capacity he has acted as system architect in the design and development of several network security systems for the Department of Defense and served as principal investigator on a number of network security R&D projects for almost 20 years. In his capacity as Director of the SPC, Dr. Kent monitors all security-related aspects of the service offerings of GTE Internetworking Services. He reports to the President of GTE Internetworking and coordinates with engineering, operations, and marketing to ensure the security quality of offerings. As CTO for CyberTrust Solutions, Dr. Kent provides strategic direction for this certification authority business, reporting to the President of CyberTrust.

During the last two decades, Dr. Kent's R&D activities have included the design and development of user authentication and access control systems, network layer encryption and access control systems, secure transport layer protocols secure e-mail technology, multi-level secure (X.500) directory systems, public-key certification authority systems, and key recovery systems. His most recent work focuses on public-key certification infrastructures for government and commercial applications, security for Internet routing, and high assurance cryptographic modules.

Page 962 of 3957

Dr. Kent served as a member of the Internet Architecture Board (1983-1994), and chaired the Privacy and Security Research Group of the Internet Research Task Force (1985-1998), both now under the auspices of the Internet Society. He chaired the Privacy Enhanced Mail (PEM) working group of the Internet Engineering Task Force (IETF) from 1990-1995 and co-chairs the Public Key Infrastructure Working Group (1995-). He was a charter member of the Board of the International Association of Cryptologic Research (1982-89) and served on the editorial board for the Journal of Telecommunication Networks (1982-1984). He currently serves on the editorial board of the of Journal Computer Security (1995 and on the board of the Security Research Alliance, a consortium of leading information security companies.

Dr. Kent served on the Information Systems Trustworthiness Committee (1996-98) of the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC). He was major contributor to the committee report, "Trust in Cyberspace." Previous CSTB/NRC service includes the committee on Rights and Responsibilities of Participants in Networked Communities (1993-94), the Technical Assessment Panel for the NIST Computer Systems Laboratory (1990-1992), and the Secure Systems Study Committee, which produced the "Computers at Risk: Safe Computing in the Information Age" report (1988-1990). Dr. Kent has often been called upon as a reviewer of CSTB committee reports.

The Secretary of Commerce appointed Dr. Kent as chair of the Federal Advisory Committee to Develop a FIPS for Federal Key Management Infrastructure (1996-98). The output of that committee forms the underpinning for a FIPS on Key Recovery. He previously served on the Presidential SKIPJACK Review Panel (1993-1994).

Dr. Kent has been an active participant in a number of professional conferences, as a speaker, session chair, program committee member, etc. He chaired the steering committee for the Symposium on Network and Distributed System Security (1990-1998) and was General Chair of the IEEE Symposium on Security and Privacy (1996-97). He has appeared as an invited speaker at security conferences throughout the United States, Europe and Asia.

Since 1977, Dr. Kent has lectured in the United States, Europe, Australia, and Asia on the topic of security in computer communication networks on behalf of various organizations, including the National Cryptologic School, George Washington University, M.I.T., University of Southern California, UCLA, various government agencies, and several private firms.

DR. PATRICK LINCOLN is the Director of the Computer Science Laboratory of SRI International, a leading center for research on the fundamental issues of computer security, networks, and automated formal methods. Under his direction, the lab is expanding its presence in these areas and is extending its research agenda into new areas. Dr. Lincoln joined SRI in 1992 after completing Ph.D. work at Stanford University in Computer Science. He holds a B.Sc. from MIT and has previously held positions at MCC and Los Alamos National Laboratory. Dr. Lincoln is an active researcher in the fields of networks, security, language design, and mobile code. He has published widely and made significant contributions to the formal analysis of systems, languages, and protocols in computer security, safety, and fault tolerance, and to their integration into survivable systems. He serves on the Digital Island (Nasdaq:ISLD) Strategic Advisory Board. http://www.csl.sri.com/~lincoln

Page 963 of 3957

ALAN J. MCLAUGHLIN received BS and MS degrees in Electrical Engineering from Northeastern University in 1957 and 1959, respectively. During 1959-60 he served as a Lieutenant in the U.S. Army Signal Corps Laboratories at Fort Monmouth, NJ. He was awarded the Army Commendation Medal for meritorious service. From 1961-71 he was a Lecturer at the Northeastern University Graduate School of Engineering.

From 1960 to 1962 he was a project engineer with Contronics, Inc., engaged in the design and development of automatic test equipment. He joined the engineering staff of Deco Electronics, Inc. in 1962, where he designed digital communications equipment. In 1965 he became a systems engineer with General Instrument Co., where he was involved with the design of sonar systems and associated signal processing equipment.

In 1967 Mr. McLaughlin joined the staff of MIT Lincoln Laboratory. Initially he was engaged in the design of special-purpose processors for anti-jam communications systems and later with the design of high-speed signal processors. He established a laboratory for the investigation of GaAs laser diode parameters and participated in the design of an optical communications system. In 1972 he joined the Education Technology Group where he was responsible for the design of Computer-Aided Training systems. In 1974 he was appointed Leader of the Education and Computer Technology Group.

In 1975 he was appointed Associate Head of the Computer Technology Division and a member of the Lincoln Laboratory Steering Committee. In 1978 he was appointed Head of the Computer Technology Division with management responsibility for laboratory programs in speech, radar and image signal processing, computer networks, digital processor technology, digital integrated circuits and machine intelligence technology. In 1992 he was appointed Assistant Director of Lincoln Laboratory. He is currently responsible for Advanced Electronic Technology, Air Traffic Control and Surface Surveillance programs at the Laboratory.

In 1978-79 Mr. McLaughlin served on an Air Force steering committee for advanced computer technology planning. In 1980-81 he served on a National Academy of Science study committee on modernization of Air Force computerized administrative support systems. In 1984-85 he was a member of a senior advisory committee to the Director of ARPA in the area of information processing. Since 1986 he has been a member of the ARPA Information Science and Technology Study Group. In 1988-89 he served as co-chairman and in 1990-91 chairman, of the ARPA Study Group. In 1991-92 he served on a National Academy of Science study committee on Modernization of the Worldwide Military Command and Control Information System. In 1993 he served on the Air Force Scientific Advisory Board Study on Information Architectures. In 1994-95 he served on a National Research Council Committee on Future Technologies for Army Multimedia Communications. He has served on a variety of Defense Science Board task forces: 1994-95 Acquiring Software Commercially, 1996 Defensive Information Warfare, 1996-97 Aviation Safety, 1997-98 Military Excess and Surplus Material, 1999 Investment Strategy for DARPA. Mr. McLaughlin is a member of Eta Kappa Nu and a Senior Member of the IEEE.

Page 964 of 3957

PETER STEENSMA is Chief Scientist and Senior Technical Director, ITT Aerospace Communications Division. He received his B.S. degree at Calvin College in Physics, Mathematics, and German Literature; his M.S. was received from the Polytechnic University of Brooklyn; and he was a Research Associate at Princeton University.

Mr. Steensma has 30 years of communications systems design and development experience, including mobile tactical networks, tactical switching, radio and optical fiber transmission, secure command and control networks, and satellite and terrestrial radio navigation.

Recent highlights include:

- Initiated and provided technical leadership to several programs aimed at establishing the next generation of mobile tactical communications systems, including Hand-held Multimedia Terminal and Small Unit Operations DARPA programs
- Formed international consortium of 12 nations and established a multinational joint venture company, TACONE, to set next generation NATO post 2000 communications standards
- Led conceptualization and development ITT communications products in the Tactical Internet, including SINCGARS radios (SIP and ASIP), Near Term digital Radio (NTDR), and the Internet Controller. These supported the US Army TF XXI exercises and subsequent digitization efforts
- Technically led a winning US/UK team for UK Project Bowman, a total Forward Area Battlefield Communications System for the United Kingdom Ministry of Defense. Led the development and demonstration of a Product Demonstrator, the first mobile tactical internet system. Continuing responsibility and support for developing production solution

Past positions include, Director of Systems Engineering, Director of Internal Research and Development, Manager of C2 Systems Engineering, Senior Scientist Transmission Systems.

JOHN WOODWARD is the Technical Director of the Intelligence and Special Programs Division, which executes MITRE's $35M Air Force intelligence program. Mr. Woodward also serves as corporate Director of Information Warfare, where he is responsible for ensuring that MITRE's varied information warfare activities are coordinated, responsive to broad government objectives, and of high quality.

Mr. Woodward has more than 25 years of experience in software engineering with MITRE, and has specialized in information system security for the past 22 years. Prior to his present position, he was the Associate Technical Director of the Information Systems Security Division, where he shared management responsibility for MITRE's technical center providing information security and defensive information warfare expertise throughout MITRE, and to MITRE's Department of Defense, intelligence, and Federal Aviation Administration customers.

In earlier positions at MITRE, he managed the prototype development of the Joint Worldwide Intelligence Communications System, and was responsible for MITRE's intelligence information system support to the Defense Intelligence Agency, North American Air Defense/U.S. Space

Page 965 of 3957

Command/Air Force Space Command, and the Strategic Air Command. He also led MITRE's Artificial Intelligence Technical Center. He was responsible for inventing, prototyping, and specifying compartmented mode workstations, which are now available commercially from multiple vendors. He also created and was the original chairman of MITRE's Information Policy Committee.

Mr. Woodward received masters and bachelor's degrees in applied mathematics/computer science in 1974 from Brown University.

Page 966 of 3957

Page 967 of 3957

APPENDIX C. AGENDAS

Page 968 of 3957

Page 969 of 3957

DSB Agenda 22-23 Feb 2000

To be held at the offices of
Strategic Analysis, Inc.
3601 Wilson Blvd., Suite 600
Arlington, VA 22201

Tuesday, February 22, 2000

0845 – 0900	Administrative Remarks	Mr. Wright and Col Frick
0900 - 1000	Eligible Receiver/Solar Sunrise	Lt Col Perry Luzwick, OSD
1000 - 1100	* **Classified** (Network Intrusion)	CDR Bob Gourley, JTF-CND
1100 – 1200	DoD Insider Threat IPT results	Mr. Tom Bozek, OSD
1200 – 1300	Lunch/Free Discussion	
1300 –1400	Global Information Grid Architecture	Mr. John Osterholz/Mr. Terry Hagle, OSD
1400 - 1500	DoD Web Security Initiatives	Ms. Linda Brown, OSD
1500 – 1630	* **Classified** DIA Threat/I&W	John Yurechko
1630	Summary/Wrap-up/Time for Panels as needed	

Wednesday February 23

0845 – 0900	Administrative Remarks: Mr. Wright/Col Frick	
0900 – 1100	* **Classified** NSA Overview to include threat/red teaming/strategy	Mr. Larry Castro/CAPT Ed Kinerva
1100 – 1200	Navy IA overview/capabilities	CAPT James Newman
1200 – 1300	Lunch/Discussions	
1300 – 1400	AF IA overview/capabilities	Lt Col Dave Warner/Lt Col Susan Pardo
1400 – 1500	Army IA overview/capabilities	Mr. Phil Loranger/LTC Krist
1500 – 1600	DISA IA overview/vision (pending) or time for panel breakouts	

Note: morning and afternoon breaks will be taken as needed. Original plans for this plenary session included a brief from DTRA (ruling was that it can be given at the future but only at SCI level) and Kosovo Lessons Learned (still trying for this, but releasability issue with Joint Staff at this time).

Page 970 of 3957

DSB Agenda 27-28 March 2000

To be held at the offices of
Strategic Analysis, Inc.
3601 Wilson Blvd., Suite 600
Arlington, VA 22201

Monday, March 27, 2000

0845 – 0900	Administrative Remarks	Mr. Wright and Col Frick
0900 - 1000	Army IA Initiatives	LTC Lundgren
1000 - 1200	Panel Chairs Outbrief Progress/Issues to Date	
1200 – 1300	Lunch/Free Discussion	
1300 –1430	Joint Staff Perspectives	BG Quagliotti, Joint Staff/J6
1430 – 1530	CIAO/National Plan	Mr. John Tritak
1530 - 1630	Industry IA Perspectives	Mr. Chris Christiansen, IDC
1630	Wrap up	

Tuesday, March 28, 2000

0800 – 0830	Opening Remarks	Dr. Mike Frankel *Panel Chairman*
0830 – 0930	Defense in Depth II	Col Pat Phillips *J6K*
0930 – 1030	Information Assurance Technical Framework (IATF)	Dave Luddy *NSA*
1030 – 1100	Break	
1100 – 1200	Network Management System (NMS)/ Base Information Protect Air Force	COL Roger Robichaux *Air Force*
1200 – 1:00	Lunch/Discussions	
1:00 – 2:00	GIG IA Architecture Overlay	Terry Mayfield *IDA*
2:00 – 3:00	I3A	Mr. Doug Troester *MITRE* LTC Roy Lundgren
3:00 – 3:15	Break	
3:15 – 4:45	Discussion	
4:45 – 5:00	Wrap-up	

AGENDA

DSB Task Force on Defensive Information Operations

April 19-20, 2000

Booz-Allen & Hamilton

Hamilton Building Room 2014

April 19, 2000		
0730	Registration	
0800	OSD Human Resources IPT Studies	CAPT Katherine Burton
0900	Joint Vision 2010/2020	Col Andrew Twomey
1000	DoD PKI Program	Mr. Mike Green
1100	DISA Future Concepts	Mr. Richard Hale
1200	Lunch/Overflow of morning briefs	
1300	Logistics IA study: Theater Distribution	Ms. Virginia Wiggins
1400	TRANSCOM IA Initiatives/GTN	Jacques Sabrie
1500	InfoSec Research Council (IRC)	Dr. John McLean Dr. Carl Landwehr
1600	DARPA Initiatives	Dr. William Mularie
April 20, 2000	Sub-Panels meet	

Page 972 of 3957

DSB IAA PANEL
Agenda 20 April 2000

Thursday, April 20, 2000

0800 – 0830	Opening Remarks	Dr. Mike Frankel *Panel Chairman*
0830 – 0930	Navy/Marine Corps Intranet	Mr. Scott Henderson *SPAWAR*
0930 – 1030	DII Security Architecture	Mr. Richard Hale *DISA*
1030 – 1100	Break	
1100 – 1130	ISO Security Reference Model	Dr. Stephen Kent *BBN Technologies*
11:30-12:00	Lincoln Lab Security Metrics	Mr. Alan McLaughlin *MIT/LL*
12:00 – 12:30	Lunch/Discussions	
12:30 – 1:15	Gold Security Architecture Reference Model	Mr. Terry Mayfield *IDA*
1:15 – 2:00	IA Operation Readiness Metrics	LtCol Lisa Lemza J-6
2:00 – 2:15	Break	
2:15 – 5:00	Discussion and Wrap-up	

Page 973 of 3957

Agenda

Defense Science Board Spring Quarterly Meeting

May 24-25, 2000

Thursday, May 25, 2000 (3E869)

0800	Defensive Information Operations Study	Mr. Larry Wright
0830	Network Security & Architecture	Dr. Michael Frankel
0900	Defensive Information Operations Legalities	Mr. Stewart A. Baker
0930	Defensive Information Operations Organization	MGEN John P. Casciano, USAF (Ret.)
1000	General Henry Shelton, USA, CJCS	
1030	Break	
1045	Defensive Information Operations Policy	Mr. Richard Wilhelm
1115	Defensive Information Operations Technology	Mr. Richard M. Mendelowitz
1200	Lunch in Blue Room (3D854) hosted by Hon. Jacques S. Gansler, Under Secretary of Defense (Acquisition, Technology & Logistics)	
1315	Annual Group Photo (River Entrance)	
1330	Intelligence Needs for Civil Support	Dr. Ruth David Mr. Peter Marino
1430	Hon. Jacques S. Gansler	
1530	Closing Comments	DSB Chairman
1545	Adjourn	

Page 974 of 3957

DRAFT AGENDA

MAY 26, 2000
DSB TASK FORCE ON DIO
STRATEGIC ANALYSIS, INC.
3601 WILSON BLVD. SUITE 600
ARLINGTON, VA 22201

Time	Topic	Briefer
0800	Pervious DARPA IA perspective	Sami Saydjari
0900	DARPA IA (follow-on)	Mike Skroch
1000	USSPACE	Col Larry Klooster
1100	CISCO perspectives	J. Romain
1200	Lunch	
1300	Biometrics	Jeff Dunn, NSA
1400	NSA Senior IA perspectives	John Nagengast
1700	Adjourn	

DRAFT AGENDA
DSB TASK FORCE ON DIOAT
SAIC SCIF
4001 N. Fairfax Drive, Suite 500
Arlington, VA
Tuesday, June 13, 2000

TIME	TOPIC	BRIEFER
0800-0930	Performance Needs/Developing technology	Lee Hammarstrom & Pat Dowd
0930-1030	Chessmaster and recent events	Mike Shore
1030-1200	History of IW	ADM Bill Studeman, USN (Ret)
1200-1:00	Lunch	
1:00-2:00	CIA Strategic Warning/ Threat	Dr. Tom Donahue
2:00 – 3:00	Discussion	
3:00 – 4:30	IA Metrics	Mr. Terry Bartlett/DIAP
4:30 – 5:00	Wrap-up	

DSB IAA PANEL
Agenda
June 14, 2000
To be held at the offices of
Strategic Analysis, Inc.
3601 Wilson Blvd., Suite 600
Wednesday, June 14, 2000

7:30 – 8:00	Coffee – Sign-in	
8:00 – 9:00	TA Security Standards	Mr. James Barnette DISA
9:00 – 9:30	Results of a DARPA sponsored study on "Information Assurance for Mobile Operations" An approach and some preliminary results on: "Intrusion Detection for the Lower Tactical Internet"	Mr. Al Mclaughlin/MIT/LL
9:30 – 9:45	Break	
9:45 – 12:00	Architecture Development and Recommendations	
12:00 – 12:30	Working Lunch	
12:30 – 3:30	Architecture Development and Recommendations	

Page 976 of 3957

DSB IAA PANEL
Agenda
July 12-14, 2000
To be held at the offices of
Strategic Analysis, Inc.
3601 Wilson Blvd., Suite 600

Wednesday, July 12, 2000

TIME	TOPIC	BRIEFER
8:00 – 8:30	Coffee - Sign-in	
8:30 – 10:30	IAA Introduction	Dr. Mike Frankel
10:30 – 10:45	Break	
10:45 – 11:45	IA Wireless Issues	Mr. Pete Steensma
11:45 – 12:30	Lunch	
12:30 – 1:30	Reference Model	Dr. Stephen Kent Dr. Patrick Lincoln Mr. John Woodward
1:30 – 2:30	IA Metrics/Standards	Mr. Al McLaughlin
2:30 – 3:30	Technical Architecture	Dr. Stephen Kent Dr. Patrick Lincoln Mr. John Woodward
3:30 – 4:30	System Architecture	Dr. Stephen Kent Dr. Patrick Lincoln Mr. John Woodward

Page 977 of 3957

Thursday, July 13, 2000

8:00 – 8:30	Coffee – Sign-in	
8:30 – 10:00	COE	Mr. Ken Wheeler DISA
10:00 – 11:30	JWICS	Mr. Jim Watson DIA
11:30 – 12:30	General Issues Discussion	All
12:30 – 1:00	Lunch	
1:00 – 5:00	Integrate Briefings	All

Friday, July 14, 2000

8:00 – 8:30	Coffee – Sign-in	
8:30 – 9:00	Front End of Outbrief	Larry Wright
9:00 – 9:15	Findings & recommendations – Legal Panel	Stewart Baker
9:15 – 9:30	Findings & recommendations – Policy Panel	Rich Wilhelm
9:30 – 9:45	Findings & recommendations – Organization Panel	John Grimes
9:45 – 10:00	Findings & recommendations – Technology Panel	Rich Mendelowitz
10:00 – 10:15	Findings & recommendations – IAA Panel	Mike Frankel
10:15 – 15:00	Task Force Discussion on outbrief and other issues	All

Page 978 of 3957

Page 979 of 3957

APPENDIX D. ACRONYMS

Page 980 of 3957

Page 981 of 3957

ABIS	Advanced Battlefield Information System
AFRL	Air Force Research Laboratory
AH	Authentication Header
ARL	Army Research Laboratory
ASD/C3I	Assistant Secretary of Defense for Command, Control and Communications
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
BSC	Base Switching Center
BTS	Base Transmission System
C2	Command and Control
C3I	Command, control, communications, and intelligence
C4ISR	Command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAC	Common Access Card
CAP	Common Air Picture
CC	Common Criteria
CCA	Clinger-Cohen Act
CCITT	Consultive Committee on International Telegraph and Telephone
CDPD	Cellular Digital Packet Data
CEC	Cooperative Engagement Capabilities
CECOM	U.S. Army Communications Electronics Command
CERT	Computer Emergency Response Team
CGP	Common Ground Picture
CINC	Commander in Chief
CIO	Chief Information Officer
COE	Common Operating Environment
COI	Community of interest Connection-oriented interconnection
COMSEC	Communication Security
CONUS	Continental United States

COP	Common Operational Picture
CORBA	Common Object Request Broker Architecture
COTS	Commercial off the shelf
CVE	Common vulnerabilities and exposures
DARPA	Defense Advanced Research Projects Agency
DBS	Direct Broadcast Satellite
DCE	Distributed computing environment
DDR&E	Director Defense Research and Engineering
DEERS/RAPIDS	Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System
DFAR	Department of Defense Federal Acquisition Regulation Supplement (DoD)
DEPSECDEF	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DIAP	Defense-wide Information Awareness Program
DiD	Defense in Depth
DII	Defense Information Infrastructure
DISC4	Director of Information Systems, Command, Control, Communications, and Computers
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DIRNSA	Director National Security Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security
DoD	Department of Defense
DoS	Denial of Service
DOTMLPF	Doctrine, Organization; Training and Education, Materiel; Leadership; Personnel; and Facilities
DSB	Defense Science Board
DSL	Digital Subscriber Line
EJB	

ESC	Electronic Systems Center (U.S. Air Force)
FGAC	Fine grained access control
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GIG	Global Information Grid
GloMo	Global Mobile
GSM	Ground station module
HLR	Home Location Register
HQ	Headquarters
HQMC	HQ Marine Corps
IA	Information Assurance
IAA	Information Assurance Architecture
IATF	Information Assurance Technical Framework
IC	Intelligence Community
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IASA	Information Assurance Systems Architecture
IATA	Information Assurance Technical Architecture
IATF	Information Assurance Technical Framework
ICMP	Internet Control Message Protocol (DoD, TCP/IP)
IER	Information Exchange Requirements
IETF	Internet Engineering Task Force
III	Integrated Information Infrastructure
IKE	Internet Key Exchange (previously ISAKMP)
IM	Information Management
IN	Intelligent Network
INFOCON	Information condition
InfoSec	Information Security
IO	Information operations
IOC	Initial Operational Capability
IP	Internet Protocol

Page 984 of 3957

IPsec	Internet Protocol security
IS	Information Superiority
ISDN	Integrated Service Digital Network
ISO	International Organization of Standardization
ISP	Internet Service Provider
ISR	Intelligence, Surveillance and Reconnaissance
ISX	Information Superiority Experiment
IT	Information Technology
ITEF	Internet Engineering Task Force
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union (CCITT)
IW-D	Information Warfare-Defense
JCS	Joint Chiefs of Staff
JFCOM	Joint Forces Command
JIER	Joint Information Exchange Requirements
JMRR	Joint Mission Readiness Report
JOA	Joint Operational Architecture
JROC	Joint Requirements Oversight Council
JSA	Joint System Architecture
JSMB	Joint Space Management Board
JSTARS	Joint Surveillance Target Attack Radar System
JTA	Joint Technical Architecture
JTF	Joint Task Force
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
JV 2020	Joint Vision 2020
JWICS	Joint Worldwide Intelligence Communications System
KMI	Key Management Infrastructure
LAN	Local Area Networks
LDAP	Lite Directory Access Protocol
LEO	Low Earth Orbiting

Page 985 of 3957

LMDS	Local Multipoint Distribution System
M&S	Modeling and Simulation
MCEB	Military Communications Electronics Board
MEO	Mid Earth Orbiting
MIL-STD	Military Standard
MMDS	Multichannel Multipoint Distribution System
MRC	Major Regional Conflict
MSC	Mobile Switching Center
MSP	Message Security Protocol
NEO	Near Earth Orbit
NIAP	National Information Assurance Partnership
NIPRNET	Non Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NRE	Non-Recurring Engineering
NRL	Naval Research Laboratory
NRO	National Reconnaissance Office
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
NSB	Naval Studies Board
O&M	Operation and Maintenance
OA	Operational Architecture
OASD/C3I	Office of the Assistant Secretary of Defense, Command, Control, Communications & Intelligence
OMFTS	Operational Maneuver from the Sea
OODA	Observe, Orient, Decide, Act
OPFAC	Operations Facility
OPGP	Open PGP (Pretty Good Privacy)
OPNAV N6	Navy Operations
OPNET	Operations Network
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense

Page 986 of 3957

OSI	Open Systems Interconnect
PA&E	Program Analysis and Evaluation
PCS	Personal Communications Systems
PDA	Personal Digital Assistants
PEM	Privacy Enhanced Mail
PEO	Program Executive Office
PFF	Packet filtering firewall
PGP	Pretty Good Privacy
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PKIX WG	Public Key Infrastructure Working Group
PM	Program Manager
POM	Program Objective Memorandum
POP	Point of presence
PPP	Point to Point Protocol
PSTN	Public Switched Telecommunications Network
QoS	Quality-of-service
R&D	Research and Development
RM	Reference Model
RSTA	Reconnaissance, Surveillance and Target Acquisition
RSVP	Resource Reservation Protocol
RTP	Real Time Protocol
S&T	Science and Technology
S-HTTP	Secure HyperText Transfer Protocol
SA	System Architecture
SDE	Secure Data Exchange
SET	Secure Electronic Transactions
S-BGP	Secure Boundary Gateway Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SCP	Service Control Point
SILS	Standard for Interoperable LAN Security

Page 987 of 3957

SINCGARS	Single Channel Ground and Airborne Radio System
SIPRNET	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPAWAR	Space and Naval Warfare Systems Command (formerly NAVELEX)
SPKI	Secure Public Key Infrastructure
SSH	Secure Shell
SSL	Secure Socket Layer
SSNMP	Secure Simple Network Management Protocol
SSP	Switching Signal Point
STP	Signaling Transfer Point
SUO	Small Unit Operations
SYN	Synchronization
TA	Technical Architecture
TAFIM	Technical Architecture Framework for Information Management
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
TLSP	Transport Layer Security Protocol
TOR	Terms of Reference
TRANSEC	Transmission Security
TTP	Tactics, techniques and procedures
UHF	Ultra High Frequency
UL	Underwriters Laboratories
USAF	U.S. Air Force
USCG	U.S. Coast Guard
USD/AT&L	Under Secretary of Defense for Acquisition, Technology and Logistics
USPACOM	U.S. Pacific Command

Page 988 of 3957

AOAR	Area of Assigned Responsibility
VCJCS	Vice-Chair Joint Chiefs of Staff
VoIP	Voice over Internet Protocol
VLR	Visitor Location Register
VPN	Virtual Private Network
WAN	Wide area network
WIN-T	Warfighter Information Network-Tactical
WWW	World Wide Web
XML	Extensible Markup Language

Page 989 of 3957

ANNEX B

Defense Science Board Task Force
on
Defensive Information Operations

Panel Report on Technology

REPORT OF FINDINGS, DISCUSSION/OBSERVATIONS AND RECOMMENDATIONS

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

INTRODUCTION 3

RESEARCH TOPICS 7

Early Capability Assessment 7

Prevention and Protection 8

Consequence Management 12

Attribution 13

CROSS-AREA RESEARCH 15

Modeling and Simulation 15

Theory of Vulnerabilities 15

Interdependencies 15

Broad-Based Fundamental Research 16

GIG Research Coordination 16

Costs 17

CONCLUSIONS AND RECOMMENDATIONS 19

APPENDIX A. Task Force members A-1

APPENDIX B. Acronyms B-1

Page 991 of 3957

Page 992 of 3957

EXECUTIVE SUMMARY

Within the Department of Defense, the next several years will be marked by steadily increasing reliance on automated information systems. In accord with Joint Vision 2020 (JV2020), the Department will be proactive in supporting and shaping this evolution.

In recognition of this reliance on information systems and in reaction to attacks on DoD computer systems, the Department has begun a wide range of activities that focus on prevention of problems through protection of computer networks. The rapid advances in information and communications technology mean that as the years pass, entirely new infrastructures, embodying new technologies, will emerge – and each will be accompanied by its own set of new vulnerabilities. As a result, protection of networks will necessarily require continuous improvement. These protections will require vigorous and focused research. It is the view of this Technology Panel that an increase in research beyond current levels is required to minimize the vulnerability gap that will always exist between network vulnerabilities and network protection. It should be noted that DoD requirements for protection are likely to go well beyond what is required by the private sector.

As computer networks and weapon systems lose their individual identity and merge into one, protection will be necessary, but not sufficient to assure that networked information will be available when required. As this Defense Science Board has noted, despite the best network protection, attacks will occur and some will succeed. When a computer network has been attacked, the commander must be able to know:

- When will the system be restored?
- How much of the system will be restored?
- How much of the original system will operate?
- What are the consequences of limited network availability?
- Will the information on the network be reliable?
- How will the commander know for sure that the information is reliable?
- What options will be available to the commander?

Today, the answer to these questions would be, "We do not know." This is clearly a bad answer in peacetime and a totally unacceptable answer during a military operation.

The Department has reached a milestone with its awareness of computer network vulnerabilities, and with funded programs to address protection and defense of networks. Unfortunately, while restoration of network service, data integrity, and confidence in the data on the network are as important to success of JV2020 as network protection, these activities remain largely ignored and are essentially unfunded. Successful development and implementation of these "consequence management" functions are the next major milestone for DoD Information Assurance (IA).

Page 993 of 3957

The Department must also aggressively address its information assurance (IA) research and development (R&D) personnel requirements now, in order to avoid more serious problems in the next few years as more personnel leave the Department and fewer high-caliber R&D managers remain. Although this topic is addressed more extensively by another Panel report, we believe it is so fundamental that we endorse and highlight the finding. Education and training issues must be among the very first steps that the Department should take in this area. As urgent as the other IA technology issues are that we discuss below, this issue is the highest priority in the technology area. Without enough qualified and well-trained technical people, virtually all of the issues that the Department faces in IA will be even more difficult to resolve.

Protection of DoD networks is fundamental to the success of future operations, and this protection depends upon a very focused R&D program. However, this Panel finds that IA R&D activities are distributed among the Defense Advanced Research Projects Agency (DARPA), the services, and defense agencies. Some long-term research is ignored, and some short-term research is redundant. Accordingly, this Panel proposes a new and very focused management of IA R&D. Establishing an information assurance R&D office in the Office of the Secretary of Defense (OSD) that reports to the Global Information Grid (GIG) architect is the first step in bringing focus to IA R&D management. This R&D office will assure that DoD research for IA be coordinated, be subject to multi-year planning, take into account private-sector research, and be adequately resourced to minimize DoD network vulnerabilities on a rapid but achievable timetable. Given today's commercial product cycles, it is unlikely that any new DoD-sponsored research will produce protection results that can be transferred within three years into critical networks. DoD research must therefore be a long-term, continuous investment activity that should not be expected to play a significant role in the near term.

Moving resources from minimally funded protection activities to network restoration activities will not result in an acceptable solution for either problem. Establishing a new milestone of consequence management calls for additional funding. Since the commercial world has largely ignored this issue, solutions will have to start with a vigorous DoD R&D program. This Panel believes that the minimum R&D investment that should be added to current efforts to improve the overall security of the GIG is $350 million over five years– about twice the level of funding today.

Page 994 of 3957

INTRODUCTION

The 1996 Defense Science Board (DSB) Summer Study brought attention to the increasing reliance of DoD on networked computer systems. The DSB report noted the vulnerability of these computer systems, and the fragility of the information residing on and passing across these networks. It made strong recommendations that the Department increase emphasis on the protection of these systems and the information they held. The report also recommended that computer network defense (CND) become integral to the development and deployment of DoD networks.

During the four years since that report, the Department has made considerable progress on these recommendations. Awareness of computer network vulnerabilities is much higher, and various system components have been deployed specifically for network security. Research programs, principally at DARPA and the National Security Agency (NSA), have emphasized those defensive technologies that DoD requires but commercial systems are unlikely to include.

However, during that same period of time:

- DoD has greatly increased its reliance on information contained in, processed by, and distributed over networked computer systems.
- Information superiority has become essential to achieving JV2020. This vision requires highly secure networked systems.
- Intrusions into DoD networked computer systems have become more sophisticated and more frequent. (The frequency of these intrusions is similar to what is being experienced in the non-DoD environment.)
- Development and deployment of new network technology has greatly outpaced information assurance technology, increasing the vulnerability of DoD systems.

As a result, despite the considerable progress that is apparent within DoD, a computer network vulnerability gap has continued to increase. Systems complexity is growing faster than solutions. And while new network capabilities will most certainly always outpace defensive technologies, considerable DoD R&D must be devoted to computer network defense to manage and reduce the vulnerability of this critical capability.

Potential adversaries have recognized both the increasing reliance of DoD on networked computer systems and the opportunity they now have to diminish the effectiveness of DoD operations through active network attacks. For example, representatives of both China and Russia have expressed the belief that they can neutralize U.S. capabilities through information operations. The "Unrestricted War" concept from China and the Russian nationalist Vladimer's comment that "we can bring the entire West to its knees with our computer specialists" are examples of that thinking.

In order to assure the availability and integrity of critical DoD computer networks, the Department must develop a long-term strategy that posits a desired end-state for information assurance that is consistent with JV2020 and provides a roadmap for achieving that end-state. While many areas need to be included in an overall roadmap, the information assurance R&D

Page 995 of 3957

roadmap is fundamental. The key for DoD to be prepared on the scale required is an information assurance R&D program supporting the protection needs of the global information grid.

The information volume that JV2020 will need to handle and protect will be vast. It is already possible to project data rates that will require protection in the range of multiple terabits per second. These rates are comparable to moving the current Library of Congress electronically every minute. The DoD and intelligence databases in 2020 almost certainly will be many hundreds of times those of the current Library of Congress. While secure remote access to data will reduce somewhat the requirement for data rates and bandwidth that increase in proportion to the size of databases, it is still obvious that protecting information in the volumes required for successful execution of JV2020 will be a daunting task.

It has recently been understood that no matter how sophisticated defense of computer networks becomes, they will remain vulnerable to a determined adversary, disgruntled employee, or simply natural events. Experience shows that as our defensive capabilities increase, so will the adversary's offensive ones. U.S. adversaries over the next 20 years will be developing a range of attack capabilities that will likely cover every possible node and path of DoD networks.

There will certainly be attacks against DoD networks. Many will be ineffective, but more importantly *some attacks will succeed.* The results of a successful attack will range from an irritation or embarrassment all the way to serious disruption of critical DoD networks or information. The severity will depend on the attacker's skill level and resources, and the defenses DoD has in place. These attacks could result in serious damage to a critical DoD network, but could also compromise a warfighter's confidence in the information system he or she has to rely on – no matter what the attack actually accomplished.

Unfortunately, today DoD has no methodology for dealing with the consequences of a successful attack and restoring integrity in its systems. And so, with the ever-increasing reliance of DoD on computer networks as an integral component of war fighting, **this Defense Science Board finds that it is now necessary to develop technologies to help recover and restore its networks and the data they contain**. One of the key tasks in this area will be to restore the integrity of networked computer systems that have been attacked, or are thought to have been attacked, and restore confidence that they remain ready for their intended purpose. Warfighters must have confidence in their information and the technology that provides it. The technologies that will deliver effective defense in depth of DoD, be able to recover and reconstitute those networks after an attack, and restore their integrity, need considerable emphasis.

It should be noted that any list of research areas compiled today would certainly not be a complete list for tomorrow. Part of the information assurance R&D management challenge in the rapidly evolving world of information technology, is the frequent examination of those research areas most needed to provide defense of and integrity restoration to the latest computer network developments and deployments. Against the tide of technological advances and determined adversaries, considerable R&D will be required just to maintain the level of security we have today. Much of the R&D required by the DoD will not come from the private sector. To achieve and maintain the higher levels of protection required by JV2020, it will be necessary for DoD R&D investment to keep pace.

The DoD must provide the support for an aggressive R&D program that has the breadth and depth to deal with the entire spectrum of information assurance issues. These issues range from near-term needs to thwart the latest threats that surface, to long-term basic research. The latter

Page 996 of 3957

must be coupled with an examination of the R&D strategies necessary to satisfy the full range of JV2020 requirements. Further, the R&D program must result in products that are unique to DoD requirements and which complement and enhance commercial systems. Many of these research programs will necessarily be long term—not suited to short-term evaluations.

The specific amount of R&D funding required is likely to be a matter of debate, but the general level needed is at least a factor of two over the DoD information assurance R&D spending of today. There are many areas that are today minimally funded, which this report highlights. There are certainly many more areas that time did not allow us to pursue, or that have simply not yet been articulated.

Page 998 of 3957

RESEARCH TOPICS

The pace of technology growth guarantees that any list of needed research topics will be incomplete shortly after it is written. Part of the information assurance R&D management challenge in the rapidly evolving world of information technology is the frequent examination and re-evaluation of those research areas most needed to provide defense of and integrity restoration to the latest computer network developments and deployments.

Keeping in mind the need for frequent re-evaluation of R&D programs in light of commercial developments, research successes, and new deployments, there are four general topic areas that prove useful in categorizing R&D for computer network defense. This report provides findings on areas of necessary research in each category of a network attack timeline, namely:

1. Early Capability Assessment
2. Prevention and Protection
3. Consequence Management
4. Attribution

What follows is a general description of each of these topics together with some representative technologies that this Panel feels currently need increased attention.

EARLY CAPABILITY ASSESSMENT

Computer network defense, like any defense, is most effective if the intentions and capabilities of an identified adversary are understood, and when it is known that offensive operations have, in fact, begun. The technology for this entire area of intelligence, indications and warning, intention, and identity-determination is complicated by legal and policy issues, which are discussed elsewhere in this report. Examples exist today of attacks which have gone unnoticed, of intrusions with unknown purpose, and of network disruptions that have remained un-diagnosed. This is a technology area that must mature as JV2020 develops. Some necessary research topics include the following.

Cyber Intelligence Tools

One of the weakest aspects of U.S. defensive information operations is our extremely limited ability to detect, assess, and understand both hostile information operations (IO) capabilities and precursor indications and warning of attack. A program is required to develop tools to attenuate these shortcomings. Advanced active agents using secure mobile code would be developed that could gather information without taking any hostile actions. "Picket" or "sentinel" agents could provide early warning of hostile action or intent. This program will ideally result in an array of tools that will provide a much greater understanding of hostile IO capabilities against the United States and its allies and better warning of incipient attacks.

Attack Pattern Discovery

No methods exist for automated or assisted discovery of existing or novel attack patterns or signatures, particularly for those attacks that are distributed across many computers or networks.

PREVENTION AND PROTECTION

Much of the progress within DoD since the 1996 DSB report has been in the area of protection of DoD networks and prevention of unauthorized access. These are very important and sensible places to begin the defense process. However, as DoD becomes more and more dependent on networks, and as the complexity of these networks increases, the opportunities for disruption will also increase. R&D is required that is specifically designed to prevent problems caused by both insiders and outsiders, to prevent unknown attacks, and to guard against commercial systems with unknown flaws. The science of network security is currently immature, but with proper R&D infusion, the foundation for the protection required by JV2020 can be put in place.

Representative areas of research to enhance protection of DoD networks and prevention of unauthorized access would include those that follow.

Scalable Global Access Control

Current DoD network architecture calls for a secure network with authorized access via tokens – a public key infrastructure (PKI). The scope of this security apparatus is enormous. It will involve distribution of secure capability to multiple locations in many countries. It will require limited access for foreign coalition partners. It will necessitate the distribution of millions of tokens – some number of which must be issued and revoked on a daily basis. It will require rapid implementation and expansion during a period of crisis. It cannot burden the user. It must withstand insider attacks.

These are severe requirements. PKI has not been modeled and tested under extremes of this type. It is the security backbone of the future, and must be supported by a vigorous R&D program that addresses its scalability, its extremes, and any vulnerability. It requires the same attention to detail that continuous testing of high-grade cryptographic systems has had over the past several decades.

Malicious Code Detection and Mitigation

The need to nullify malicious code is acute for both the defense information infrastructure and the national information infrastructure because of increased connectivity and reliance on the Internet, increasing prevalence of mobile code, and likely development of and access to code by disgruntled insiders and outsiders.

Malicious code is defined as a program that is written or introduced into a system by someone with malicious intent. The program is intended to damage system function without the operator's knowledge or consent. It is the most rapidly emerging and least understood cyber threat to DoD information systems. Examples of such code are Trojan horses, viruses, worms, trap doors, and time bombs, and each has had notorious successes in worldwide attacks against commercial and military networks and systems. Ominously, the latest versions of these codes represent a merging of the characteristics and capabilities of these existing threats into new, more

Page 1000 of 3957

powerful forms. Code mobility provided by the World Wide Web has further facilitated the spread of malicious code.

Presently, malicious code is being countered by firewalls, virus-checking software, and similar defensive mechanisms. These mechanisms rely on knowledge of past attack modes. The response to new attacks is reactive, i.e., the response occurs after the attack has been initiated, significant damage to data has been done, and systems have been shut down to cleanse them. Well-designed attacks are succeeding, with such denial-of-service events as Trinoo scripts and "I love you" viruses not only damaging services, but also eroding confidence in the security of both commercial information and the systems required for national defense.

Future research needs to enable malicious code defenses to become more proactive. It must enable real-time detection and neutralization of attacking codes, the development of tolerant system architectures, and the creation of security policies and policy enforcement mechanisms. Though security policy may seem a vague abstraction, it is crucially important in controlling malicious code. Without a security policy that defines what actions are prohibited, it is difficult to argue that any code is malicious and even harder to define policy enforcement mechanisms.

Mitigating and eliminating malicious code in its many forms is crucial for protecting the information infrastructures that are an integral part of our society and the backbone of JV2020. Research for the following areas will require a multi-disciplinary approach that brings together experts from computer science, information security, and real-time systems design. Overarching research needs to be undertaken in the following areas: (1) defining a malicious code taxonomy to facilitate research discussion, (2) providing a mapping between this taxonomy and the kinds of mechanisms that would be needed to protect and detect malicious code, and (3) designing new software architectures and tolerance measures that would facilitate elimination of malicious code. In addition, specific research is required for addressing malicious code, including: (1) semi-automatic source code inspection for existing attacks (static), (2) dynamic code scanning, (3) system integrity checking, (4) reverse engineering, and (5) code signing. This research will broaden coverage of the information assurance spectrum, advance an emerging information assurance industry, and contribute to a deeper understanding of defensive information operations.

Mobile Code Security

Mobile code security decomposes into three challenges:

- Protect hosts from malicious inbound code
- Protect code from malicious hosts
- Construct survivable distributed systems capable of tolerating compromised elements

Although the question of protecting hosts from malicious code is far from resolved, this challenge represents a special case of the general malicious code. The distributed nature of malicious mobile code opens opportunities not available to isolated systems.

Protecting individual parts of mobile code from malicious hosts represents a more difficult problem given natural dependencies on the executing platform. Although general solutions seem distant and speculative at this point, the potential at least bears further exploration.

Page 1001 of 3957

Conversely, it may be possible to leverage code mobility in constructing survivable distributed systems more capable of tolerating compromised elements. This potential stems from the ability to dynamically distribute an application across many hosts. Such dynamic fragmentation could eliminate a priori information necessary for adversarial strategic targeting. Moreover, if future network bandwidth and computing power facilitate shipping both internal memory structures (e.g., stack) and code snippets around the network, architectures could be constructed with far less exposure at any given time. The challenge of leveraging code mobility to increase survivability seems quite promising as a general area of research.

Anomalous Behavior Detection

The technologies for detecting anomalous behavior are too brittle to produce robust and useable results. Outcomes are laden with false alarms and missed events, both of which increase human and system workload, while reducing confidence in results. These technologies are badly needed for mitigation of the insider threat, as well as for underpinning downstream technologies for detection of related threats.

Fault Tolerance

There is a paradigm-shift taking place in the technical approach to information assurance and defensive information operations. The decades-old approach of resisting attacks and trying to keep all intruders out does not work in the new Internet age. Prevention and avoidance techniques must be augmented with fundamentally secure architectures that can tolerate mobile and malicious code, active content, distributed denial-of-service attacks, and insider threats. We must strive to make systems inherently more tolerant and resilient to attacks, malicious faults, and insider misuse and abuse.

Fault-tolerance technologies have been successfully used to construct highly available and reliable systems for transportation and financial sectors as well as real-time control of plants, vehicles, and command and control systems. Such fault-tolerant systems have been designed to cope with naturally occurring faults and failures such as hardware component faults, design errors in software, and environmentally induced faults such as transients caused by lightning. Advanced research is needed to adapt these technologies for intentional faults and attacks mounted by a human adversary. Research is also needed in creating fundamentally new intrusion- and attack-tolerant systems that use and exploit design diversity, stealth, randomness, and uncertainty as built-in system attributes.

Page 1002 of 3957

Investment in the following specific technologies is important to achieve the goals of survivable, fault-tolerant systems:

Proof Carrying Code
Secure Mobile Code Languages
System Health Monitors/Tolerance Triggers
Stealthy System Structures
Dynamically Reconfigurable System Architectures
Data Recovery Schemes
Composability of Trust
Design and Implementation Diversity
Uncertainty, Randomness, Agility, and Deception
Code Execution Real-Time Monitors
Fragmentation, Redundancy, and Scattering
Security Policy Specification

High-Speed Encryption

Over-the-network access, both to classified and unclassified-but-sensitive information, is of critical importance, as the Global Information Grid becomes reality. The near-instantaneous global access available once one is "inside" the protected network raises the issue of how to recover quickly from problems such as the loss of an encryption device. There is also the necessity to rapidly add or remove coalition partners from a network during international operations.

For the DoD to conduct operations using the GIG, it must have the ability to almost instantaneously remove selected (compromised) users from the grid, while at the same time permitting the remaining users to continue to conduct their operations. Important pieces of this complex problem are being solved. The STU-III model was a start, but the supporting infrastructure does not scale to required levels. There are upgrades underway, but they are not of the scope necessary to address JV2020 requirements.

At least three major technical challenges exist. First is the development of a high-speed encryption device that can scale to the 10 Gbps rate and beyond. A second challenge is to build an encryption device that is protocol-, algorithm-, and key-agile. This class of device is required if the GIG is to be interoperable with legacy devices and with coalition partners. The third challenge is to reduce the cost of the security functions and to integrate them into embedded capabilities that are transparent to the users. The more transparent the security functions are, the more they will be used and not bypassed in time of crisis. The DoD needs to work with vendors in the earliest stages of developments to integrate highly scaleable security into their products.

Advanced Intrusion Detection/Monitoring

Intrusion-detection technologies currently produce only moderately reliable results in simple environments, and even less-reliable results in complex environments. In terms of correlating and fusing information from distributed sensors in distributed attacks, what little technology exists is too immature to be useful. Intrusion-detection technologies are critically dependent on

Page 1003 of 3957

monitored sensory data. However, with respect to what is monitored and the places from which the monitoring data are taken, little to nothing is known about either how to decide what should be measured, or how to determine the most effective placement of sensors in an operational environment.

CONSEQUENCE MANAGEMENT

Some network attacks will be successful, and DoD does not have adequate technology in place to address the consequences of the successful attacks. Even as we improve our ability to protect networks and systems from attacks, some attacks will be successful. When a successful attack occurs, we must have tools, techniques, and procedures in place to limit the consequences. The need to continue operations, even at a reduced level, is critical in military operations. Research is needed to improve our ability to address the impacts of successful attacks. Some of the areas that should be included in a research program are self-healing networks and systems, network isolation, integrity restoration, and recovery and reconstruction.

DoD needs to fund research that will allow networks and systems to isolate attacks, gracefully degrade performance if necessary, and automatically heal themselves to a level that will allow users to be confident in using the networks and the information on the networks.

Integrity Restoration

DoD does not have a methodology for restoring integrity in its systems. If a user loses trust in a system, because of an attack (internal or external), or because of a perceived problem, there is a need to validate that the system is performing all functions accurately. Trust in a system can be lost as a result of bad data, natural events, degraded performance, fear of tampering, inconsistent data or decisions, or anything that causes the user to question the usefulness of the system. Tools and methodologies are needed to address system user questions such as:

- Was something done to the system?
- What was done to the system?
- Is the system OK?
- Is the data reliable?

Only if the integrity of the network can be assured to the satisfaction of the user will the system be used as intended.

Recovery and Reconstitution

When a network or system is successfully attacked, there is a need to return it to a useable level of service and ensure that the same attack will not produce the same negative result. Recovery is the process of taking a system from an unacceptable level of performance to a minimum level. Reconstitution is the process of taking a system from the unacceptable or minimum level of performance and returning it to full performance. In addition, the reconstituted system should not be susceptible to fail in the same way from the same attack. The ability to recover and reconstitute a system will increase trust, improve protection against future attacks, and provide systems that have increased availability.

Page 1004 of 3957

ATTRIBUTION

Once it is determined that a network has been attacked, automated tools are necessary to understand exactly who initiated the attack. Attribution is essential to establish the attacker's motive and to determine an appropriate response.

Observed and reported attacks against DoD computer networks are growing at a rapid rate. As better defense audit tools become available, the number of incident reports will most certainly increase. In general, it is impossible at present to determine the origin and intent of the incident originator. Such incidents could be the result of accidents, curiosity, thrill seeking, intelligence gathering, or deliberate attempts to damage DoD computer networks. The identification of the originator of the incident is one of the pieces of information necessary to scope the response. However, attribution tools are slow at best, are complicated by legal issues, and often fail to reach the masked identity of a skillful attacker.

An extensive R&D program focused on attribution needs to be developed. This is an area where extensive civil, law enforcement, and DoD interaction is essential. Some suggested areas of research include those that follow.

Message Signature Processing

Advanced research is needed to develop algorithms that transform extremely high-bandwidth Internet traffic channels into near-real-time searchable signature spaces such that an attack can be quickly correlated against the passively collected signature stores at multiple nodes. Near-real-time correlation capabilities could narrow the potential set of attributable source points and facilitate rapid engagement of appropriate traps and traces.

Active Code Beacons

Attacks that rely on covert target responses could theoretically be co-opted by the infusion of active code beacons in the return traffic – beacons that would provide attribution information. Research is needed to develop this and other active attribution concepts.

Identification Friend or Foe (IFF) tools

Research in this area would determine if the Identification Friend or Foe concept could be extended to cyberspace to support authentication functions with minimal resource requirements.

Page 1005 of 3957

Page 1006 of 3957

CROSS-AREA RESEARCH

There is a broad category of needed R&D that does not fit within the attack phases described earlier, but rather is common to most or all of them. Precisely because of this somewhat non-specific nature, there is much less research being conducted than necessary for the long-term health of the GIG and DoD's overall information infrastructure. In most cases, this R&D lacks a logical "ownership" – it often does not fall clearly within the responsibility of an organization or an industry, and as a result is insufficiently funded.

Below we provide a list of what this Panel believes are the most important areas of research that cut across the attack timelines. Each is discussed in turn.

1. Modeling and Simulation
2. Theory of Vulnerabilities
3. Interdependencies
4. Broad-Based Fundamental Research
5. GIG Research Coordination

MODELING AND SIMULATION

Progress in defending and protecting the GIG will require a far greater ability to model and simulate the performance of information infrastructures than we have today. Currently, much of today's modeling and simulation is based on ad hoc, relatively inaccurate techniques that are specially – and slowly – developed for each specific application. Advanced modeling and simulation techniques will be necessary to characterize and observe the behavior of networks and systems, especially under stressed conditions. Such capabilities will be essential to using an IA test bed effectively. A successfully executed R&D program should result in tools that accurately characterize a wide variety of information infrastructures. Even more advanced versions would allow a rapid, automated way of performing such modeling and simulation exercises.

THEORY OF VULNERABILITIES

Neither system administrators nor commanders can fully rely on today's vulnerability analyses, which are ad hoc, incomplete, unreliable, and unrepeatable. Although some ad hoc analyses can be useful, no theory or associated science exists whereby vulnerabilities can be systematically and completely discovered, assessed, and measured in terms of their effect on operational readiness.

As has been pointed out in earlier studies, one of the most significant gaps in IA research is system-level security engineering, particularly in the area of system-level security architectures. System-level security engineering must be further supported by basic research in IA fundamentals, particularly in the areas of availability and integrity.

INTERDEPENDENCIES

To date there has been very little research into the interdependent effects that can accompany the interconnection of multiple infrastructures, both of the same general type and completely

Page 1007 of 3957

different ones, e.g., the interdependencies between information networks and the electric power grid. The possibility of cascading and nonlinear effects from such interdependent systems is rhetorically acknowledged but little understood or studied. While responsibility for networks or other infrastructures is often easily identifiable, no organization has an institutional responsibility for interdependent effects. As networks and infrastructures become ever more tightly interconnected, the likelihood and magnitude of such effects will become greater.

This research would seek to understand the nature and origin of interdependent effects and how they propagate between and among infrastructures of varying degrees of complexity. Feedback control theory, network analysis, advanced modeling techniques, and other disciplines would be used in conducting this research, which would seek to assess both intentional (hostile) attacks and naturally occurring instabilities (such as network "storms"). As research progressed, infrastructures with increasing numbers of nodes and interconnections would be studied. At some point, an IA test bed would become an invaluable tool for such analysis.

This research program would seek to shed greater light on the mechanisms and modes of propagation of interdependent effects and suggest technical, management, and policy steps that could serve to both reduce the likelihood of these effects occurring and damp them out once they occur.

Broad-Based Fundamental Research

There is relatively little fundamental research on information science, network theory, and network failure. In the private sector, the chief focus is on product development. Private-sector research rarely looks beyond a two-year time horizon. Government and academia have more of a charter to do this kind of research, yet they are not as attuned to needs as is the private sector. At an October 1999 meeting at the White House, the chief technology officers of 15 telecommunications and information technology companies agreed that the private sector had little incentive to conduct such research, although they, along with academia and government, certainly had the necessary resources.

GIG Research Coordination

Management of IA R&D in DoD is fragmented and not focused to meet the rapidly changing threat environment.

The recognition of the GIG as a weapon system calls for a different model for the planning and execution of an IA R&D program to support system implementation. A focused research program will involve academia, industry, and government researchers. Other findings in this report have identified areas where increased funding needs to be applied. This report also points out that the IA environment has changed significantly over the past four years and is likely to change rapidly in the coming years. Such rapid change requires that a flexible R&D plan be developed, one that maintains a balance between near- and long-term problems.

The GIG Executive Office established by the Information Superiority Board (see Architecture Recommendation #1) will develop an R&D plan to execute the additional funding recommended by the DSB.

Page 1008 of 3957

- The plan will be developed in cooperation with the Under Secretary of Defense Acquisition, Technology and Logistics, the Assistant Secretary of Defense C3I, service laboratories and centers, and appropriate DoD agencies.
- The Information Superiority Board will approve the plan.
- The approved plan will be executed through existing DoD R&D activities (service laboratories and centers, and DoD agencies).

In conjunction with increased research, there is a need to increase the number and quality of people available to conduct IA research. While progress has been made in IA R&D over the last four years, the number of qualified researchers to conduct required research does not meet demand. There is a need to attract more students and faculty in IA research areas. Consistent funding levels and long-term commitments to specific technical thrusts are needed to have a significant impact on the academic community. Qualified researchers will not only allow for increased amounts of research to be performed, but it will also provide a talent pool for industry and government to reduce current projected hiring shortfalls.

Costs

The Panel was briefed on existing DoD IA and related R&D programs, which were noted earlier. These programs are budgeted at about $350-400 million per year. Given the major role that the GIG will play in the decade ahead, this figure represents a serious underfunding of a critical defense requirement. The Panel's first compilation of R&D that would make a useful contribution to the IA challenge had a total five-year price tag of $3-5 billion. A program of this magnitude would not only be fiscally unaffordable, but it would also likely exhaust the human resources available to execute the program. Accordingly, the Panel prioritized the research options and developed three categories of IA R&D programs.

Category 1 R&D is of the highest priority and encompasses R&D that the Panel believes is the minimum that should be added to current efforts to improve the security of the GIG. This R&D category has a five-year estimated cost of $350 million.

Category 2 R&D is intermediate in priority and is considered important to securing the GIG and providing a sustained basis on which to maintain GIG security well into the future. It has a five-year estimated cost of an additional $1.2 billion.

Category 3 R&D is lower in priority but would make useful contributions to GIG security and would minimize chances of major vulnerability surprises to both the DoD-unique information infrastructures and the civilian information infrastructures that directly support DoD. It has a five-year estimated cost of an additional $2.7 billion.

Page 1009 of 3957

These programs are presented below at their recommended funding levels at each level of funding:

	Category 1 $(M)	Category 2 $(M)	Category 3 $(M)
Scaleable network architectures, sensing, diagnosis:	15	35	80
Malicious code detection and mitigation:	15	30	70
Self-healing networks and systems:	20	65	150
Remediation, recovery, and reconstitution:	30	100	250
Attribution, traceback, forensics, tagging:	25	75	170
Advanced IA modeling and simulation:	30	130	300
Global key management and scalable global access control:	20	55	140
Integrity restoration:	15	50	120
Advanced steganographical techniques:	10	35	80
Metrics research:	10	35	80
Interdependent effects:	15	40	100
Advanced network sensors:	5	25	60
Cyber intelligence tools:	5	35	80
Mobile code security:	10	35	80
Anomalous behavior detection:	5	20	50
Fault-tolerant systems:	15	45	100
High-speed encryption:	40	75	180
Network fault management:	5	20	50
Network isolation:	10	30	60
Electronic friend or foe identification:	5	20	50
Theory of vulnerabilities:	5	20	50
Automated vulnerability assessment tools:	10	20	50
Advanced visualization tools:	5	35	80
Advanced intrusion detection and monitoring:	10	25	60
Attack pattern discovery:	5	35	80
Advanced biometrics research:	0	15	40
Integration tools for coalition warfare:	5	10	50
Research on related societal-issues:	5	35	100

Page 1010 of 3957

CONCLUSIONS AND RECOMMENDATIONS

The rapid advances in information technology and telecommunications have created a comparably accelerated need for a vigorous, sustained, and balanced program of information assurance R&D. This Panel emphasizes in the strongest possible terms that the IA R&D challenge will be dynamic, growing, and likely never-ending. There are several reasons for this:

- Those who would wish to attack our information infrastructures will constantly be developing new techniques to do so.
- The rapid advances in information and communications technology mean that as the years pass, entirely new infrastructures embodying new technologies will emerge – and each will be accompanied by its own set of new vulnerabilities.
- These new technologies will offer entirely new tools to those who would attack these systems.
- As both current trends and the dictates of complexity theory suggest, systems will become ever more tightly connected and coupled. This will provide new avenues for non-linear and interdependent effects to exhibit themselves, whether through attack or just non-hostile information "storms."

The Department has been alert to the issues that the IT revolution poses to the composition of future forces. However, the Department is:

- Not addressing its IA R&D personnel requirements with sufficient aggressiveness or creativity, which will likely lead to more serious problems in the next few years as more personnel leave the Department and fewer high-caliber R&D managers remain. Although this topic is addressed more extensively by another Panel report, we believe it is so fundamental that we also need to emphasize the finding. Education and training issues must be among the very first steps that the Department should take in this area. As urgent as other IA technology issues are that we discuss below, this issue is the highest priority in the technology area. Without enough qualified and well-trained technical people, virtually all of the issues in this field that the Department faces will be made much worse.
- Providing insufficient R&D funding to help ensure that the GIG, on which it is placing virtually complete reliance for all future operations, will be secure enough that decision-makers and field commanders will have confidence in the system.
- Managing its current information assurance R&D in a fragmented way that is not sufficiently focused on the information assurance requirements of the GIG. The Department is strongly committed to the Global Information Grid. This commitment requires that those responsible for building and managing the GIG must implement a more robust IA R&D program to assure GIG security in the future.

While the Department's information assurance capabilities are today increasing with time, its dependence upon its information infrastructure is increasing even faster. Unless the Department moves aggressively to address its IA R&D issues, the vulnerability gap will definitely increase.

Page 1011 of 3957

To strengthen information assurance, the Panel recommends changes to DoD R&D management. Specifically it suggests the following:

- Establishing an information assurance R&D office within OSD that reports to the GIG architect.
- Providing funding of IA R&D *above the current baseline* to this IA R&D office. The actual R&D should then be executed through DARPA, NSA and the service laboratories. Over time, we believe that much of the existing baseline R&D should be shifted to the IA R&D office.
- Providing the IA R&D office with the flexibility to shift some level of funding to meet rapidly emerging threats and vulnerabilities.

Finally, it must be emphasized that these technologies will require *new* investment. Moving resources from minimally-funded protection activities to network restoration activities will not result in an acceptable solution to either problem. Establishing a new milestone of consequence management calls for additional funding. Since the commercial world has largely ignored this issue, solutions will have to start with a vigorous DoD R&D program. This Panel believes that the minimum R&D investment that should be added to current efforts to improve the overall security of the GIG is $350 million over five years– about twice the level of funding today.

Page 1012 of 3957

APPENDIX A. PANEL MEMBERS AND GOVERNMENT ADVISORS

Co-Chairs:

Mr. Rich Mendelowitz	General Dynamics
Dr. Robert Mueller	Raytheon Company

Members:

Mr. Bruce MacDonald	Consultant
Dr. Joe Markowitz	Consultant
Dr. Roy Maxion	Carnegie Mellon University
Dr. Dennis Polla	University of Minnesota

Government Advisors:

Dr. Doug Maughan	DARPA/ITO

Page 1013 of 3957

Page 1014 of 3957

APPENDIX B. ACRONYMS

CND	Computer Network Defense
DARPA	Defense Advanced Research Projects Agency
DSB	Defense Science Board
GIG	Global Information Grid
IA	Information Assurance
IFF	Identification Friend or Foe
IO	Information Operations
JV2020	Joint Vision 2020
NSA	National Security Agency
OSD	Office of the Secretary of Defense
PKI	Public Key Infrastructure
R&D	Research & Development

Page 1015 of 3957

ANNEX C

Defense Science Board Task Force
on
Defensive Information Operations

Panel Report on Organization and Operations

REPORT OF FINDINGS, DISCUSSION/OBSERVATIONS AND RECOMMENDATIONS

TABLE OF CONTENTS

TABLE OF FIGURES iii

EXECUTIVE SUMMARY 1

INTRODUCTION 3

I. Organization and Operations Policy 4

II. Resources 11

III. Personnel 15

IV. Operational Readiness 23

Conclusion 31

APPENDIX A. References A-1

APPENDIX B. Task Force Members B-1

APPENDIX C. Policy Matrix C-1

APPENDIX D. Organization and Operations Panel Questionaire D-1

APPENDIX E. DIAP Program Development and Integration Team (PDIT) Briefing E-1

APPENDIX F. Acronyms F-1

Page 1017 of 3957

Page 1018 of 3957

TABLE OF FIGURES

Figure 1 - Organization and Operations Panel Focus Areas 3

Figure 2 - OSD-Internal Taxonomy Differences: A Case In Point (IA vs. CIP) 4

Figure 3 - DIO Policy Assessment 5

Figure 4 - IO/IA/CIP Organizational Relationships 6

Figure 5 – Information Operations Problem Space 7

Page 1019 of 3957

Page 1020 of 3957

EXECUTIVE SUMMARY

Although the Department of Defense (DoD) has responded to most of the recommendations of the 1996 Defense Science Board (DSB) report[1], progress has been hampered by an incomplete policy framework, insufficient funding, and, most significantly, the fact that the Defensive Information Operations (DIO) challenge has grown more difficult. The goalposts have been moved during the play. The entire DIO landscape continues to be populated with conflicting definitions and policies, unclear roles and responsibilities, and apparent competition among the information operations, information assurance, and critical infrastructure protection (IO/IA/CIP) policy focus areas. The General Accounting Office and DoD Inspector General's office, in several reports[2] issued since the 1996 DSB report,[3], have identified persistent policy and resource issues associated with IA implementation. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) raised the same concern in its *Ninth Assessment of the Information Security Status of Government Systems.*[4] The Organization and Operations Panel recommends improving this situation by declaring a moratorium on changes to existing IO/IA/CIP-related definitions, while progressing toward agreement on definitions for terms used in common by the DoD and intelligence community, but for which agreed definitions do not now exist. Simultaneously, the panel recommends that specific service- and agency-level policy documents be prepared as required to locally implement aspects of policy established at the Secretary of Defense/Office of the Secretary of Defense (SecDef/OSD) and/or Chairman of the Joint Chiefs of Staff (CJCS) level. The panel recommends the Network Operations (NETOPS) framework be adopted throughout DoD, with Commanders-in-Chief (CINCs), services and agencies collocating their network management and IA/computer network defense operations in the same center. The panel further recommends that the U.S. Space Command be authorized to establish a DoD-wide DIO threat detection and warning capability, using the modified GIG as a technology baseline. This capability should include a feed to the National Operations and Intelligence Watch Officer Network (NOIWON) system. The panel also recommends that a Defense Science Board study be commissioned to specifically address information-attack (cyber) indications and warning.

The panel recognizes that few of the needed improvements cited in this report will come free of cost. However, seen against the value of the underlying equities, the resource requirements identified are small. More to the point, the panel recognizes that military operations and national security, writ large, cannot be successfully prosecuted in the information age without heavy reliance on networked information technologies in public and private hands. Military operations and national security activities must acknowledge and plan for the unintended consequences of commercial infrastructure interdependencies, and networked information technologies must be ever more secure, reliable, and available to meet the full range of foreseeable scenarios and

---

1 Defense Science Board, Information Warfare-Defense 1996.

2 GAO/AIMD-96-84, GAO/AIMD-98-92, GAO/AIMD-99-107, GAO/NSIAO-00-107; DoD IG Reports 99-069, D-2000-058, D-2000-124.

3 Defense Science Board Report, IW-D 1996.

4 NSTISSC Report, Feb 2001 (draft).

Page 1021 of 3957

contingencies. There is simply no other option. The panel recommends that DoD develop a DIO funding strategy and profile, establishing priorities where sufficient funding does not exist; continue to conduct front end assessments (FEA) to shape DIO issues for program and budget decisions; establish a program element (PE) structure for all DIO resources; require mandatory migration of all DoD DIO resources into the new PE structure; address DIO requirements in the Joint Requirements Oversight Council (JROC) (CINC/Service participation); and establish program funding support for DIO requirements. Fully staffed requirements and Planning Program and Budgeting System (PPBS) visibility of all information assurance activities, especially the services' execution of Title X "staff, equip, and train" responsibilities, will greatly assist the U.S. Space Command in planning and executing its more focused and limited operational missions of computer network defense and computer network attack.

The "human face" of DIO is seen through qualitative and quantitative assessment of personnel – military, civilian and contractors – engaged in critical information-protection functions. The panel has identified serious deficiencies in each of these areas, while recognizing that the primary threat to total system security takes the form of trusted – but untrustworthy – insiders. Absent a broad based and sustained effort in the areas of hiring, training, retention, and security, all progress and expense associated with DIO hardware and policy could be for naught. The panel recommends DoD provide recruitment, retention, and proficiency pay for critical DIO skills (authorities exist to do this); develop formal career paths for DIO officer, enlisted, and civilian personnel; develop an outsourcing strategy to complement DoD key DIO resource needs; establish policy to develop and implement formal education training and awareness (ETA) programs for DIO; and require contractor personnel performing outsourced DIO functions to meet ETA criteria required for government employees. Furthermore, the panel recommends that the department strengthen and expand the role of the Reserve Component in DIO by implementing the Reserve Component Study and the DSB Task Force on Human Resources Strategy Study recommendations.

The panel focused primarily on the operational readiness aspects of DIO given its belief that Joint Vision 2020 cannot be achieved without assured access to information. While topics such as policy, personnel, and resourcing are closely related matters of concern, the readiness of joint forces to protect their access to superior information is the prime consideration. Readiness itself can be dissected into issues of metrics, the adequacy and currency of doctrine, rules of engagement, etc. Supporting processes such as red teaming, while addressed in the 1996 DSB report, have not progressed satisfactorily, and existing efforts fall far short of visible needs in this area. The panel recommends DIO be integrated into all operational mission planning to better assure information superiority; DIO be incorporated into formal readiness reporting mechanisms to better measure unit readiness; DIO red teams be formalized and empowered throughout the DoD to stress and evaluate readiness; and computer emergency or incident response teams (CERTs/CIRTs) be established and supported in the department to provide standard alerting and emergency response procedures.

The point is made in the Policy section of the DSB DIO report that national-level policies are deficient in this area. At the same time, policy discontinuities exist both internally in DoD and between DoD and other components of government necessarily engaged in total governmental DIO efforts. Issues of concern in their own right, these unresolved policy debates also stymie efforts to achieve much-needed progress in areas of resource management and training.

Page 1022 of 3957

INTRODUCTION

The Organization and Operations Panel met between January and August 2000 to review DoD policy, military readiness, organization, training, and resources, and the relationship of each to DIO. Its charter was to examine how the department is organized to execute DIO missions and maintain its readiness for DIO operations.

In the course of conducting this assessment, the Organization and Operations Panel met as a group, received briefings, and considered topics related to its mission, while also participating in task force-wide meetings and discussions. This approach permitted division of effort to focus on the categories of activity listed below. At the same time, it also facilitated identification of cooperative associations between and among issues. An example of the latter would be the relationship between structured readiness reporting by operational units and special-purpose units such as Red Teams. Readiness is measured against defined standards. Red Teams have specific criteria that they operate against which may or may not address those standards, but are a test against a stated level of readiness.], engaged in the level of readiness against defined standards. To provide some background support for proposed recommendations, the Organization and Operations Panel sponsored a DoD questionnaire about Information Assurance (IA) activities to solicit input on issues of concern to the DIO Task Force. The questionnaire results, analysis, and conclusions are provided in Appendix D to this Annex.

The Organization and Operations Panel identified four major categories of findings related to the DoD's execution of the IA/CND/DIO mission areas. These findings are supported by the survey results and are organized into the focus areas enumerated in Figure 1. Discussion of the panel's findings and recommendations follows.

1. Organizational Policy
   - 1.1 Policy and Definitions
   - 1.2 Organizational Roles, Missions, Responsibility Confusion
   - 1.3 Collocation of Network Management and Computer Network Defense Operations
   - 1.4 Threat Warning and Attribution; Indications and Warning
2. Resources and Management
   - 2.1 DIO funding throughout DoD
   - 2.2 Program Element Structure
3. Personnel Issues
   - 3.1 Career Path Management
   - 3.2 Education and Training
   - 3.3 Know Your Insider
   - 3.4 Reserve Component
4. Operational Readiness
   - 4.1 Integration of DIO into mission planning and execution
   - 4.2 Readiness Assessments, Reporting, and Metrics
   - 4.3 Red Teams
   - 4.4 Computer Emergency Response Teams

Figure 1 - Organization and Operations Panel Focus Areas

Page 1023 of 3957

I. ORGANIZATION AND OPERATIONS POLICY

A. Policy and Definitions (Internal to DoD and the Intelligence Community)

FINDINGS: Conflicting definitions and usage related to IO, IA, and CIP within the DoD and Intelligence Community (IC) causes resource and equity fights within the national security community and inhibits progress in resource management, training, and other important areas.

DISCUSSION: This problem exists on several levels. Some DoD/IC definitions and terms are not fungible across government and/or acceptable within the civil sector working cooperatively with government on critical infrastructure protection; those issues and recommendations are found elsewhere in this report.

Traditionally, the Defense Department and intelligence community have worked closely and cooperatively on many issues of great importance to national security. DIO is another issue requiring close inter-working, given the importance of the mission and clear need each organization has for the other in this still-new area. However, in fact, the two are divided by definitional gridlocks that are sometimes subtly nuanced, but behind which lie equity and resource stakes considered important by one or both parties. Some progress has been made in these areas, but many important terms and understandings remain unresolved at present.

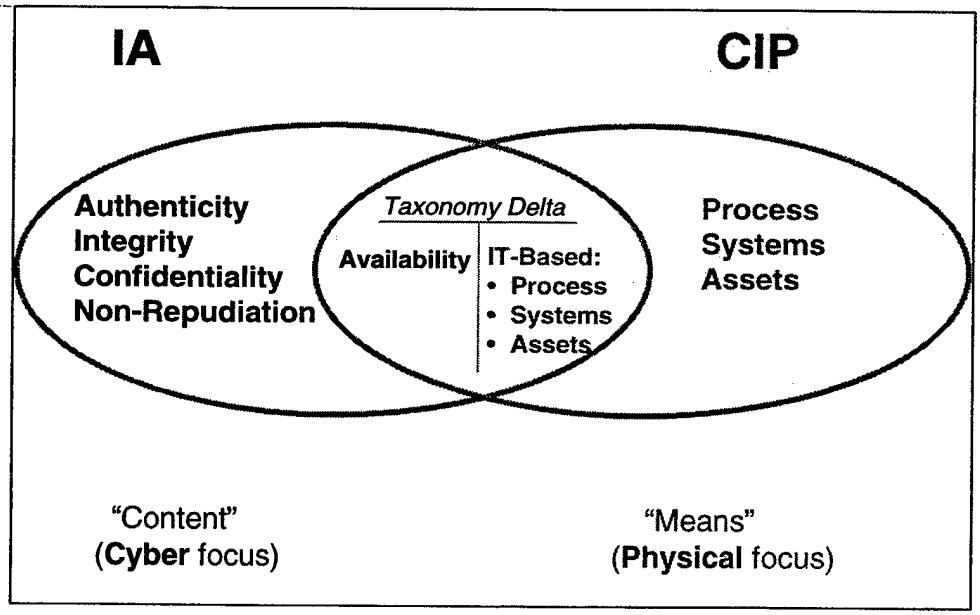


Figure 2 - OSD-Internal Taxonomy Differences: A Case In Point (IA vs. CIP)

At another level, the newness of IO, IA, and CIP within DoD has resulted in tremendous acceleration of the normal evolution of thinking on matters of doctrine, policy, organization, roles and missions, and resource priorities. The frequency with which proposed new approaches to basic definitions and organizational associations have been framed and put forward is matched only by the vehemence of the partisan advocacy for or against any such suggested refinement in

operational procedures or capabilities. If permitted to continue unchecked, the resultant continuous "churning" of the size, shape, and ownership of IO and/or its underlying parts, including IA/CIP/DIO, would significantly handicap broader efforts to inculcate awareness and support for this field within the total force.

Several of the most important aspects of a total DIO management and capability structure are dependent on a relatively stable set of definitions. For example, the goal of providing senior decision makers with the ability to sense, manage and defend "DIO resources" in the aggregate is clearly dependent on a stable understanding of exactly what is included in DIO and what is excluded Reports that have reached the task force that some resource holders have cynically "redefined" IO to include or exclude certain resources on a case basis are particularly disturbing in this regard.

Training is another area very dependent on a clear and common understanding of basic facts regarding definition, doctrine, authority, and thus roles and missions. Trainees – whether executives or entry-level personnel – all require the benefits of a broadly-based, rigorous, and progressive DIO education, training, and awareness program, as discussed elsewhere in this section of the report. All of them must hope that what they learn will remain valid for some useful period of time.

In order to assess policy for DIO, the panel created a matrix identifying public law, executive orders, national security decision directives, and DoD and other issuances. This matrix is found at Appendix C of this Annex. The extent of the matrix supports the panel's finding that policy formulation and thought development in this area has been both recent and intensive. The panel identified some ninety-five (95) policy documents related to this topic, with fully 39% of them having been authored or updated within the past three years.

Source	Total Number	Number Authored or Updated Within 3 Years	Percent Authored or Updated Within 3 Years
Public Law & Executive Branch Issuances	24	3	13
DoD Issuances	50	24	48
Joint, Agency & NSTISSC Issuances	21	10	48
TOTAL	**95**	**37**	**39**

Figure 3 - DIO Policy Assessment

RECOMMENDATIONS:

- Deputy Secretary of Defense (DepSecDef) declare a two-year moratorium, effective immediately, on changes to any IO/IA/CIP definitions reflected in joint documents (DoD DIR 3600.1, JP 3-13, etc.). Services and agencies should use this time to

prepare and publish component-level policy documents as required to implement aspects of policy established at the SecDef/OSD and/or CJCS level.

- Leadership of the Bilateral IO Steering Group (BIOSG) Under Secretary of Defense (Policy)(USD(P) and Director, Intelligence Community Management staff) agree to establish, within one year, common/agreed definitions for IO/IA/CIP terms not now resolved in joint documents.
- BIOSG develop and distribute, at the end of the one-year period of resolution, a common lexicon as an aid to facilitating government-wide IO-related definitional commonality.

Time: To be implemented by October 2001

Estimated cost of implementation: Minimal other than administrative costs.

B. Organizational Roles, Missions, Responsibility Confusion

FINDINGS:

- Roles, missions, and responsibilities of organizations in DIO conflict and frequently overlap (unclear/inconsistent chains of command).
- Concepts of Operations (CONOPS) for DIO mission execution are immature or do not exist.
- Where mission assignments have been made, lack of resources inhibits execution (e.g., USSPACECOM, JPO-STC).

DISCUSSION:

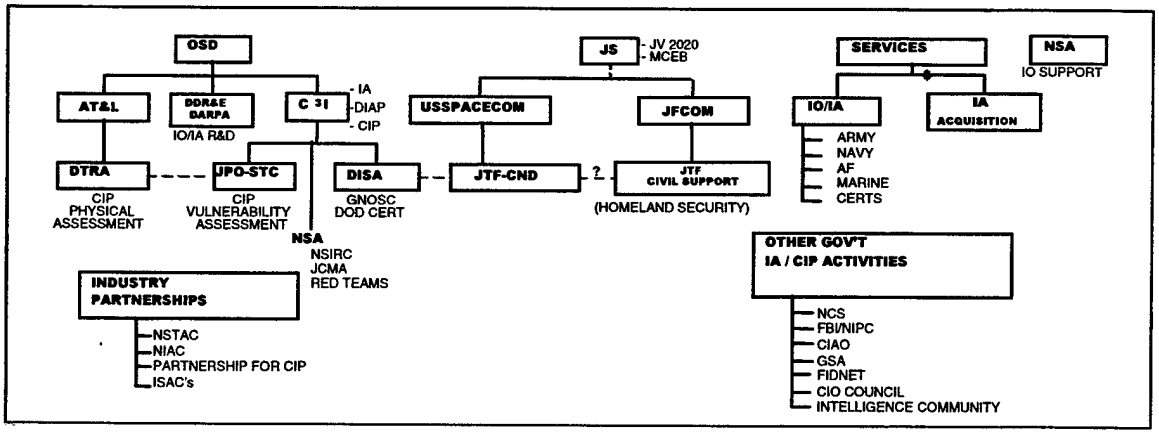


Figure 4 - IO/IA/CIP Organizational Relationships

As the concept of DIO has evolved and matured, concerns have been raised about the appropriate roles, missions, and responsibilities of the CINCs, Services, and Agencies in this

area. Recent-real world events and exercises have illustrated that clarification of who is responsible for what activities in DIO is essential. In response, the DoD established the Joint Task Force-Computer Network Defense (JTF-CND) and its component activities in 1998, along with a number of other activities and commands within the military Services to carry out those operational activities deemed necessary for this new mission area. Unfortunately, none of this activity was accompanied by clear policy on who was supposed to do what. Existing policy does not address this mission area, and extrapolation of existing policy has resulted in inconsistent interpretations of roles, missions, and responsibilities across the DoD, as illustrated in Figure 4, above. The department has conducted a number of studies, front end-assessments, and working groups to clarify the issue, but guidance in this area has fallen behind reality. Additionally, where these new missions have been taken on, funding and manpower have been taken out of hide and are inadequate to accomplish what is required. Even where specific responsibilities have been tasked, inadequate resources have hampered the activities' abilities to accomplish taskings. Specific examples of this lack of funding include the Defense-wide Information Assurance Program (DIAP), the JTF-CND, and the Joint Program Office for Special Technology Countermeasures (JPO-STC). None of the activities listed has been funded or staffed appropriately to accomplish its assigned mission.

Another problem arising out of unclear roles, missions, and responsibilities is the distinction between the entirety of DIO, IA, and CND. DIO, as defined in DoD directives and joint publications, includes all activities within IA and some additional activities. CND is an activity within DIO, but is not IA. The relationships among these activities are illustrated in Figure 5, below.

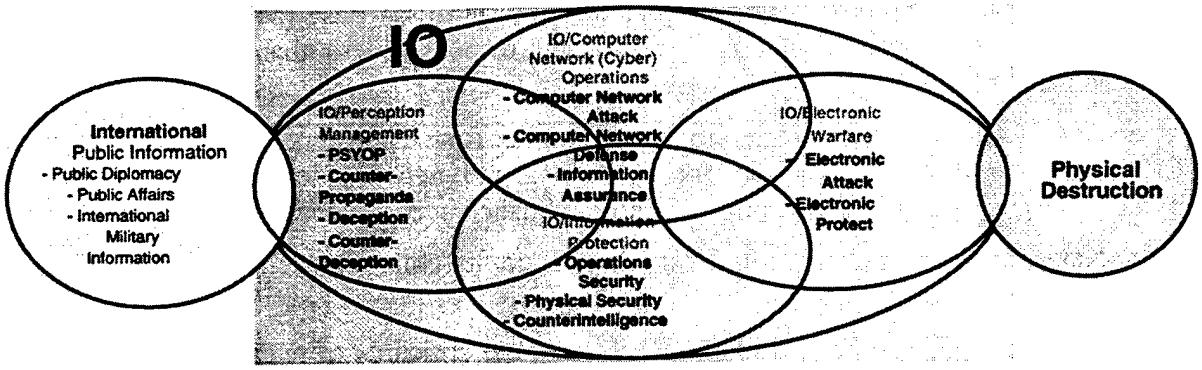


Figure 5 – Information Operations Problem Space

The problem these overlaps in responsibility present is that organizations performing these activities can and do conflict over who is responsible for accomplishing what activity. An example is JTF-CND. Its mission is specifically CND, yet it is not clear what IA responsibilities may or not be included in that mission.

The lack of clarity in roles, missions, and responsibilities has also affected those organizations responsible for carrying out Critical Infrastructure Protection (CIP) activities or homeland defense activities and their relationship to the DIO organizations. Two examples illustrate the problem: (1) the existence of the CIP and DIAP as separate entities within ASD(C3I) and (2) the responsibility of USSPACECOM for Computer Network Defense

Page 1027 of 3957

(CND)(these are titles and should be capitalized) as opposed to the responsibility of USJFCOM for Homeland Defense when there is a computer network attack against the homeland.

RECOMMENDATIONS:

- SecDef and CJCS clearly define roles, missions, and responsibilities of organizations tasked with DIO functions, including clarifying chains of command and relationships with other organizations.
- When tasking organizations to perform these additional functions, resources should be provided, along with priorities of execution of missions.

Time: To be implemented by October 2001

Estimated cost of implementation: Minimal for definitions. Resources for tasking addressed in separate recommendation.

C. Collocation of Network Management and Computer Network Security

FINDINGS: DoD does not universally collocate its Network Operations Centers with information assurance (IA)/computer network defense (CND) activities.

OBSERVATIONS: Significant operations and security synergy is being realized by the collocation of the DISA Global Network Operations and Security Center (GNOSC) and the Joint Task Force for Computer Network Defense (JTF-CND). The United States Marine Corps (USMC) Network Operations Center at Quantico Marine Corps Base (MCB) is an outstanding example of the efficiencies, security control, and responsiveness that can be provided by collocated network management and IA/CND operations.

USSPACECOM's recent efforts to establish the first Theater C4 Coordination Center (TCCC) with similar potential network operations and network security functionality is a convincing case for similar organizations being established at each CINC headquarters.

The Navy, Air Force, Army, and most agencies do not collocate their network management and security operations.

The Joint Staff Vice J6 briefed the DSB stressing the criticality of realizing NETOPS for the actual operations of the Global Information Grid (GIG).

The DSB was not briefed on, nor is aware of, any DoD initiative to establish an alternate JTF-CND location should the current DISA location be unable to support GNOSC/JTF-CND operations.

The DSB is convinced the NETOPS concept proposed as part of the GIG vision has significant merit and should be adopted throughout DoD – specifically, the collocation of network management and IA/computer network defense operations in the same center.

BACKGROUND: The operation of the network, or NETOPS, is the primary means of operating the GIG. NETOPS meets these needs by means of the standardized organizational and operational integration of three functions: network management, information assurance, and information dissemination management (IDM) (these are all usually referred to as titles).

Page 1028 of 3957

Network management provides visibility of extent and intensity of activity, traffic load, and throughput potential. Network management will enable dynamic rerouting based on priority, system status, and capacity. The effects of disruptions and intrusions will be minimized through allocation of traffic to unaffected available network paths. Network management will also allow the rapid reconfiguration of networks in order to isolate an incident (e.g., malicious code) to a specific location.

IA is focused on protecting information and information systems. IA provides the organized, manned, trained, and equipped workforce to guard and secure information and information systems. IA incorporates protection, detection, deterrence, and defense capabilities and processes to shield and preserve information and information systems.

RECOMMENDATIONS:

- CINCs, Services, and Agencies take appropriate action to collocate their Network Operations Centers with their comparable IA/Computer Network Defense operations.
- DISA and JTF-CND, in conjunction with U.S. Commander in Chief Space Command (USCINCSPACE), determine the optimum alternate location for collocated GNOSC and JTF-CND missions should the current DISA location become combat ineffective..

Time: To be implemented by 1 October 2002

Estimated cost of implementation: $10-25M over the FYDP

D. Threat Warning and Attribution, "Indications & Warning"

FINDINGS: Recommended improvements in GIG architecture and security provide a technology baseline to permit creation of a tactical time-sensitive, information-attack, warning sensor grid. Such a network would also support goals of assigning attacker attribution confidently and rapidly. Any plan to achieve this outcome would span the domains of policy, law, technology, and organization, and would require actions in several sectors of government, as well as private industry.

DISCUSSION: The recommended actions to secure the GIG architecture, taken together, have the effect of "raising the bar" of protection for DoD information infrastructures. At the same time, however, the panel acknowledges that at least some attacks will succeed in penetrating the security of the GIG. In all cases, there is a need and value in understanding that someone is trying to penetrate and degrade the GIG, even if the attack is not entirely successful. The ability to rapidly, reliably, and confidently identify, characterize, and attribute information attacks against the GIG – and thus, against the nation – is a major national security requirement in the information age.

The recommendations in this report that are related to technology can all be accomplished within the authority of the Secretary of Defense. However, as noted elsewhere in this report, issues related to timely sharing and use of information-attack data are currently unresolved in policy, as they relate to various equities of the federal government. If the scope of interest is expanded to include the extensive commercial infrastructures upon which critical DoD processes

Page 1029 of 3957

and missions depend, the problem becomes not merely one of policy but also of law, culture, and public sentiment.

If one may presume the availability of timely sensory inputs from GIG-derived sources as a minimum, along with commercial inputs, what remains is to identify the physical and organizational focal point(s) for conduct of an information-attack indications and warning mission, associated personnel requirements, and the chartered authorities and responsibilities those watch-standers would have, including interfaces with larger, classic governmental warning structures.

The I&W Process: Indications and Warning (I&W) is conducted today within a policy framework that assigns roles and responsibilities to a distributed set of organizations throughout the Defense Department and the Intelligence Community.

This structure is well designed to act upon the availability of credible and coherent data, permitting it to "ring the bell," rapidly engaging various authorities to respond as appropriate. However, the problem in the case of information attack is that at present and heretofore, there has been no structured sensory network to reliably provide timely data on which to act.

Precedent may be found in the North American Air (later, Aerospace) Defense Command (NORAD). NORAD is predicated upon an architecture of sensors, reporting links, and analytic nodes, supported by appropriate authorities and focused on a single – but very large, complex, and important – mission: the air defense of the North American continent. The output of the NORAD system is an input into the dissemination architecture displayed and described above.

IMPLEMENTATION: The panel sees the "NORAD model" as a potentially promising approach to information-attack detection, analysis, and warning. Using the upgraded and modified GIG as a sensory baseline, relatively minor modification to the U.S. Space Command's current Computer Network Defense charter and responsibilities would permit identification of an organizational focal point for information-attack threat detection and attack warning within the joint military command structure, feeding the existing NOIWON process as discussed above.

Having established a baseline DoD-internal capability in technology, policy, and organization, the next step will be to expand the information-attack I&W process across the federal government, with the goal a truly national information-protection regime. The information-sharing and trust issues related to this objective are readily acknowledged to be serious and complex, and will have to be addressed [or "treated as such"? treated as such will work] throughout the federal government and across the government-civil interface. The panel immediately acknowledges that the required degree of cooperation is only achievable within a process including extensive discussion and negotiation with private stakeholders; legislative and policy initiative; and continued technological effort, all of which must occur over time. There is cause to be hopeful, however, as the panel has noted the progress being made by such organizations as the National Security Telecommunications Advisory Committee, the Partnership for Critical Infrastructure Security, and other organizations. No specific date targets are established by this panel for the creation of an information-attack I&W regime of national dimensions. However, the requirement is embraced and the vision is put forward, with hope that future study groups and scholars will continue to add specificity and support to this vital initiative in the national interest.

RECOMMENDATIONS:

- SecDef modify the Unified Command Plan as necessary to authorize Commander in Chief, U.S. Space Command (USCINCSPACE) to establish a DoD-wide DIO threat detection and warning capability, using the modified GIG as a technology baseline.
- USCINCSPACE develop the required capability as a feed to the NOIWON system.
- USD (AT&L) commission a Defense Science Board study to specifically address information-attack indications & warning and make detailed recommendations for implementation of such a program.

Time: Initiate implementation by 1 Oct 2002 and reach Full Operational Capability (FOC) by October 2006.

Estimated cost of implementation: $150M over the FYDP.

II. RESOURCES

Despite all of the rhetoric and press coverage associated with the threats to and vulnerabilities associated with critical infrastructures, there is scant evidence that the Department has allocated sufficient resources--dollars, people, and leadership--to defensive information operations. *The Report of the President's Commission on Critical Infrastructure Protection*[5] and the *National Intelligence Estimate on Information Warfare*[6] both highlighted the growing vulnerabilities to our networks and the evidence that both nation-states and transnational groups are aware of the vulnerabilities and are seeking ways to exploit them asymmetrically. No nation on earth, and certainly no transnational group, can match the U.S. military "bomb-for-bomb" and "bullet-for-bullet"; however, several have the capacity, and apparently the intent, to develop capabilities that can affect our ability to plan and conduct military operations and that touch the lives of ordinary Americans in ways that are physically and economically dangerous. The physical sanctuary that the American people and their military have long enjoyed does not exist in the information age.

A. DIO Funding Throughout DoD

FINDING: The Department has not sufficiently funded protection of its networks and DIO programs. Of particular concern is the Sensitive- but-Unclassified (SBU) information critical to JV 2020. For example:

- Exploding SBU network infrastructures are at risk while pressure increases for more interconnectivity between various security domains and public domains.
- Network interconnectivity in and of itself is causing DoD to invest in non-traditional security initiatives to provide information integrity, electronic identification and authentication, non-repudiation, and availability over and above traditionally funded legacy confidentiality (i.e. Communications Security (COMSEC)) programs

---

5 PCCIP Report, Oct 1997.

6 NIE for IW, mmm yyyy.

Page 1031 of 3957

- The Insider threat is largely ignored, raising trust issues with both SBU and classified networks.
- The looming COMSEC modernization bill to replace aging infrastructure will add further strain on commitment to the SBU problem.

DISCUSSION: In 1996, the DSB recommended funding levels to address deficiencies identified in the Department's DIO budget. Since that time, the funding levels for DIO have increased only slightly in relative dollars, but the requirements and the situation regarding DIO have changed significantly.[7] In 1996, funding was primarily for classified systems. Subsequently, the Department has realized that its unclassified systems and networks that process sensitive and mission-critical information require protection, but the requirements in this arena have far outstripped the funding available [pick one] to address the problem. Although it may look to the uninformed observer that funding has increased slightly, the reality is that the problem has grown much more comprehensive in scope and funding has failed to keep up with requirements. The result is unfunded mandates and the robbing of critical long-term programs to pay for immediate short-term concerns.

Exacerbating the situation, the DoD has yet to articulate a clear strategy for funding and implementing DIO. There are documents that describe some pieces of a *strategy (DoD Chief Information Officer Information Technology Management Strategy*[8] and the Global Information Grid[9], but they are incomplete and/or immature and insufficiently detailed to provide a clear picture of the DoD's priorities in this arena. The result of this lack of strategy has been an inconsistent DIO funding profile across the Department, with components making internal decisions about what they can afford regardless of the impact on the overall needs of the DoD. In a shared risk environment, this inconsistent implementation of DIO requirements results in uneven levels of assurance, increasing the risk to all. The lack of an overall strategy, coupled with outdated, incomplete policy, also makes it difficult for the components, and therefore the DoD as an organization, to justify the increased funding levels that they need to address the requirements.

---

7 DIAP PDIT Brief of 14 Jul 2000

8 DoD DIO ITM Strategy, Oct 1999)

9 DoD CIO P&GM No. 6-8510, 16 Jun 2000.

Page 1032 of 3957

RECOMMENDATIONS:

OSD should direct the following actions:

- ASD(C3I): Develop DIO funding strategy and profile, establishing priorities where sufficient funding does not exist.
- Conduct front end assessments (FEA) in February 2001 to shape issues for the summer program reviews (PRG) of the 03-08 POMs:
  - DIO Research & Development (R&D) investment: Under Secretary of Defense for Acquisition, Technology & Logistics (USD (AT&L)) lead,
  - COMSEC Modernization: ASD(C3I) lead,
  - CND investment: USCINCSPACE lead,
  - GIG implementation investment: ASD(C3I), AT&L, J6 co-leads, and
  - Training/personnel investment: USD(P&R), ASD(C3I) co-leads.

Time: To be implemented by 1 October 2001

Estimated cost of implementation: $250K contract support to FEAs

B. Program Element Structure

FINDINGS: The current DoD DIO resource management structure hampers effective oversight and executive review.

DISCUSSION: Numerous efforts over the years have attempted to capture, categorize, and manage DIO resources with little success. In the past, DoD captured the bulk of the costs associated with protecting IT resources within its Information Systems Security Program (ISSP). While this program accounted for the bulk of the Department's information security investment, the program does not cover the following information security costs:

- Costs embedded within acquisition programs/initiatives
- Intelligence Community (IC) costs
- Costs within the operating support funds for base/camp/post/stations
- DoD law enforcement (cyber-crime activities) costs
- DARPA information security research programs
- The information security programs of those Agencies not part of the ISSP program (all agencies other than NSA and DISA)

The Defense-wide Information Assurance Program (DIAP) was tasked with the responsibility to provide "oversight, coordination, and integration of the Department's IA resource programs."[10] The DIAP has spent the three years since its inception trying to

[10] OASD(C3I) Memo, 12 Feb 1999.

Page 1033 of 3957

understand what is and is not included in the ISSP, where additional DIO expenditures within the Department may exist, and how to gain sufficient visibility into these expenditures. The objectives of these efforts have been to understand the scope of the DIO funding and where deficiencies may exist, to provide DoD leadership with the ability to make informed decisions concerning funding. A briefing was given to the DSB DIO Task Force that presented the results of that work (Annex E). It was apparent however, that visibility into DoD components' budgets to determine IA expenditures is still incomplete and the current PE structure does little to correct the problem. The panel's conclusion is that without a Program Element (PE) structure, the ability to accomplish effective management of the DoD's funding resources for DIO will continued to be hampered by lack of visibility.

There are, however, potential negative repercussions that could result from this PE structure and the resulting increase in visibility. The most significant of these repercussions is that DoD components may continue to "hide" DIO expenditures in other funding lines to ensure that they retain flexibility to reallocate internally as conditions dictate. Ensuring that the components retain overall control of their funds, with the understanding that they may receive tasking requirements that they will have to fund somehow, may reduce this activity. Additionally, DoD leadership should refrain from taxing the components' DIO resources during the next Future Year Defense Plan (FYDP) while this key information superiority area is undergoing critical and extensive change. In return, the components need to be honest about the risk management decisions they have made about what to fund and what not to fund and where shortfalls may exist. With that information, DoD has a better chance of justifying additional resources where shortfalls exist.

In addition to establishing a PE structure, DoD needs to ensure that DIO requirements, where appropriate, are vetted and approved through the formal requirements processes. The absence of this step has resulted in unclear priorities on programs and funding, leaving the components to make arbitrary decisions about what they can afford to fund. By vetting through the formal requirements processes, the DIO requirements are both documented and justified, allowing the CINCs who have a major role to play in the actual execution of the DIO mission to have a voice in funding priorities that they currently do not have. Additionally, once the requirements are formally documented, components responsible for funding can be held accountable for decisions made contrary to that requirement – something that is impossible to do under the current situation.

RECOMMENDATIONS:

Director, Program Analysis and Evaluation(PA&E), in concert with ASD(C3I), should effect the following:

- Establish a program element (PE) structure for all DIO resources
- Require mandatory migration of all DoD DIO resources into new PE structure
- Address DIO requirements in the JROC (CINC/Service participation)
- Establish program funding support for DIO requirements

Time: To be implemented by 1 October 2002

Page 1034 of 3957

***Estimated cost of implementation*:** Total IA budget for DoD should be around $3B/year, an increase of about $1.4B over the current documented funding.

III. PERSONNEL

A. Find and Keep the IT Talent

FINDINGS: The DoD shortage of IT professionals is serious and growing.

DISCUSSION: The complexities of solving the DoD shortage of IT professionals, when viewed in the larger context of the private sector, are serious. Shortages in the supply of IT professionals are not confined to the DoD – they exist for other federal agencies, nationally and globally. More than one million information technology jobs are vacant around the world and the number is likely to increase. By 2002, there will be 850,000 vacancies in the United States and more than one million in Europe.

Recruiting is difficult when colleges and universities are only producing enough IT graduates to fill half of the growing annual requirement. Several U.S. companies have begun recruiting foreign nationals to fill their IT jobs. Under the H-1B non-immigrant category of U.S. immigration law, U.S. employers may sponsor 65,000 professional foreign nationals each year. to The turnover rate among IT professionals in the private sector is 30%, five times the rate for the private sector as a whole. The private sector is, therefore, providing a number of incentives to combat these shortages.

The Department's ability to compete with the private sector in the area of compensation is limited by personnel practices and guidelines, and by law, in the case of military personnel. The private sector is able to react quickly to any substantive compensation change made in the government, making it difficult to maintain comparability in pay and benefits.], There are a few government authorities that offer limited relief.

The Office of Personnel Management (OPM) authorized specific flexibilities for civilian personnel to help address the government-wide recruiting and retention problems facing managers.[11] A recent Integrated Process Team (IPT) within DoD revealed that few of these flexibilities are being used within the Department.[12] Many reasons can be given for this situation, including an unwillingness to differentiate between civilian employees on different types of pay scales, but the most significant reason is lack of funding. As the DoD has sought to reduce its size, the funding for personnel and personnel incentives has also suffered. Instead of targeting reductions to functions that are no longer needed, most activities have taken percentage reductions across the board, exacerbating shortages for key skills.

On the military side, the Services have recognized the need for key IT skills and have begun targeting recruiting and retention bonuses to encourage individuals to remain on active duty. Although these bonuses cannot compare with those offered by the civilian community, they are a tacit recognition of the pay discrepancies. Additionally, other incentives, such as choice-of-duty assignments and DoD schools are used to entice military personnel to remain.

---

11 "OPM Report, Nov 1998.

12 *IA/IT HR IPT Report*, 27 Aug 1999.

Page 1035 of 3957

Even with adequate incentives, there will be insufficient personnel with specific technical skills available for DoD. This means that a realistic approach to solving the problem must consider outsourcing as an alternative. This approach was explored in some detail by a separate Defense Science Board Task Force on Human Resources Strategy. This DSB recommended pursuing military and DoD civilian tasks only on those tasks essential to the business of governing. All others should be addressed by the private sector for those functions it does best.[13] This alternative, however, should not be seen as a way to save money, but instead as a method to augment and acquire key IT skills. A Government Accounting Office (GAO) report of August 2000 reports that there are some savings associated with outsourcing, but the documentation of such savings is inadequate.[14] Unfortunately, in the rush to outsource, little thought has been given to careful planning of what should and should not be outsourced. This planning requires a clear statement of "Inherently Governmental" that is understood and executed in a consistent way. . Although there is a policy document that describes "Inherently Govermental," the applicability to the IT arena is not clear.[15] There is a current effort to provide this clarification with an Integrated Process Team (IPT) consisting of USD(P&R), USD(AT&L), and ASD(C3I) membership. With this clarification, DoD should develop an outsourcing strategy for key IT skill sets that complement those available from DoD civilian and military personnel.

Other, more creative alternatives should also be considered. It is a well-established fact that IT personnel move around more frequently in their jobs than those in other skill areas. This fact can be a problem for encouraging individuals to take on government service if one expects that the choice is a full career choice. If it is accepted that these frequent moves are part of a valid career choice, then alternative employment programs should be encouraged that facilitate this fluid work force. One alternative may be an "Education and Training for Service (ETS)" model that requires a minimum payback of employment for education. This program could provide dual benefits in encouraging more students to consider an IT career, as well as providing education incentives with a promise of employment. It could also provide a constant refreshment of talent in a constantly changing IT environment.

RECOMMENDATIONS:

- SecDef direct more aggressive recruitment, retention, and proficiency pay for critical DIO skills (authorities exist to do this)
- ASD(C3I), in coordination with USD(P&R), develop formal career paths for DIO officer, enlisted, and civilian personnel
- Develop an outsource strategy to complement DoD key DIO resource needs
- Develop an Education and Training for Service (ETS) model – 3-5 years tenure

Time: To be established by 1 October 2001

Estimated cost of implementation: $25M per year

---

13 Defense Science Board Report, Feb 2000, p. vii.

14 GAO/NSIAD-00-107, Aug 2000.

15 OFPP Policy Letter 92-1, 23 Sep 2000.

B. Sensitize and Train Users

FINDINGS: The DoD workforce at all levels is ill-prepared to execute the DIO mission because current training efforts are fragmented, inadequately scoped, and poorly documented

DISCUSSION: The attacks against the DoD's information infrastructure have heightened awareness of the importance of training in protecting the department's information resources against attacks. Because of the shared risk environment created by highly connected and interdependent information systems, all individuals using, administering, maintaining, and managing systems and networks must understand the threats and the policies, procedures, and equipment designed to mitigate these threats. A training continuum (from cradle to grave, from the lowest civilian and military to the highest) must ensure that all personnel understand the threat and their role in protecting DoD's networks. An analogous program that can provide insight into how training affects successful mission performance is the DoD safety program, particularly aviation safety.

Training for all users of DoD computer systems is mandated by statute,[16] with additional guidance provided by Office of Personnel Management (OPM) regulation,[17] Office of Management & Budget (OMB) circular,[18] and DoD directive.[19] In spite of this direction, user training was unevenly implemented, requiring issuance of additional guidance by ASD(C3I) and USD(P&R) in 1998.[20] This policy memo also levied an initial requirement for system administrator and maintainer training and certification. Outside of user training the level and content of training for other personnel with DIO responsibilities (i.e. systems administrators, auditors, accreditors etc) in the Department varies. In some areas there are comprehensive training programs available for all DoD personnel. Unfortunately, the Department does not take full advantage of these programs. In other cases, training has been either unavailable or too expensive for the IA workforce. As a result, the level of training for the DoD IT/IA workforce is uneven at best. The training content also varies across the Department, which is a potentially serious threat to the Department's joint warfighting capability. The previously mentioned policy did not address this issue, nor did it address training for personnel performing other IA functions, or establish a permanent, recurring requirement for those identified functions. That task was taken on by an IPT established in September 1998 by ASD(C3I) and USD(P&R).[21] This IPT produced a report that made a series of recommendations to begin establishing permanent training and certification requirements for critical IA functions.[22] The report resulted in a recently signed DepSecDef policy memo.[23]

The Department has made great strides in developing and implementing a DIO training continuum, but much work remains to be done. As the training requirements are developed, they need to not only incorporate the emerging OPM civilian personnel standards and be validated

---

16 Public Law 100-235, ***1987.***

17 OPM Regulation 5CFR930.301-305, 3 Jan 1992.

18 OMB Circular A-130, 8 Feb 1996.

19 DODD 5200.28, 21 Mar 1988.

20 OSD Memo, 29 Jun 1998.

21 DepSecDef Memo, 14 Jul 2000.

22 ***IA/IT HR IPT Report***, 27 Aug 99.

23 DepSecDef Memo, 14 Jul 2000.

Page 1037 of 3957

against commercial/private sector standards (where those exist), but also included in the formal training mechanisms of the Department. Without this formalizing of the requirements into the normal training mechanisms, they will not become institutionalized into how the Department does business. Additionally, it makes little sense to require military and DoD civilians to be trained to a standardized requirement if contractors performing the same functions are not held to those same standards. The recent CIO GIG Guidance & Policy Memo (G&PM) establishes the initial requirement for these training standards.[24] Realizing that [this] may require modification to existing contracts, contracting officers need to ensure that any new contracts or modifications to existing contracts providing DIO services/functions contain standardized requirements and performance metrics to hold contractors accountable for meeting these requirements.

RECOMMENDATIONS:

SecDef (ASD(C3I) & USD(P&R), USD(AT&L)) should:

- Establish policy to develop and implement formal education training and awareness (ETA) programs for DIO throughout DoD to do the following:
    - Codify the DIO training program within the formal DoD Joint Training System (JTS)
    - Ensure DIO programs are consistent with commercial and DoD certification standards
    - Require contractor personnel performing outsourced DIO functions to meet ETA criteria required for government employees

***Time*:** To be implemented by 1 Oct 2001

***Estimated cost of implementation*:** $150M over the FYDP

C. Know Your Insiders

FINDINGS:

- Insiders are our first line of defense and the most dangerous cyber threat
- Systems administrators have the "keys to the kingdom," yet often require no special "reliability" investigations, such as those in the Personnel Reliability Program

DISCUSSION: The Insider Threat is one that has long been recognized as having the potential to cause the most damage to systems as compared to damage caused by outside attackers– both inside the government and in the private sector. An insider is identified as anyone who "is or has been authorized access to a DoD information system, whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector."[25] An insider has the

---

[24] DoD CIO P&GM *No. 6-8510,* 16 Jun 2000.

[25] Department of Defense, "DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team". 24 April 2000, p.3

Page 1038 of 3957

capability to disrupt interconnected DoD information systems, to deny the use of information systems and data to other insiders, and to remove, alter, or destroy information. Documentation of this recognition exists in many fora – including a number of DoD documents that discuss the issue and make recommendations on how to mitigate the risk of the insider. The most comprehensive of these is a recently released report listing the recommendations of the Insider Threat Integrated Process Team, chartered by ASD/C3I.[26] This report identifies the basic sources of insider security problems as (1) maliciousness, (2) disdain of security practices, (3) carelessness, and (4) ignorance of security policy, security practices, and proper information system use. The key elements of a strategy to minimize the impact of the insider threat are:

- Establish criticality of systems
- Establish trustworthiness
- Strengthen personnel security and management practices
- Protect information assets
- Detect problems
- React and respond

The report goes on to make a total of 59 recommendations in 7 areas, which, if adopted, will significantly improve the ability of DoD to mitigate the insider threat risk.

A separate report addressing training and certification issues for critical IA functions also makes recommendations to mitigate the insider threat for personnel performing critical IA functions.[27] This report specifies that personnel performing critical IA functions – defined as those that require the individual to have privileged access to networks and operating systems – require special attention to ensure that they can be trusted. These critical IA personnel include systems administrators who have the most ability and access to both protect and damage DoD networks. A third report, issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), also addresses the insider threat,[28] as does a 1997 DoD IG report.[29]

There are many ways to address the problem, but all require knowledge of who the critical personnel are, and what the critical processes and systems are. The Y2K effort provides a model of how to distinguish between critical and non-critical systems and processes. The results of this discrimination process can provide a mechanism to focus attention and constrained resources on those systems and processes that are most critical to the Department. However, there is as yet no mechanism to identify critical personnel, although the recommendations by the Information Assurance/Information Technology Human Resources Integrated Process Team (IA/IT HR IPT) begin to accomplish that objective. These recommendations were recently approved by

---

26 ***Insider Threat IPT Final Report, 24 April 2000.***

27 ***IA/IT HR IPT Report***, 27 Aug 1999.

28 ***NSTISSC Report***, Feb 2001(draft).

29 DoD Office of the Inspector General, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," Report PO 97-049, 25 September 1997

DepSecDef; however, it will take several years just to identify who are systems administrators.[30] This step is absolutely essential because systems administrators are the most critical of all those who perform IA functions. Systems administrators can be military personnel who are performing this function in a full-time or part-time capacity, DoD civilian personnel (also full-time or part-time), or contractor personnel performing functions, which have been outsourced. Regardless of their status, all individuals performing these functions must be held to a consistent–and high--standard.

It is not enough, however, to ensure that those performing critical functions are trustworthy, because the most rigorous screening may still miss identifying a potential problem insider. Screening also does not prevent someone who had no intention of misusing the system initially from doing so at a later date. Therefore, monitoring of both personnel and systems must be done to detect those who are not using the system as intended. Such observation requires establishment of a clear, legal, and enforceable monitoring policy so that all personnel using the systems are aware that their activities will be monitored. This policy can also act as a deterrent to anyone who may contemplate unauthorized activity and aid in holding those accountable who violate the policy. The Department has a monitoring policy, but it needs revision to accomplish the objectives stated. The technical means to monitor are available, but require proper configuration and deployment within the network architecture.

Access control processes and mechanisms are also required to prevent individuals from unauthorized access to information and processes. Passwords can provide some measure of control, but require a management process to ensure they are regularly changed. Furthermore, the files need to be protected from disclosure and users need to be aware of their responsibility in protecting passwords. Passwords have their flaws; other access control mechanisms should be employed, such as PKI and biometrics. The DoD PKI program[31] will address many of the issues presented by access control, and the DSB DIO Task Force applauds this effort. However, deployment could be jeopardized by insufficient funding and lack of follow-up in the enabling of applications for PKI.[32] The biometrics program, with the Department of the Army as the executive agent,[33] also shows promise in addressing this issue, but inadequate funding could also jeopardize this program.

The Insider Threat is, therefore, well–documented, and numerous recommendations and programs in several fora exist that, if implemented, would significantly reduce the impact of this threat. However, a number of the recommendations have yet to be implemented. The reasons for this situation vary, but lack of resources and difficulty in developing appropriate policy appear to be the primary factors. This DSB recognizes that the Department has acknowledged the problem, but the lack of policy and resources to address a very real and growing problem is of concern.

---

30 DepSecDef Memo, 14 Jul 2000.

31 ASD(C3I) Memo, 12 Aug 2000.

32 OASD(C3I) DIAP Report Apr 2000.

33 National Security Act, 1947.

RECOMMENDATIONS:

- ASD/C3I identify those IT personnel who are critical for DIO activities
- DepSecDef mandate the following processes and procedures:
  - System administrator auditing software
  - Open-source, commercial-style background investigations
  - Peer accountability
  - Pre-employment agreements
  - Credit checks
  - Standardized procedures for access to and control of systems
  - Two-person integrity (TPI) for specific critical functions that must be accomplished on a network/system
  - Policy for system monitoring and reporting of improper/unauthorized actions
  - Contractor personnel standards identical to those established for DoD personnel in similar positions

Time: To be implemented by 1 Oct 2001

Estimated cost of implementation: $5Mper year

D. Reserve Component

FINDING: Significant personnel resource shortfalls affect execution of the DIO mission at all levels in DoD.

The *Reserve Component Study* of February 2000 was chartered to provide recommendations to the ASD(C3I) on the subject of expanding the role of the Reserve Component (RC) in domestic preparedness in two specific areas of defensive information operations: information assurance and computer network defense. The study made two recommendations: 1) bolster RC support for USSPACECOM and JTF-CND, and for the Services by strengthening the RC support to the Service component commands (Land Information Warfare Activity (LIWA), Fleet Information Warfare Command (FIWC) and Air Force Information Warfare Command (AFIWC) and 2) establish Service Joint RC Virtual IA/CND units.[34]

Virtual RC support to LIWA, FIWC, and AFWIC can provide several advantages. The increase in virtual manning could result in improved mission accomplishment and extended "normal business hours" coverage (the United States' Reserve Components in states encompass six time zones from the east coast to Hawaii); an increase in Service component commands' talent pool (RC members with high technology skills can be reassigned or recruited to perform inactive duty training near home); development of a skilled pool to man the Service component

[34] ASD(RA) Study, Feb 2000.

Page 1041 of 3957

commands during annual training periods of the virtual JWRAC virtual reservists and guardsmen; and an increase in Service component commands' mobilization base. Using the RC in these ways would require little or no addition of on-site staff or facilities. Issues that must be addressed include how to identify reservists with the right skills; the management challenge of virtual drilling; and possible Service reluctance to depend on the RC for full-time support.

Increased RC support to the Service component commands would leverage the expertise of skilled reservists with civilian-acquired skills, capable of conducting virtual operations in support of service missions. The virtual augmentation could perform portions of the service missions that are not completed due to real-world mission pressure or could augment staff during weekends and during summer months.

In addition to the *Reserve Component Study*, there were recommendations made in the *Defense Science Board Task Force on Human Resources Strategy* published February 2000.[35] The task force identified a number of priority areas for shaping both the civilian and military workforce, including the Reserve Component: 1) moving to a seamless integration of active and reserve components with a single, integrated personnel and logistics system, and 2) constituting a task force to study and develop a plan that will merge, over time, the Army and Air Force reserve units with their respective National Guards. The report asserts that the transformation is necessary to prevent the personnel problem from worsening.

According to the report, the benefits of integrating these forces include:

- An organization that supports the way the Department operates and deploys
- A more simplified relationship between the active and reserve components
- Reduced overhead from the separate administrative and support structures that exist today
- Stronger ties with U.S. communities

Although the Services have made significant progress towards the goal of full integration, now is the time to leverage that progress by eliminating the separate personnel and logistics structures under which the Reserve Component now operates. Further improvement in the presentation of forces could be achieved by the integration of the reserve force with the National Guard force. This consolidation would require vision and persistence in the face of political pressures, and the challenge would have to be taken up by both the Administration and the Congress.

The DoD increasingly relies on its reserve component to fulfill its mission, both from a resources and skills available standpoint. However, because the two systems remain separate, management of the joint configuration must be relearned each time the reserve component deploys. The report identifies several issues that will have to be addressed to make the integration a reality, including legal, psychological, and administrative hurdles that must be overcome. The report sums it up this way:

> *The Department should move to a more seamless integration of active and reserve components with a single, integrated personnel and logistics*

[35] DSB Report, Feb 2000.

Page 1042 of 3957

system. The task force recommends that the Secretary of Defense constitute a special task force to make specific recommendations to move toward a single reserve component for the Army and Air Force. However, the task force emphasizes that the move to a more seamless military force should not be delayed awaiting the integration of the reserve components, but should be undertaken as a high priority project under the current active duty and reserve organization.[36]

RECOMMENDATION:

The Deputy Secretary of Defense should direct USD(P&R) and ASD(C3I) to implement

- *Reserve Component Study* recommendations and
- *Defense Science Board Task Force on Human Resources Strategy* recommendations.

Time: To be implemented by 1 October 2001

Estimated cost of implementation:

- For Reserve Component Study: $10.5M over the FYDP
- For Human Resources Strategy DSB: as determined by the study, applicable to IT workforce.

IV. OPERATIONAL READINESS

A. DIO Integration into Mission Planning & Execution

FINDINGS: DIO is not adequately integrated into mission planning and execution.

DISCUSSION:

- Control conflicts exist between operational and support equities when services are disrupted.
- Network discipline and CND compliance are issues of concern (e.g.,training, standard operating procedures (SOPs), command emphasis).
- Issue of what Components should support the U.S. Space Command's CND mission is still under discussion.
- CINCSPACE should develop a Continuity of Operations Plan (COOP) should JTF-CND lose capabilities.
- It has not yet been determined what CND information should be posted on DOD Global Command and Control System's (GCCS) Common Operational Picture (COP).
- It is not clear what the U.S. Space Command should protect as part of its CND mission beyond the SIPRNET and NIPRNET.

---

[36] Ibid., p. 52.

Page 1043 of 3957

Integrating DIO into all phases of operational exercises, testing and evaluation, and operational assessments will better ensure that network systems fully consider DIO from design through acquisition and to integration and employment. Implementing DIO into training and plans will ensure that operational plans consider the assuredness of the information they are depending on, and that networks and network personnel are exercised and stressed to better respond when failures and attacks do occur. Planning and exercising for network attacks better prepares the on-scene commanders and operators to respond to attacks or failures in a measured and appropriate manner. Accordingly, as part of exercises and operational plans, developing a set of responses, or delineating the rules of engagement for responding, will ensure any response is appropriate, measured, and authorized.

RECOMMENDATIONS:

- The SecDef, through CJCS, should issue guidance to make DIO a key element of all military planning and operations, to include promulgating Rules of Engagement (ROE) and continuity-of-operations plans and conducting unit training and exercises.

Time: To be implemented by 1 October 2001.

Estimated cost of implementation: Approximately $500k for initial actions. Additional funding requirements will need to be identified and submitted for funding via the PPBS process.

B. Readiness Assessments, Reporting, and Metrics

FINDINGS: There is no adequate system for assessing DIO readiness across DoD.

DISCUSSION:

- Readiness assessment mechanisms are incomplete and fragmented.
- Numerous efforts are ongoing to measure IA/CND/DIO readiness of DoD activities (e.g., CJCSI 6510.04 and DIAP IA metrics efforts).
- CJCSI 6510.04 does not address or apply to all DoD agencies.
- DoD IA readiness includes assessing, evaluating, and enhancing the readiness posture of DoD IA capabilities.

The success of operational missions is now more than ever dependent on the assured and timely delivery of information from operational commanders to operating forces. Planning for, testing, exercising, protecting, and resourcing the assuredness of those systems that deliver that vital information has not kept pace with the emphasis placed on using the information in some operational manner. Yet, assuring the security and availability of information is critical to DoD's success in peace and war, and is a key element of achieving information superiority. DIO readiness must be measured, assessed, evaluated, and understood for operational commanders to understand and achieve information superiority.

The DoD's information systems have been, and will continue to be, under attack. When disruptions occur to the flow of information, either through attack or system failure, operations suffer.

- System failures are often unpredictable and unavoidable. Network operations reconstitution after a system failure depends on the skill, experience, training, and ability of network technicians.
- System attacks are also often unpredictable and unavoidable. Responses and network reconstitution to network attacks also vary depending on system administrator skill, experience, training, and ability.
- Disabling a network as a response to the threat of attack has the same effect as a successful attack.
- The ability of any given command to better face the challenge of a system failure or attack is improved through planning, training, assessment, and practice.

Policy needs to be established which will lead to a structured, mandated, and recurring DIO assessment capability across all elements of the Global Information Grid. An effective DIO readiness reporting mechanism, accompanied by a viable response mechanism to provide proactive and responsive solutions, is as important as anticipating ammunition shortfalls and assessing more traditional critical warfighting systems, and will in the end save money and conserve other resources. Many different organizations, elements, and activities must be brought together within the DIO readiness system to achieve synergy, efficiency, and effectiveness throughout all facets of the system.

Critical success indicators for the readiness system include the people, operations, training, equipment, infrastructure, and processes that characterize the DIO readiness posture of the DoD described as follows:

- People: The ability to attract and retain qualified, cleared, available, accountable, and motivated personnel to sufficiently staff DIO-related mission requirements
- Operations: The ability of CINCs/Services/Agencies to ensure organizations, procedures, and tools are effectively synchronized to execute DIO actions in order to defend information capabilities; thus providing timely, reliable, integrated, and secure information to achieve mission objectives
- Training: The ability to specify and then satisfy DIO training requirements across the DoD by external and internal education, training, and awareness programs that meet nationally and/or internationally recognized quality and curriculum criteria and that generate qualified and certified DoD DIO work force and users.
- Equipment and Infrastructure: The ability of the DoD's defense-in-depth architecture to ensure authenticated and authorized access to information across service and mission boundaries, throughout all applicable equipment and infrastructures (cyber and physical), and with adequate levels of confidence in information availability, confidentiality, and integrity while being processed, stored, or in transit
- Processes: The ability of the DoD to institutionalize across the Department measurable, repeatable, reliable, valid, cost-effective, streamlined, consistently applied, and well-documented DIO processes

Page 1045 of 3957

RECOMMENDATIONS:

SecDef, through CJCS, should:

- Promulgate guidance in the Joint Mission Readiness Review (JMRR) and other appropriate Service readiness reporting systems.
- Specify policies to hold commanders accountable for aspects of DIO readiness within their control.

Time: Initial actions by June 2001, with completion not later than June 2002.

Estimated cost of completion: $12.5M over FYDP

C. Operational Readiness Assessment (Red Teams)

FINDINGS: Due to lack of clear policy and resources, aggressive, comprehensive, effective operational Red Team activities are lacking across DoD.

DISCUSSION:

- Operational readiness assessment involves the Cyber Operations Readiness Triad (CORT): vulnerability assessments, vulnerability evaluations, and red teaming.
- Vulnerability assessments, vulnerability evaluations, and an aggressive, no-notice red-teaming program are lacking across DoD.
- Red-teaming that is being done is inadequately funded, insufficiently staffed, poorly coordinated, and hampered by lack of clear policy.
- Formal Computer Network Attack (CNA) red-teaming efforts, definition, and authorities have yet to be defined.

The purpose of an operational readiness assessment (ORA) is to examine and test an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

The ability of a network system to survive a focused attack and continue to provide the information needed by operational commanders in a timely manner is intrinsically part of information superiority. The ability of any particular system to survive an attack can be attributed to the technical health of the system and the skill, experience, training, and ability of the system technicians. Due to the networked nature of the Global Information Grid (GIG), a weakness within any particular system may cause a vulnerability within the network as a whole.

Evaluating network technical health through testing for system upgrades and patches, proper password management procedures, and firewall standards - just to name a few methods- is necessary to ensure administrators have maintained their systems according to manufacturer updates and established procedures. Similarly, system administrators must be trained and

Page 1046 of 3957

exercised in recognizing and responding to unauthorized attacks and intrusions, from both within and without of the system. Training and assistance teams provide a vulnerability assessment of networks and help provide the local system administrators with the skills they need to maintain system operations.

The different equipment and software that make up information systems have known and unknown vulnerabilities associated with them. Timely installation and maintenance of manufacturer upgrades and patches for known vulnerabilities helps maintain a higher level of security and assuredness, but often comes after vulnerabilities have been widely known and exploited. This may put operations at risk if the military community does not aggressively test, appraise, and evaluate the hardware and software that makes up the information systems. Evaluations of hardware and software identify vulnerabilities not widely known within the public domain and permit the military to work with developers to correct the vulnerability before hackers can exploit it. This level of evaluation, however, is best done during Research Development Test and Evaluation (RDT&E) and Operational Test and Evaluation (OT&E) so that the best network systems can be acquired that meet the overall DoD information superiority objectives.

Actual readiness of in-place information systems can be measured only through the aggressive testing of a system by an independent (red) team. Red team assessments are conducted throughout the DoD, but often with inadequate resources and limitations placed on their ability to conduct an aggressive assessment. Additionally, red teams are being applied unevenly throughout DoD, which results in some commands being highly effective in thwarting network attacks while others may only have minimal capability in doing so. Also, different red teams evaluate systems using different standards and measures of effectiveness, which may lead to a false sense of security within certain commands. Since a potential aggressor seeks out the most vulnerable system to penetrate or attack to achieve his ends, this uneven approach to red teams may lead to an unrealistic sense of security when in fact, little exists.

It is important for doctrine to be developed that would guide the CORT process to ensure all of DoD is at the same level of DIO readiness. Specifically, red-team structures, authorities, responsibilities, and functions should be specified for all DoD activities, and organized in a manner to make maximum synergistic use of the teams and in-place assets. Accordingly, Operational Readiness Assessment Teams should be aligned for each of the military departments, Defense Threat Reduction Agency (DTRA) for weapons of mass destruction (WMD) purposes, NSA for DoD and national requirements, and Joint Forces Command to organize reserve forces for appropriate missions.

Operational readiness assessments should be conducted often and randomly because any introduction of a new equipment or software upgrade changes the design, and hence the vulnerabilities, of the system. Highest priority should be given to upper echelon command-and-control systems, highly classified systems, and the systems of those forces preparing for operational deployment. But each system within DoD should receive complete CORT assistance not less than every five years.

Because of the nature of networked systems, and DoD's reliance on contractors and vendors, policy should be extended to subject those contractors and vendors who are involved in applicable DoD activities to the same red-teaming standards as DoD.

Page 1047 of 3957

RECOMMENDATIONS:

Formalize and empower DIO Red Teaming throughout the DoD by:

- Developing a three-level CORT assessment capability:
  - Level I: Vulnerability Assessment (VA)
  - Level II: Vulnerability Evaluation (VE)
  - Level III: DIO Red-Team
- Establishing policy that defines authorities and responsibilities
- Expanding the number, scope, and frequency of Red Teams to include:
  - Once every 3 years for specified LAN-WAN elements
  - As soon as possible after major system/network changes
  - Prior to all force deployments
  - Not less than once every 5 years for all systems and networks
  - That include contractors/vendors to the extent it applies to those government activities
- Providing adequate staffing and resources to accomplish expanded mission
- Reinvigorating and updating draft DoDD 3600.3 to include the CORT process
- Designating NSA as the DoD element responsible for developing tools, tactics, techniques, procedures (TTP), standards, and training to operationalize ORA
- Resourcing NSA to expand its ORA team to meet mission need

Time: 1 October 2001

Estimated cost of implementation: $30M per year.

D. Computer Emergency Response Teams / Computer Incident Response Teams (CERT/CIRT)

FINDINGS: DoD CERT/CIRT activities vary in their execution and are not inclusive of all DoD CINCs/Services/Agencies (C/S/A).

DISCUSSION:

- Not all Defense agencies have or have access to CERT-/CIRT-like services for their enterprises.
- An overall DIO readiness posture cannot be clearly understood today.
- Tools, response procedures, and reports differ among CERT/CIRTs.
- Doctrine is inconsistent.

Page 1048 of 3957

CERT/CIRTs provide initial indication of external attack against DoD network systems by using automated monitoring tools to determine when unauthorized probes, scans, intrusions, and service denials occur. The information provided by the CERT/CIRTs permits a clearer understanding of the level, severity, and scope of network attack. This information is also used to alert other DoD network users of attack, and to permit counter measures to be implemented which would mitigate the attack. The sum of all this information is a significant indicator of the readiness and ability of information systems to achieve information superiority.

Today, the various CERT/CIRTs use different tools to monitor network activity and, when suspicious activity is noted, report the information using differing methods and procedures. Further, the tools the CERT/CIRTs use are based on identifying recognizable and known network security vulnerabilities, and are not easily configured to protect against emerging or changing technological threats. These differences and shortcomings mean inequities exist when CERT/CIRTs measure and assess network health, which leads to inefficiencies throughout the system or a false sense of assuredness. For the assessments to be valuable, it is important that they be derived from measurements that are accurate and timely, and able to be dynamically updated to identify and warn against the most up-to-date threats. Additionally, to be easily accessed and understood throughout DoD, the assessments need to have a common format and reporting guidelines.

Because of the nature of their mission, technicians at CERT/CIRTs are particularly adept at understanding and mitigating network vulnerabilities. Therefore, CERT/CIRT technicians provide a critical technical capability and expertise for other commands to draw from when needed, especially in preparation for or during operational employment. However, the current number of CERT/CIRTs and the number of technicians within the CERT/CIRTs, do not adequately meet all the assessment and on-site assistance needs of all CINCs/services/agencies.

RECOMMENDATIONS:

USSPACECOM, supported by OSD/JCS policy and procedure, should improve the DoD CERT structure and scope by:

- Developing doctrine/TTPs on emergency response, including a deployment policy when necessary
- Implementing CERT/CIRT clearinghouse capabilities
- Providing access to standardized and advanced tools and methodologies
- Establishing common reporting formats and a shared common database
- Developing a standardized alerting process
- Establishing additional CERT/CIRTs where needed at C/S/A

Time: To be implemented by 1 October 2001

Estimated cost of implementation: $50-70M over FYDP

Page 1049 of 3957

Page 1050 of 3957

CONCLUSION

The Findings, Discussion and Recommendations described in this report were those that the Panel felt necessary to address the situation and correct deficiencies in organizational and operational issues noted during their investigation of the state of DIO within DoD. A number of activities had been initiated by the Department in response to previous reports (both DSB and others), but were too immature to determine whether the activities would be successful or were actually addressing the identified problems satisfactorily. The strongly held opinion of the majority of the Panel members was that, although there were some technological issues to be addressed in DIO, the majority of the issues impacting the ability of the Department to execute this mission were unclear, conflicting or non-existing policies, non-existing or conflicting operational procedures and inadequate resources. Lack of success in resolving the problems in these areas will continue to hamper the Department irrespective of the availability of technological solutions. The number of activities identified within the Department demonstrates a growing awareness of this fact and the need to develop a solid foundation for action. None of the recommendations mentioned in this report are particularly new or original to the Panel, nor are they difficult to understand or implement with strong, consistent leadership from OSD. That leadership is the key to success.

Page 1052 of 3957

APPENDIX A. REFERENCES

1. Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) Memo, subj: "Defense-wide Information Assurance Program (DIAP) Implementation Plan", 12 February 1999.

2. Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) Memo, subj: "DoD Information Management (IM) Strategic Plan Version 2.0", 19 October 1999. http://www.c3i.osd.mil/org/cio/ciolinks/references/itmstpln/itmstpln-memo.html

3. Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) Memo, subj: "Department of Defense (DoD) Public Key Infrastructure (PKI)," 12 August 2000. http://www.c3i.osd.mil/org/sio/ia/pki/pki_08122000.pdf

4. Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), *Information Superiority Final Report,* undated (FOUO.)

5. Assistant Secretary of Defense for Reserve Affairs, *Reserve Components Information Assurance Study,* Washington, D.C. February 2000. http://www.defenselink.mil/pubs/jrvio2001.pdf

6. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01B, "Requirements Generation System", 15 April 2001. http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3170_01b.pdf

7. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3401.01B, "Chairman's Readiness System", 19 June 2000. http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3401_01b.pdf

8. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3401.02, "Global Status of Resources and Training System", 20 October 1997.(includes Change-1, 19 March 1999. http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3401_02.pdf

9. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01C, "Information Assurance Implementation (IA Defense in Depth and Computer Network Defense)", draft of 1 August 2000.

10. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.04, "Information Assurance Readiness Metrics," 15 May 2000.

11. Critical Infrastructure Assurance Office, *Practices for Securing Critical Information Assets*, CIAO, Washington, D.C., January 2000.

Page 1053 of 3957

12. Defense Science Board, *Report of the Defense Science Board Task Force on Information Operations - Defense (IW-D),* Washington, D.C. November1996. http://cryptome.org/iwd.htm

13. Defense Science Board, *Report of the Defense Science Board Task Force on Human Resources Strategy,* Washington, D.C. February 2000.

14. Department of Defense, *Report to Congressional Defense Committees: Year 2000 (Y2K) Lessons Learned,* 15 March 2000.

15. Department of Defense Directive 5200.28, "Security of Automated Information Systems

16. (AISs)," 21 March 1988. http://web7.whs.osd.mil/pdf/d520028p.pdf

17. Department of Defense Directive 3600.3, "DoD Information Assurance Red Teaming", (draft).

18. Department of Defense Directive 3600.4, "DoD Information Operations Red Teaming (U)", (draft)

19. Department of Defense Directive 5210.42, "Nuclear Weapon Personnel Reliability Program (PRP)", . 8 January 2001 http://web7.whs.osd.mil/pdf/d521042p.pdf

20. Department of Defense Insider Threat Integrated Process Team report, *DoD Insider Threat Mitigation: Final Report,,* 24 April 2000.

21. Department of Defense, Office of the Inspector General, *DoD Management of Information Assurance Efforts to Protect Automated Information Systems,* Report # PO97-049, 25 September 1997 (FOUO)

22. Department of Defense, Office of the Inspector General, *Summary of Audit Results: DoD Information Assurance Challenges,* Report No. 99-069, Washington, D.C.,22 January 1999. http://www.dodig.osd.mil/audit/reports/fy99/99-069.pdf

23. Department of Defense, Office of the Inspector General, *Identification and Authentication Policy,* Report No. D-2000-058, Washington, D.C., 20 December 1999

24. Department of Defense, Office of the Inspector General, *Information Assurance Challenges: A Summary of Audit Results Reported December 1, 1998, through March 31, 2000,*Report No. D-2000-124, Washington, D.C., 15 May 2000 (FOUO).

25. Deputy Secretary of Defense (DepSecDef) Memo, subj: "DoD Chief Information Officer Executive Board", 31 March 2000. http://www.c3i.osd.mil/org/cio/memo_cio_exec_board3-31-00.pdf

Page 1054 of 3957

26. Deputy Secretary of Defense (DepSecDef) Memo, subj: "DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001 – March 31, 2000 – Global Information Grid", 31 March 2000. http://www.c3i.osd.mil/org/cio/doc/depsecdememo_gig3-31-00.pdf

27. Deputy Secretary of Defense (DepSecDef) Memo, subj: "Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 'Department of Defense Global Information Grid Information Assurance'," 16 June 2000. http://www.c3i.osd.mil/org/cio/doc/gigia061600.pdf

28. Deputy Secretary of Defense (DepSecDef) Memo, subj: "Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification, and Personnel Management in the Department of Defense," 14 July 2000.

29. Deputy Secretary of Defense (DepSecDef) Memo, subj: "Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 12-8430-July 26, 2000 – Acquiring Commercially Available Software", 26 July 2000. http://www.c3i.osd.mil/org/cio/doc/esi0726.pdf

30. Deputy Secretary of Defense (DepSecDef) Memo, subj: "DoD Chief Information Office (CIO) Guidance and Policy Memorandum No. 4-8460 — Department of Defense Global Information Grid Networks", 24 August 2000. http://www.c3i.osd.mil/org/cio/doc/gig4-8460-082400.pdf

31. Deputy Secretary of Defense (DepSecDef) Memo, subj: "DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 10-8460 – – Network Operations", . http://www.c3i.osd.mil/org/cio/doc/gig10-8460-082400.pdf

32. Information Assurance and Information Technology Human Resources Integrated Process Team Final Report: *Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense,* 27 August 1999. http://www.c3i.osd.mil/org/sio/ia/diap/graphics/Word-IPT_final000827.pdf

33. Information Assurance and Information Technology Human Resources Integrated Process Team Supplemental Report: *Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense,* February 2000. http://www.c3i.osd.mil/org/sio/ia/diap/graphics/WordIPTSupplementMar17.pdf

34. General Accounting Office (GAO), *Information Security: Computer Attacks at Department of Defense Post Increasing Risks,* GAO/AIMD-96-84, Washington, D.C, May 1996. http://www.gao.gov/

35. General Accounting Office (GAO), *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk,* GAO/AIMD-98-92, Washington, D.C. September 1998. http://www.gao.gov/

Page 1055 of 3957

36. General Accounting Office (GAO), *DoD Information Security: Serious Weaknesses Continue Place Defense Operations at Risk,* GAO/AIMD-99-107, Washington, D.C. August 1999. http://www.gao.gov/

37. General Accounting Office (GAO), *DoD Competitive Sourcing: Savings are Occurring, but Actions are Needed to Improve Accuracy of Savings Estimates,* GAO/NSIAD-00-107,Washington, D.C., August 2000. http://www.gao.gov/

38. Information Assurance Technology Analysis Center, *IA Metrics: Critical Review & Technology Assessment (CR/TA) Report,* DTIC, Falls Church, VA, 1 June 2000. http://iac.dtic.mil/iatac/pdf/Reports/IAMetric.pdf

39. Joint Pub 1-03.3, *Joint Reporting Structure: Status of Resources and Training System (SORTS),* Washington, D.C., 10 August 1993.

40. Joint Pub 3-13, *Joint Doctrine for Information Operations*, Washington, D.C., 9 October 1998. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

41. Joint Chiefs of Staff, *Joint Vision 2020.* http://www.dtic.mil/jv2020/jvpub2.htm

42. Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence,* Washington, D.C., 28 February 1994. http://www.spb.ncr.gov/html/jscrprt.html

43. Joint Security Commission II, *Report by the Joint Security Commission II*, Washington, D.C.,24 August 1999, (http://www.spb.ncr.gov/doc/JSC_Rpt.pdf).

44. Joint Staff, *Information Assurance: Legal, Regulatory, Policy and Organizational Considerations, 4th Edition,* Washington, D.C., August 1999. http://www.dtic.mil/jcs/

45. Keegan, Daniel, "High Tech Work Force Growing", Federal Computer Week, 18May2000, http://www.civic.com/civic/articles/2000/august/civ-cover-08-00.asp

46. Matthews, William, "IT Workforce counting on contractors", Federal Computer Week, 6 September, 2000, http://www.fcw.com/fcw/articles/2000/0904/web-survey-09-06-00.asp

47. Monroe, John Stein. "Work Force Tops CIO's Worries", Federal Computer Week, 9May2000, http://www.fcw.com/civic/articles/2000/0508/web-survey2-05-09-00.asp

48. National Defense Industrial Association, Command, Control, Communications Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) Committee, *Information Assurance Study,* August 2000.

49. National Intelligence Estimate (NIE) for Information Warfare.

Page 1056 of 3957

50. National Research Council, Computer Science and Telecommunications Board, *Realizing the Potential of C4I: Fundamental Challenges,* National Academy Press, Washington, D.C., 1999. (http://pompeii.nap.edu/catalog/catalog/cfm?record_id=6457)

51. National Security Telecommunications and Information Systems Security Committee Instruction (NSTISSI) No. 4009, "National Information Systems Security (INFOSEC) Glossary", September 2000. (http://www.nstissc.gov/Assets/pdf/4009.pdf)

52. National Security Telecommunications and Information Systems Security Committee report: *Ninth Assessment of the Status of National Security Telecommunications and Information Systems Security within the United States Government,* Washington, D.C. February 2001 (draft).

53. Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I), Infrastructure and Information Assurance Directorate, *Defense-Information Assurance Red Team Methodology,* Mitre Corporation, Washington, D.C. May 1999. (FOUO).

54. Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I), Defense-wide Information Program (DIAP), *Review of Department of Defense Public Key Enabling of Applications for FY 2001-2007,* Washington, D.C., April 2000 (FOUO).

55. Office of Federal Procurement Policy (OFPP) Policy Letter 92-1, "Inherently Governmental Functions", 23 September 1992, http://www.arnet.gov/Library/OFPP/PolicyLetters/Letters/PL92-1.html.

56. Office of Management and Budget (OMB) Circular A-130, "*Management of Federal Information Resources",* 8 Feb 1996, (http://www.Whitehouse.gov/WH/EOP/OMB/html/circulars/a130/a130.html).

57. Office of Personnel Management (OPM) Regulation 5CFR930.301-305, "Training Requirement for the Computer Security Act," 3 January 1992, (http://www-08.nist.gov/secplcy/opm_plcy.txt).

58. Office of Personnel Management (OPM), *Recruiting and Retaining Information Technology Professionals,* November 1998, (http://www.opm.gov/y2k/html/recruit1.htm).

59. President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations,* October 1997.

60. Public Law 100-235, *"Computer Security Act of 1987.*

61. Simpson, Doug, "The Ones That Got Away", Federal Computer Week, 7 Aug 2000,http://www.civic.com/civic/articles/2000/august/civ-cover-08-00.asp.

Page 1057 of 3957

62. Simpson, Doug, "Devising New Lures", Federal Computer Week, 7 Aug 2000,http://www.fcw.com/civic/articles/2000/august/civ-coverside-08-00.asp.

63. "The Three Rs of Bonuses and Allowances," FEDweek, http://www.fedweek.com/NewHotNews/3RsBonusAllow.htm.

64. Under Secretary of Defense (Personnel and Readiness)/Assistant Secretary of Defense (Command, Control, Communications and Intelligence) Memo, subj: "Information Assurance (IA) Training and Certification," 29 June 1998.

65. U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800-16, *Information Technology Security Training Requirements: A Role-and Performance-Based Model,* Gaithersburg, MD, April 1998, http://csrc.nist.gov/nistpubs/index.html.

66. The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0,* Washington, D.C., 2000.

Page 1058 of 3957

APPENDIX B. PANEL MEMBERS AND GOVERNMENT ADVISORS

Chairman:

Mr. John Grimes	Raytheon Company

Members:

MajGen John Casciano, USAF (Ret)	Litton/TASC
Mr. William Gravell	TRW
LTG Patrick Hughes, USA (Ret)	Private Consultant
Mr. Lowell Thomas	Verizon Communications

Government Advisors:

Mr. Arnold Abraham	OASD (C3I)
CAPT Katharine Burton, USN	OASD (C3I)/DIAP
Mr. Peter Fonash	National Communications System
Mr. Gus Guissanie	OASD (C31)
CAPT Basil Harris, USN	J6K Joint Staff
BrigGen Paul LeBras, USAF	J-2 Joint Staff
LtCol Susan Pardo, USAF	AF/SCMI

Page 1059 of 3957

Page 1060 of 3957

Page 1061 of 3957

APPENDIX C. POLICY MATRIX

Public Law and Executive Branch Issuances					
Public Law	**Executive Orders**	**Presidential Decision Directives**	**National Security Directives**	**OMB Circulars**	**NIST Standards & Guidance**
Computer Fraud & Abuse Act (18 USC 1030) 1986	United States Intelligence Activities EO 12333 4 Dec 1981	Security Policy Coordination PDD-29 27 Sep 1994	National Policy for the Security of National Security Telecommunications and Information NSD No. 42 Jul 1990	Management Accountability and Control OMB Circular-123 21 Jul 1995	Information Technology Security Training Requirements NIST Special Publication 800-16 April 1998
Computer Security Act of 1987 (PL 100-235)	National Security Telecommunications Advisory Committee EO 12382 13 Sep 1982	Combating Terrorism PDD-62 22 May 1998		Financial Management Systems OMB Circular-127 Revised 23 Jul 1993	
Government Performance and Results Act of 1993	National Industrial Security Program EO 12829 6 Jan 1993	Critical Infrastructure Protection PDD-63 22 May 1998		Management of Federal Information Resources OMB Circular-A130 Revised 8 Feb 1996	
Paperwork Reduction Act of 1995 (PL 104-13)	U.S. Advisory Council on the NII EO 12864 15 Sep 1993				
Information Technology Management	Classified National Security Information EO 12958 17 Apr 1995				

Page 1061 of 3957

Public Law and Executive Branch Issuances					
Public Law	**Executive Orders**	**Presidential Decision Directives**	**National Security Directives**	**OMB Circulars**	**NIST Standards & Guidance**
Reform Act of 1996 (PL 104-106)					
Security and Freedom Through Encryption Act. (I believe this has never become law.)	Access to Classified Information EO 12968 4 Aug 1995				
	Critical Infrastructure Protection with Amendments EO 13010 15 Jul 1996				
	Federal Information Technology EO 13011 17 Jul 1996				
	Administration Of Export Controls On Encryption Products EO 15 Nov 1996				
	Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet EO 13035 11 Feb 1997				

Page 1062 of 3957

Page 1063 of 3957

DoD ISSUANCES										
8500 - General	**8510 - Certification & Accreditation**	**8520 - Security Management (SMI, PKI, KMI, EKMS)**	**8530 - Computer Network Defense**	**8540 - Interconnectivity /Multi-Level Security**	**8550 - Network/Web (Access, Content, Privileges)**	**8560 - Assessments (VAP, Red Team, TEMPEST Testing)**	**8570 - Education, Training, Awareness**	**8580 - Other**	**8590 - Critical Infrastructure Protection**	***Related Information Assurance Issuances***
Guidance and Policy for Department of Defense Information Assurance) Guidance and Policy Memorandum No. 6-8510 Jan 2000	DoD Information Technology Security Certification and Accreditation Process (DITSCAP) DoDI 5200.40 10 Feb 1998	PKI Roadmap, Version 3 29 Oct 1999	Computer Network Defense DoDD O-8530.aa DRAFT	Secret and Below Initiative (SABI) DoD Memorandum 20 Mar 1997	Policy for Establishing and Maintaining a Publicly Accessible DoD Web Information Service Policy Memorandum 9 Jan 98	Computer Security Technical Vulnerability Reporting Program (CSTVRP) DoDI 5215.2 2 Sep 1986	Information Assurance Training & Certification DoD Memorandum 29 Jun 1998		Critical Asset Assurance Program (CAAp) DoDD 5160.54 20 Jan 1998	Unauthorized Disclosure of Classified Information to the Public DoDD 5210.50 27 Feb 1992
Security Requirements for Automated Information Systems DODD 5200.28 21 Mar 1988	DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document DRAFT DoD-M 5200.40-M 21 Apr 1999	Department of Defense (DoD) Public Key Infrastructure (PKI) Policy Memorandum 6 May 1999	Computer Network Defense DoDI O-8530.bb DRAFT	DISN Connection Security Requirements 15 Dec 1999	Information Vulnerability and the World Wide Web DoD Memorandum 24 Sep 1998	Communications Security Telephone Monitoring and Recording DoDD 4630.6 26 Jun 1981	Policy on Department of Defense (DoD) Electronic Notice and Consent Banner DoD Memorandum 16 Jan 1997		Critical Asset Assurance Protection DoDD 5160.54 DRAFT	DoD Industrial Security Program DoDD 5220.22 8 Dec 1980
Communications Security (COMSEC) (U) 5200.5 Apr 1990	Department of Defense (DoD) Security Certification and Accreditation Process DoDI 5200.40 DRAFT 30 Nov 1999	PKI X.509 Certificate Policy for the U.S. DoD 13 Dec 1999	Department of Defense Information Assurance Vulnerability Alert (IAVA) DoD Memorandum 30 Dec 1999	DISN SIPRNet Connection Approval Process, Supplements 1-4 15 Dec 1999	Web Site Administration Policies and Procedures DepSecDef Memorandum 7 Dec 1998					Security of Defense Contractor Telecommunications (Includes Change 1) DoDI 5210.74 16 Nov 1996
Security of DoD Contractor Telecommunications 5210.74 Jun 1985	DoD Trusted Computer System Evaluation Criteria DoD 5200.28 STD Dec 1985	PKI Operating Documents DoD Memorandum 13 Dec 1999		Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) OSD Policy Memorandum 22 August 1999	Electronic Newspaper Policy DoDI 5120.4 Policy Memorandum 29 May 1996					Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems DRAFT 28 Feb 2000
Computer Security Evaluation Center DoDD 5215.1, Includes Change 1 16 Nov 1994		Smart Card Adoption and Implementation DoD Memorandum 10 Nov 1999			Clearance Procedures for Making Electronic Information Available to the Public DoD Memorandum 17 Feb 1995					DoD Information Security Program DoDD 5200.1 13 Dec 1996

Page 1063 of 3957

DoD ISSUANCES										
8500 - General	**8510 - Certification & Accreditation**	**8520 - Security Management (SMI, PKI, KMI, EKMS)**	**8530 - Computer Network Defense**	**8540 - Interconnectivity /Multi-Level Security**	**8550 - Network/Web (Access, Content, Privileges)**	**8560 - Assessments (VAP, Red Team, TEMPEST Testing)**	**8570 - Education, Training, Awareness**	**8580 - Other**	**8590 - Critical Infrastructure Protection**	***Related Information Assurance Issuances***
Control of Compromising Emanations (U) C5200.19 May 1995		Public Key Enabling of Applications for the Department of Defense Public Key Infrastructure (PKI) DoD Memorandum DRAFT 24 Nov 1999								Information Security Program DoD 5200.1-R 14 Jan 1997
										Personnel Security Program Regulation, Including Change 3 DoD 5200.2-R 23 Feb 1996
										DoD Freedom of Information Act (FOIA) Program DoDD 5400.7 29 Sep 1997
										Control of Compromising Emanations OASD (C3I)
										DoD Technical Architecture Framework for Information Management, Vol 6: DoD Goal Security Architecture Version 3.0 30 Apr 1996
										Electronic Warfare (EW) and C3W Countermeasures DoDD 3222.4 31 Jul 1992
										Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems DoDD 4630.5 12 Nov 1992

Page 1064 of 3957

Page 1065 of 3957

DoD ISSUANCES										
8500 - General	**8510 - Certification & Accreditation**	**8520 - Security Management (SMI, PKI, KMI, EKMS)**	**8530 - Computer Network Defense**	**8540 - Interconnectivity /Multi-Level Security**	**8550 - Network/Web (Access, Content, Privileges)**	**8560 - Assessments (VAP, Red Team, TEMPEST Testing)**	**8570 - Education, Training, Awareness**	**8580 - Other**	**8590 - Critical Infrastructure Protection**	***Related Information Assurance Issuances***
										Clearance Procedures for Making Electronic Information Available to the Public DoD Memorandum 17 Nov 1999
										Policy on Operational Test and Evaluation of Information Assurance DoD Memorandum 17 Nov 1999
										DoD Information Operations (U) S3600.1 Dec 1996
										Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection DoDD 5200.39 10 Sep 1997

JOINT, AGENCY, and NSTISSC ISSUANCES				
Joint Staff	**DISA**	**NSA**	**NSTISSC**	**DCI**
Defensive Information Operations Implementation CJCSI 6510.01B 22 August 1997			National Information Systems Security (INFOSEC) Glossary NSTISSI No. 4009, January 1999 (Revision	Policy for the Protection of Classified non-SCI Sources and Methods Intelligence (SAMI) **DRAFT #21** 11 Apr 00

Page 1065 of 3957

Page 1066 of 3957

JOINT, AGENCY, and NSTISSC ISSUANCES				
Joint Staff	**DISA**	**NSA**	**NSTISSC**	**DCI**
			1)	
Defense Information System Network and Connected Systems CJCSI 6211.02A 22 May 1996			National Information Assurance Certification and Accreditation Process (NIACAP) NSTISSI No. 1000 Apr 2000	DCID 6/5T Implementation Manual for the Protection of Classified non-SCI Sources and Methods Intelligence (SAMI) **DRAFT #21** 11 Apr 00
Policy for the Defense Switched Network CJCSI 6215.01 February 1995			National Training Program for INFOSEC Professionals NSTISSD No. 501 16 November 1992	
Information Operations Condition CM-510-99 10 Mar 1999			Information Systems Security (INFOSEC) Education, Training, and Awareness NSTISSD No. 500 25 February 1993	
Joint Doctrine for Information Operations Joint Pub 3-13 9 Oct 1998			National Training Standard for INFOSEC Professionals NSTISSI No. 4011 20 June 1994	
Information Assurance Implementation (IA Defense in Depth and Computer Network Defense **PRELIMINARY DRAFT** CJCSI 6510.01C 1 Aug 2000			National Training Standard for Designated Approving Authority (DAA) NSTISSI No. 4012 August 1997	

Page 1066 of 3957

Page 1067 of 3957

JOINT, AGENCY, and NSTISSC ISSUANCES				
Joint Staff	**DISA**	**NSA**	**NSTISSC**	**DCI**
Information Assurance Implementation (IA Defense in Depth and Computer Network Defense PRELIMINARY DRAFT CJCSI 6510.01C 1 Aug 2000			National Training Standard for System Administrators in Information Systems Security (INFOSEC) NSTISSI No. 4013 August 1997	
Information Assurance (Defense in Depth) Implementation Procedures **DRAFT** CJCSM 6510.01 1 Sep 2000			National Training Standard for Information Systems Security Officers (ISSO) NSTISSI No. 4014 August 1997	
Information Assurance Readiness Metrics CJCSI 6510.04 1 May 2000			National Policy for Incident Response and Vulnerability Reporting for National Security Systems NSTISSP No. 5 Aug 1993	
			TEMPEST Countermeasures for Facilities NSTISSI 7000 Nov 1993	

Page 1067 of 3957

C-8

APPENDIX D: ORGANIZATION AND OPERATIONS PANEL QUESTIONAIRE

1.0 INTRODUCTION

1.1 Organization and Operations Panel Questionnaire

The Organization and Operations Panel of Defense Science Board (DSB) Task Force for Defensive Information Operations (DIO) issued a questionnaire in May of 2000 to assess information assurance (IA) organizational perspectives regarding current Information Assurance functions across DoD. The questionnaire was distributed to 132 organizations, drawn from the Services, CINCs, Agencies and related entities. Each of the selected organizations is currently engaged in IA missions across a wide spectrum of functional areas. The questionnaire sought to elicit information from major IA entities to determine existing roles, mission objectives, organizational relationships, and connectivity as well as to assess the community's self-perceived level of confidence and obtain information regarding perceived needs and future requirements. The results of this questionnaire were also intended to aid in measuring progress toward meeting the specific recommendations of the 1996 DSB DIO report and to develop future policy. The questionnaire presented a series of questions to participants ranging from the identification of each organization's IA missions to the assessment of funding methods for information assurance functions.

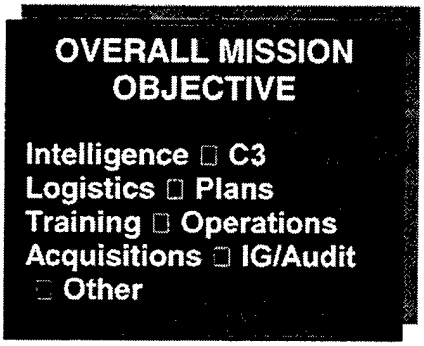
The DSB Organization and Operations Panel identified 132 organizations involved in IA activities to represent the DoD IA Community and to serve as the pool of respondents for the questionnaire. Of the 132 organizations that were sent the questionnaire, 56 responded for a response rate of 42%. Table 1 presents the distribution of the respondents by organization type.

Table 1. Questionnaire Response Breakdown

Component	No. of Responses	% Distribution
Services	38	68%
CINCs	5	9%
Agencies and Offices	13	23%
TOTAL	56	100%

The organizations that responded to the questionnaire constituted a broad cross section of overall and IA mission areas and it is therefore possible to extract some general trends from the results.

The initial questions requested the organizations to identify and prioritize both their overall and specific IA missions from the categories below:

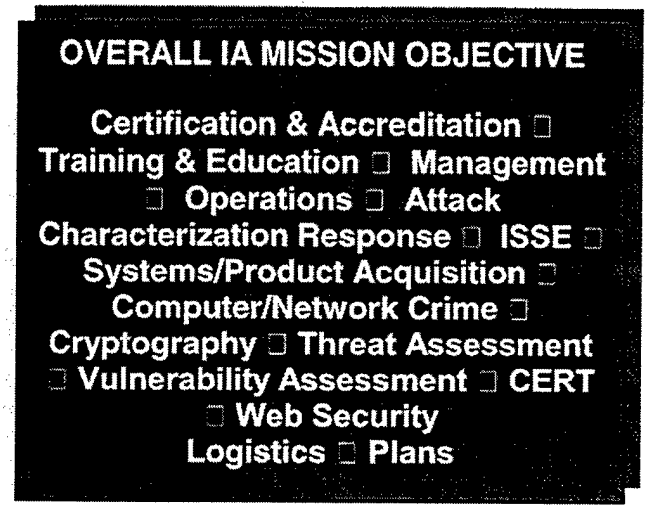


FINDINGS:

- **32% of the respondents chose C3 as their overall mission priority**
- **30% of the respondents chose "other" operations their overall mission objective**
- **14% of the respondents chose IG/Audit as their overall mission objective**
- **The remaining 24% was relatively equally divided among the remaining categories**

FINDINGS

- **31% of the respondents chose management as overall IA mission priority**
- **15% of the respondents chose CERT as overall mission priority**
- **9% of the respondents chose certification and accreditation as overall mission priority**
- **The remaining 45% was divided among the remaining categories**



The organizations were also given the opportunity to provide feedback and comments to the DSB with respect to issues of particular concern in the IA arena[1]. The comments provide a window into the opinions and concerns of the IA community that was not necessarily consistent with the specific questionnaire responses. These comments appear to suggest that while DoD has succeeded in formulating "high level" policy and guidance with respect to IA issues, the implementation of these policies in the ranks and the development of detailed operational requirements and regulations is an area that must continue to be addressed.

The questionnaire results suggest that the absence of a consistent process to implement IA policy has led to inconsistent actions being taken across the DoD. Many respondents also suggested that policy updates should be issued in a more timely manner, so as to keep pace with technological advances and to avoid the implementation of a patchwork of policy. The questionnaire responses provide a great deal of information and insight into current DoD IA posture, and identify issues that will be of significance in the near term future.

This appendix will provide an analysis of the questionnaire responses and the implied trends throughout the IA community as represented by the pool of questionnaire respondents.

---

1 *The comments are presented in greater detail in subsequent sections and Attachment A.*

1.2 DSB Questionnaire Methodology

Fifty-six organizations responded to the DSB questionnaire. Each organization was treated as an independent entity within the IA community. The analysis, therefore, strives to demonstrate a number of trends present throughout both the IA community and the Department.

The distribution of respondents is heavily Service-oriented and within that group, Army comprised the majority of the responses. However, the trends noted below appear to be consistent across all groups that responded to the questionnaire. Furthermore, the significance of the heavy Service representation is offset by the fact that the Services retain the bulk of the execution responsibilities as delineated by *Goldwater-Nichols*, and so retain primary responsibility for implementing IA programs across the Department. Accordingly, the fact that the Services constitute the bulk of respondents serves to provide an accurate depiction of the composition of the IA community on the ground. This, in turn, lends credence to the purpose of this analysis; namely to provide a window into the current state of the DoD IA community as perceived by the participants. The results also constitute a "pulse check" on the perceived availability of proper resources, policy, and funding throughout the DoD IA community.

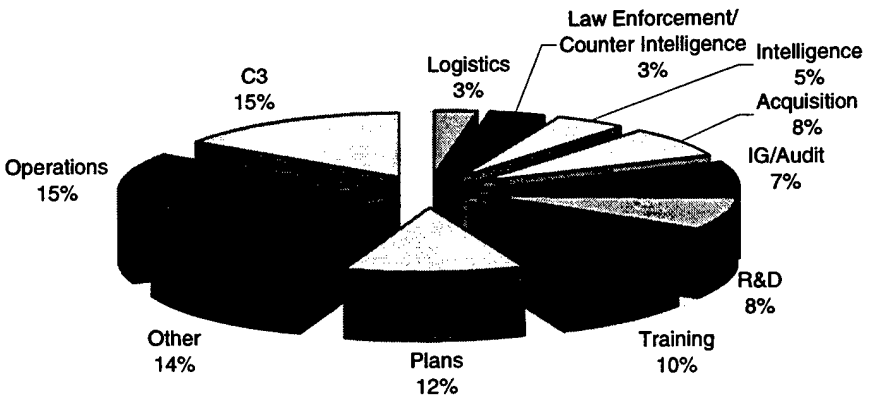
2.0 DSB QUESTIONNAIRE ANALYSIS

2.1 Mission characterization

2.1.1 What is your specific organization's overall mission and overall mission priority?

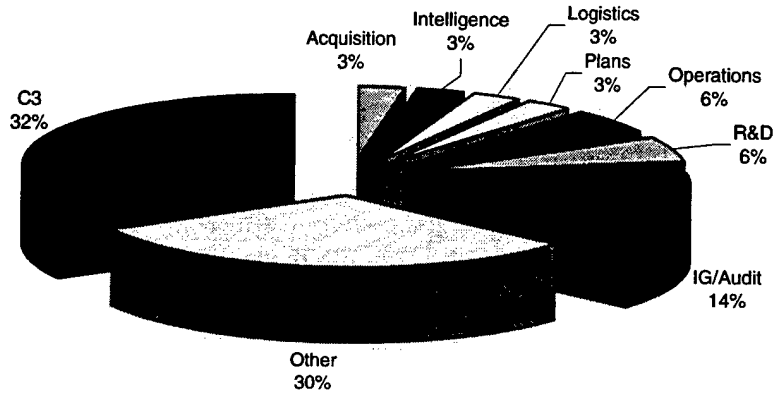
The first question posed in the questionnaire sought to capture the distribution and priority of the overall mission objectives of organizations within the IA community. Respondents were given a list of missions to choose from and requested to select all that applied to their organization. Respondents were then requested to prioritize each mission objective. Figure 1 illustrates the diverse nature of missions within the IA community. On average, each of the 56 respondents chose 2 to 3 mission objectives. Most organizations included C3, operations, and planning among their overall mission objectives.

Figure 1. DoD Overall Mission



The graph illustrates that there is a great deal of variation across the DoD IA community, in terms of mission objectives. As IA continues to gain strength and recognition as a critical element of Defense in Depth, IA issues, and the availability of IA services within the mission areas will continue to grow, placing further pressure on IA organizations for resources, training and other services. Further, while the majority of respondents are involved in C3, planning, training, or some other activity outside of the questionnaire choices, the results suggest that IA activities have become more routine, and an inherent function of DoD business processes.

Figure 2. DoD Overall Mission Top Priority



In addition to identifying their mission objectives, respondents were also asked to prioritize their overall mission objectives. Figure 2 illustrates that C3 and IG/Audit were the highest priorities identified by the respondents. The category of "other", which was the choice of a significant number of respondents, suggests that there is a sizable portion of the IA community involved in activities, which have expanded beyond the scope of the traditional mission objective choices. The results seem to suggest that IA is slowly being integrated into the routine of all organizations throughout DoD. Thus, while IA activities continue to be concentrated in organizations with a C3 mission, the results suggest that the IA community is expanding into areas such as R&D and operations.

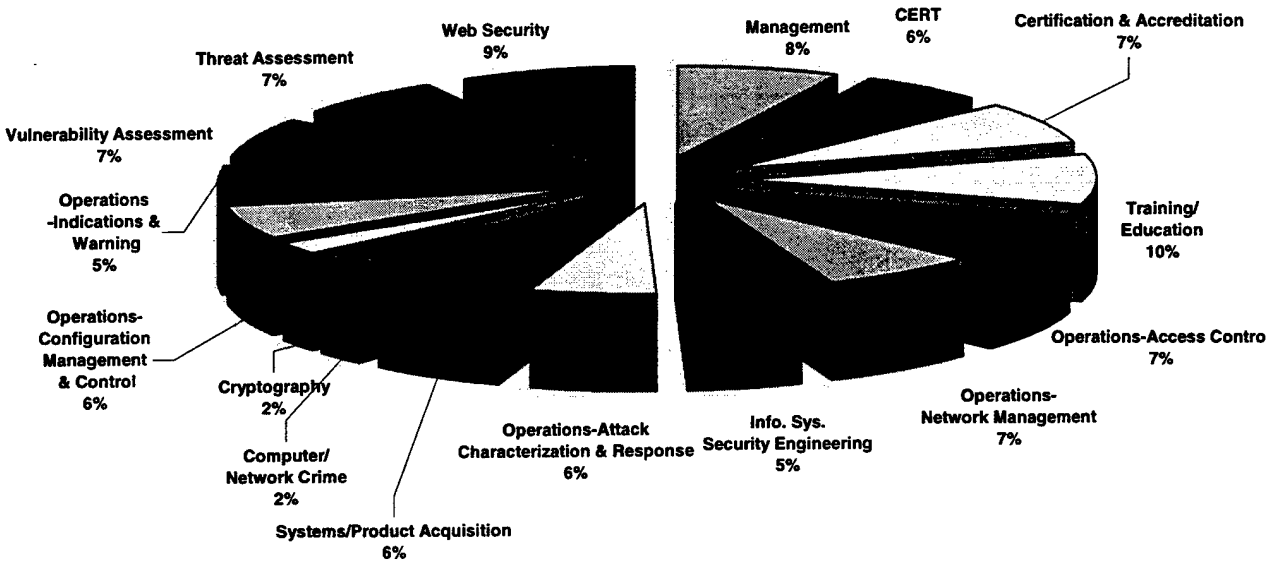
2.1.2 What is your organization's IA mission and IA mission priority?

Respondents were asked to check and prioritize the overall IA mission objectives that applied to their organization. On average, respondents chose six different objectives from the provided list. Figure 3 illustrates the distribution of the frequency with which each category was chosen.

This graph illustrates that the missions of the IA community are quite diverse and cut across numerous focus areas, with training and web security being the most frequently cited IA objectives. The graph further suggests that the IA community's activities are not simply limited to information security issues, but have also become a part of the business processes that exist in the background. IA appears to be developing into a discipline that is increasingly found in a full range of services, suggesting that IA is continuing to evolve into a mainstream activity.

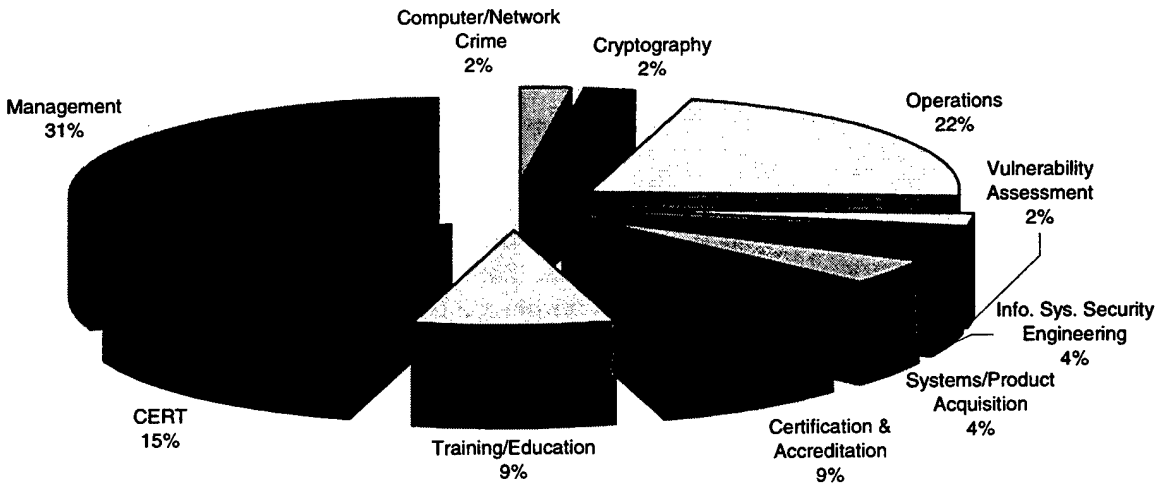
Page 1072 of 3957

Figure 3. Overall IA Mission
(Respondants were requetsed to chose all categories that applied)



The questionnaire also asked the respondents to prioritize their overall IA mission objectives. As shown in Figure 4, management was the top IA mission priority chosen by respondents, with nearly one-third of the respondents engaged in some sort of management or oversight role.

Figure 4. DoD IA Mission Priority



Further analysis of the results illustrated in Figure 4 suggests that the IA community has a clear management role, or at least believes it dedicates a great deal of resources towards general management (i.e. accounting, requirements, and funding). The frequency with which respondents chose management as a priority is consistent with the fact that IA is a pervasive issue that reaches almost every organization and activity. As there is a great deal to manage, the infrastructure must be in place to execute all IA activities and initiatives throughout DoD. Management, training, and C&A accounted for 48% of IA priorities, operations as a whole accounted for 22%, CERT accounted for 15%, and general support functions accounted for 13%. However, while these numbers suggest a great deal of variety in terms of the IA priorities throughout the community, it may also indicate that there is divide among the community in terms of mission objective.

2.1.3 Additional observations

In characterizing the IA community's "overall mission objective" and "IA mission objectives", the data suggests that the IA community continues to grow in both scope and in depth. The results also indicate that IA functions are present in a growing number of organizations with a burgeoning variety of overall IA objectives. IA should continue to expand into other organizations and mission objectives as the ability to deliver information in a safe, secure, and highly trusted manner becomes increasingly crucial to the day-to-day operations of the Department. This will be especially true as the Department's E-commerce initiative continues to grow and become standard practice.

2.2 Requirements and Resources

To achieve an overall perspective on the IA community, it is helpful to assess the community's perceptions of its ability to meet the responsibilities set forth in policy both at the departmental and organizational levels. To this end, the questionnaire sought to assess the availability of resources in the form of funding, personnel, and policy.

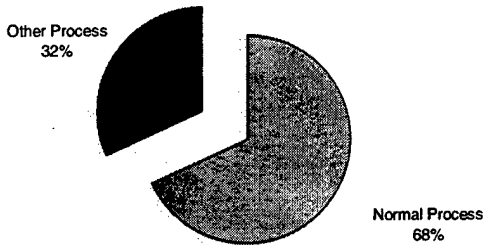
2.2.1 Have your IA requirements been identified?

Figures 5 through 8 illustrate that the respondents feel that the majority of their requirements have either been fully identified or partially identified, suggesting that they are well able to articulate their IA needs. Almost two-thirds of the respondents have been able to identify their requirements through normal processes, with organizations integrating IA into their standard requests for funding every year. This suggests that there may be sufficient procedures, processes and organizations in place to address IA issues within the PPBS cycle and the POM process.

These graphs also show that about 80% of the community is able to at least partially identify their requirements; however, 42% percent of these requirements have only been partially validated. The relatively large percentage of partially validated requirements implies that it is important to continue to investigate why there is such a substantial amount of requirements that remain only partially identified to facilitate the overall ability of the community to fund its activities.

Page 1074 of 3957

Figure 5. Requirement Identification Process



Normal process: PPBS, JROC, etc.
Other process: Vulnerability assessment or other assessment/inspection process

Figure 6. Requirements Identification Using Normal Process

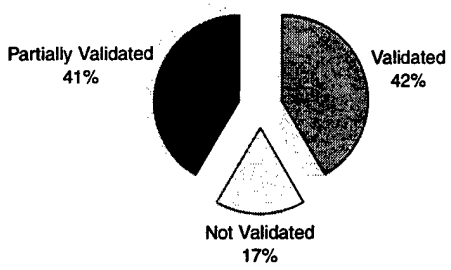


Figure 7. Requirements Identification using Other Processes

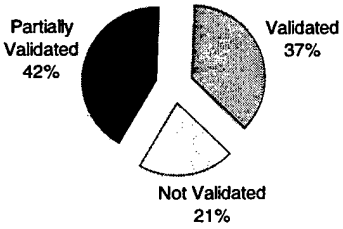
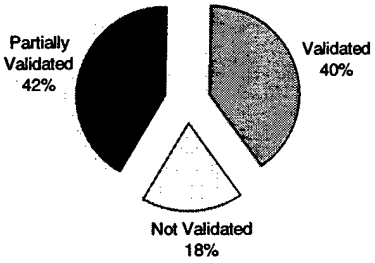


Figure 8. Requirements Identification - Process Independant



2.2.2 Have your IA requirements been resourced?

Figures 9 through 13 illustrate the perceptions among the respondents regarding the effectiveness of their investment and resources.

Figure 9. Do you have enough capital investment funding for IA?

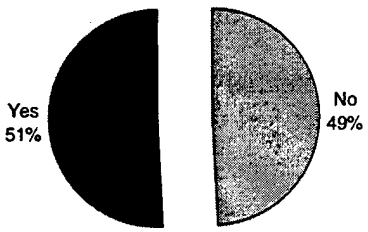
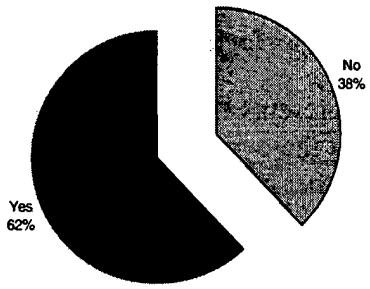


Figure 10. Do you have enough capital investment on facilities?



Page 1075 of 3957

Figure 11. Do you have enough of the right people working IA?

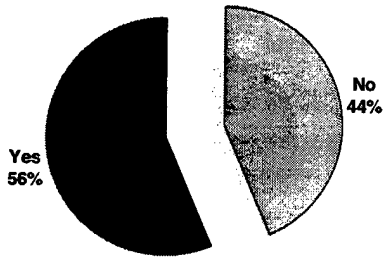


Figure 12. Are your people properly trained?

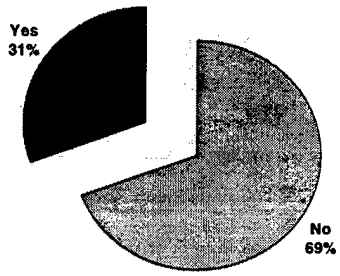
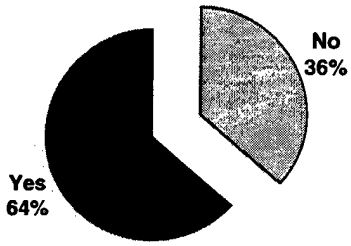


Figure 13. Do you have enough capital investment for IA operations?



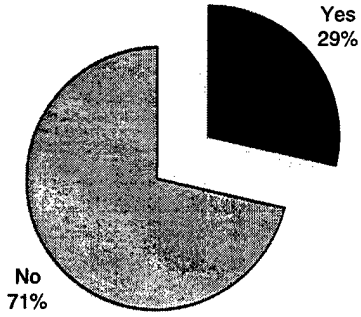
The graphs above illustrate that only about half of the respondents believe they have enough capital investment for IA in general. However, almost two-thirds of the respondents believe they have enough capital investment for facilities and IA operations. This implies that, while the respondents feel that they do not necessarily have enough total resources for IA activities, they feel they are adequately funded for facilities and operations. As almost one-third of the respondents feel they do not have the proper investment capital, further investigation would seem to be warranted.

With regard to personnel requirements, the majority of the respondents felt that they had adequate numbers of people, but that these people do not have the proper training. This correlates to the low placement of education on the IA priority list as seen in Figure 3, and suggests a need to raise the profile of IA education and training throughout the IA community.

2.2.3 Does performance of your IA mission conflict with any other responsibilities?

Figure 14 presents the results from the inquiry regarding potential mission conflict. This figure suggest that the overwhelming majority of respondents do not feel that their IA mission conflicts with their other responsibilities.

Figure 14. Does performance of your IA mission conflict with any of your other responsibilities?



In theory, an organization's IA mission should not conflict with its overall responsibilities because IA is designed to enhance the majority of IA mission objectives engaged in by the community. However, there may be instances when the practical outcome of DoD's IA policy (i.e. smart cards or PKI) may inhibit the tactical world. These services are designed to provide another layer for DoD's Defense-in-depth strategy, yet some organizations may view the additional layers of security as a liability rather than a safeguard.

2.2.4 Do you think you have the right tools to carry out your IA mission?

As a general rule, securing adequate resources in the form of funding or people is a constant challenge for any organization, regardless of the specific issue or technology. However, these issue present only one part of the overall picture. An analysis of the respondent's data implies that, for IA organizations, policy and authority tools are becoming just as important as funding. If Department policy does not clearly communicate the roles and responsibilities that Components are required to implement than it becomes nearly impossible to carry out the IA mission effectively or to cultivate change and growth.

Figures 15 through 17 suggest that while the respondents believe they have generally good information, they do not overwhelmingly believe that the proper policies are in place or that they have the proper authority over subordinates and/or organizations.

Figure 15. Do you think you have adequate and clear IA policy/guidance from above to carry out your IA mission?

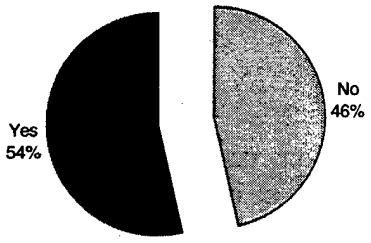


Figure 16. Do you think you have adequate authority over subordinates/organizations to carry out your IA mission?

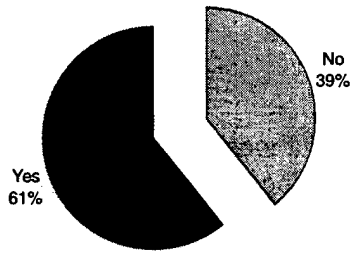
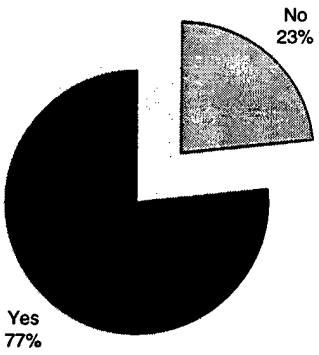


Figure 17. Do you have adequate information you execute your IA mission?



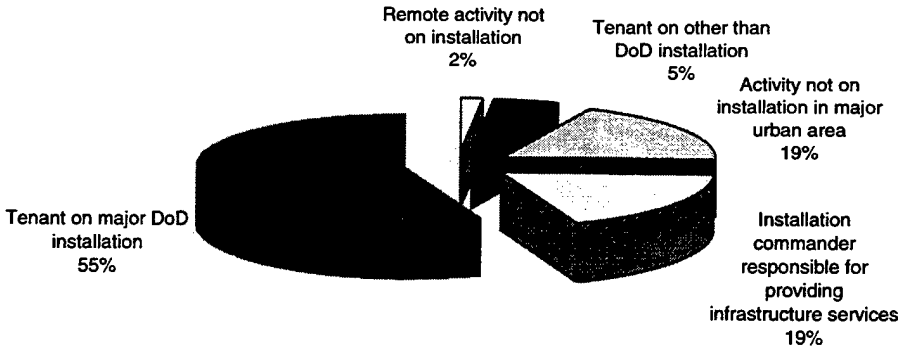
This becomes especially important in the case of Agencies and CINCs who are often dependent on the Services for the delivery of IA services. The results also point to the growing interdependence of organizations in the IA community that has developed as a result of information sharing and enhanced communication within the community.

2.3 Infrastructure Availability

2.3.1 Activity Situation

Figure 18 illustrates that the majority of DoD IA activities sit on major DoD installations.

Figure 18. What best describes your activity situation?



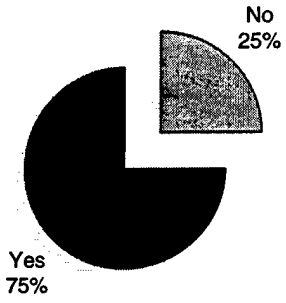
The second most common situation is activities where the installation commander is responsible for delivering infrastructure services. These may be minor installation or installations in an urban area. An additional twenty- percent of the respondents are situated in remote locations.

Page 1078 of 3957

2.3.2 Availability of DoD Infrastructure

Figure 19 addresses the availability of essential infrastructure.

Figure 19. Do you consdier DoD Infrastructure servvices in mission planning?



The results of this question illustrate that about three-fourths of the respondents consider the DoD infrastructure in mission planning. This suggests that organizations are considering both information assurance and infrastructure assurance issues, which have a symbiotic relationship. Without the availability of the various elements of the DOD infrastructure, it becomes difficult if not impossible to meaningfully execute the IA mission.

Figure 20. How do you consider DoD Infrastructure availability in mission planning?

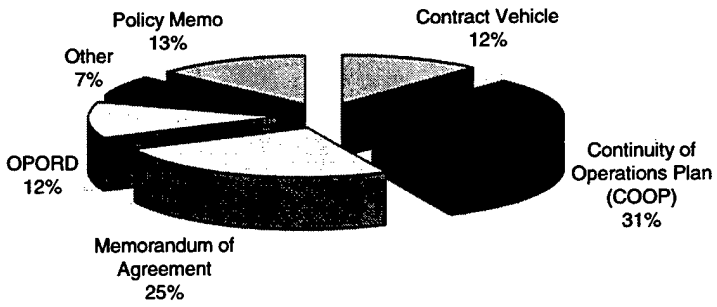


Figure 20 suggests that most respondents consider DoD infrastructure for Continuity of Operations Plans (COOPs) and for memoranda of agreement (MOA). Since the availability of the infrastructure drives COOPs and plays a key role in MOAs, it is not surprising that the respondents chose these two most frequently. In addition to assessing those situations where

Page 1079 of 3957

organizations consider infrastructure issues, it is also important to ascertain the level of an organization's confidence in the availability of infrastructure at critical times.

Figure 21. Are you confidence in that the services you require will be available whenever needed?

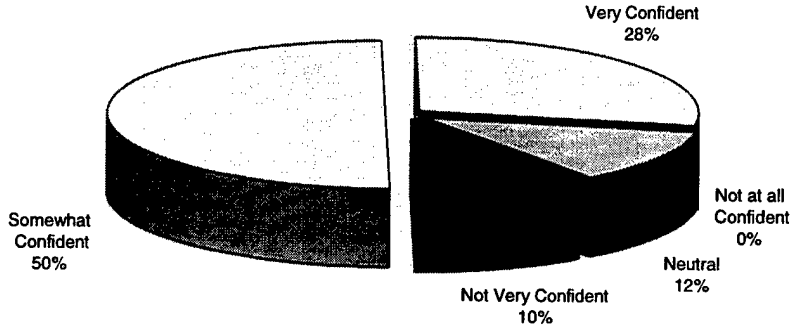


Figure 21 illustrates that only about one quarter of the respondents are confident that the infrastructure services upon which they rely will be available whenever needed, while over 50% of the respondents are only somewhat confident that the services they need will always be available. Such results suggest that there is a pronounced absence of confidence in the current ability of the DoD infrastructure to deliver services on demand.

2.4 Impact of IA Activities on Mission Performance

2.4.1 How do the following IA processes impact your mission performance?

Figures 22 through 28 illustrate the impact of IA activities on mission objectives.

Figure 22. Vulnerability Alert Process

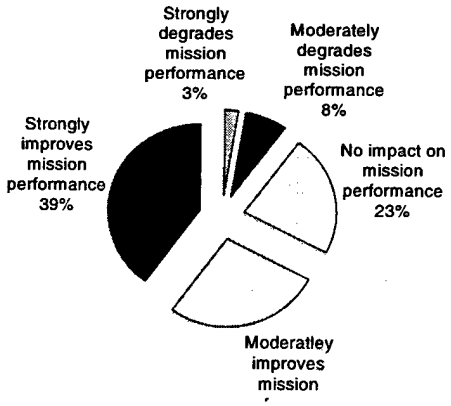


Figure 23. INFOCONS

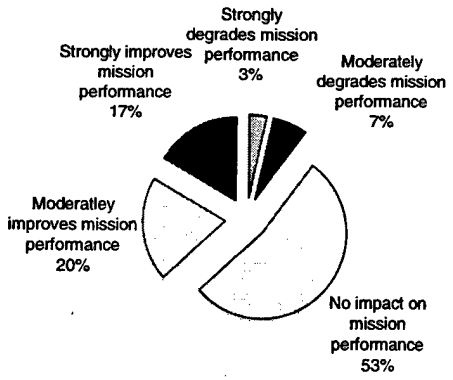


Figure 24. Incident Reporting Process

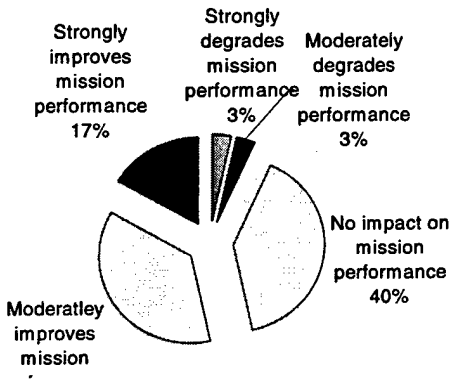


Figure 25. Accreditation Process

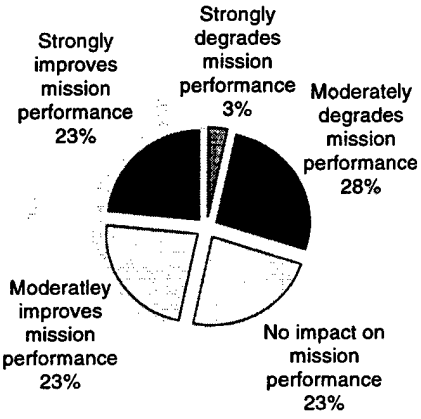


Figure 26. Vulnerability Assessment Process

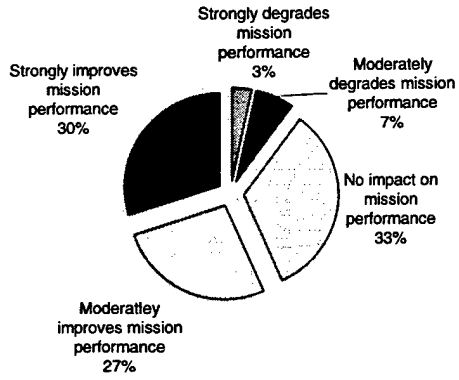
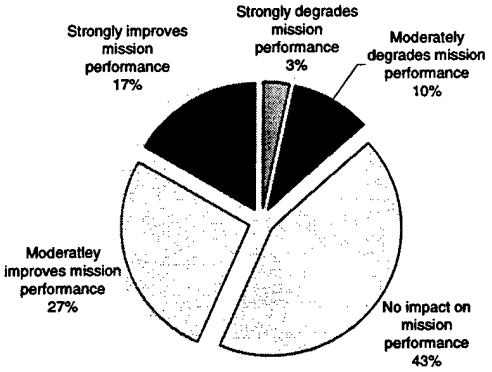


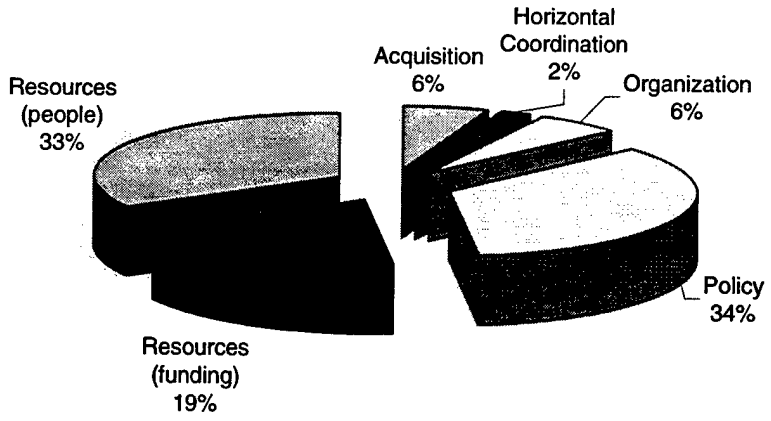
Figure 28. Recovery/Reconstitution Process



The results suggest that Vulnerability Alert Process and Vulnerability Assessment most significantly influence the respondents' mission objectives. Most of the IA activities have only very little or a moderate impact at all on mission. While virtually no IA activities have a strongly negative impact on mission objectives, threat assessment and the accreditation and certification activate moderately degrade mission performance, with respondents reporting that about one-third of the these activities were at least moderately degrading mission objective.

Page 1081 of 3957

Figure 29. Issues Warranting Attention



2.5. Issues Warranting Attention

While IA has made significant progress in expanding its reach throughout the Department, there are still a variety of issues that must continuously be examined and reevaluated. As with any program or initiative, funding and well-trained personnel will always be issues to program managers. Perhaps the most interesting result of the questionnaire analysis is the fact that policy was identified as the single biggest concern of the respondents. These results were borne out by the "*Comments*" received at the end of the questionnaire and presented in full in Attachment A.

The small numbers for acquisition, organization, and horizontal coordination suggest that communication among organizations is adequate and that the organizational structure of the IA community itself is not of great concern. However, issues such as roles and responsibilities as well as new money allocated for various IA efforts continue to challenge the organizations that are charged with implementing the changes. The concerns reflected in Figure 29 are consistent with the trend found throughout the questionnaire indicating that the community is generally confused, and in need of a greater guidance as well as policy that has more detail and applicability to their own organization's day-to-day functions.

2.6. Coordination and Interface

Respondents were asked to provide insight into the organizations they work with and draw support from in both the public and private sectors. Please see Attachment B for the results of this inquiry (i.e., a full list of organization's coordination and interface from questions 10a, 10b, and 10c).

Page 1082 of 3957

3.0 COMMENTS

In addition to the specific data represented in the graphs set forth in the previous sections, organizations were also asked to provide more general feedback on those issues not specifically covered by the questionnaire. These comments were intended to give participants the opportunity to highlight any areas of particular concern in the IA community with respect to the subject matter of the survey, and to provide the DSB with greater insight into those concerns. A frequent focus of these concerns is the expressed need for clear policy, and resources, both with respect to funding and qualified people. While many organizations responded positively to the specific survey questions directed towards the adequacy of policy and guidance, respondents' true feelings about their IA posture was clarified in the comments, and presents a somewhat less sanguine view of the state of policy at the organizational level. . This apparent discrepancy between the comments and the specific survey responses may be indicative of a desire on the part of the respondents to provide a "politically correct" response to the direct questions in the survey.

A detailed review of the comments seems to indicate that most organizations would welcome clearer policy and guidance from OSD, which would enable them to better develop policy specifically applicable to their own organizations. Many of the respondents expressed the belief that there was sufficient be "high level" policy", however, this policy was of limited use when applied to the organizational structures of the community, and their day-to-day tasks. The comments further suggest that efforts on the part of policy makers to clarify roles and responsibilities at the organizational level to facilitate the implementation of IA initiatives would be well received, as would requests for suggestions about the process at the operational level. The comments also indicated that that a lack of "low level" policy was leading to the creation of multiple concurrent and possibly inconsistent policies with respect to the delineation of varying roles and responsibilities. It was suggested that such situations should and could be addressed by undertaking a more comprehensive and wide-ranging policy effort. A related undercurrent in the comments, was the expressed desire for the IA community to begin to think and act across organizational lines and to coordinate efforts and hare information.

Respondents also suggested that policy formulation difficulties might stem from the incremental nature by which DoD develops IA policy. Which contributes to the "patchwork" of polices currently in use. This policy "incrementalism" is perceived as a barrier to timely updates, which would allow policy to keep pace with developments in technology.

Many respondents expressed the belief that the visibility of IA in the PPBS cycle must be raised in order to assure that resourcing priorities are adequately addressed in the FYDP. These funding needs are further complicated by the great diversity of IA mission objectives as represented by the survey respondents. Respondents also expressed a desire to see further discussion in order to identify activities that support multiple missions and to harness domain knowledge in support of further policy and program development and implementation. This process will be invaluable in overcoming the inherent limitations of the PPBS too allow for the full identification and validation of IA requirements in the future.

Page 1083 of 3957

A final area of concern was the IAVA and accreditation processes. There was a general consensus that the feedback and reporting loop on the IAVA process needs to be tightened, leading to better and more timely communication. Additionally, many respondents felt that the accreditation process was both too complex, and too "paper intensive", leading to delays and frustration.

Overall, the comments indicate that the IA community is beginning to view itself as a functional community that cuts across organizational lines. There is also a high level of awareness of the fact that many of the organizations are dependent on each other, as well as outside institutions, and, a broad sense of the need for better coordination and cooperation in the IA community.

4.0 CONCLUSION

The responses received to the questionnaire came from a broad cross section of IA organizations engaged across the full spectrum of IA missions. The respondents accurately reflect those organizations and components, which are charged with the primary responsibility of implementing IA programs across the DoD. The questionnaire results support the proposition that IA is becoming instantiated across all functional areas of DoD, and that while high level policy is adequate, significant work remains to be done to assure that the broad goals and objectives of DoD policy are accurately translated into usable polices at the operational level. Front line IA personnel must be provided with sufficient organizational tools and resources to competently implement their IA missions on a day to day basis. Furthermore, policy must keep pace with technology, developed and implemented in a consistent manner across the various organizations that comprise the IA community. This becomes especially crucial as the demand for IA services continues to evolve into an important element of each Component's activities.

Page 1084 of 3957

Attachment A: Noted Trends in Respondents' Comments

Unclear and Outdated Guidance from Above

We write the IA policy for the AF, however, we do not always get clear policy/guidance from OSD.

There is too much policy that is not related to performing the functions required to do the job. The problem is the incremental adding of policy over the years. We need to throw it all out and start over.

DA IA Policy needs further clarification on roles and responsibilities. Typical, rapid technology change places us in the position of not always having desired information on hand for decisions.

Adequate & clear IA policy/guidance from above - NO - as an example, there is still no clear authoritative reporting policy from JCS on IA incidents.

There are various policies out there but the focus is still at the highest (DOD) levels. The personnel putting these policies into action, need more clarity to carry out this mission.

Although large strides are being made in regard to IA/CND policies, policy is not keeping up with the speed of technology. A paradigm shift is necessary to ensure that security policy is addressed in a more timely manner.

Policy is still being formulated from the national level on down. It seems to be mile wide and inch deep. Much improvement has been made in the last two years.

Several IA policy documents are old/out of date (e.g. DODD 5200.28, Public Law 100-235, DOD 5200.28-STD (Orange Book), etc).

IA policy which addresses Certification and Accreditation (DODI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP)) is difficult to understand and use. It expanded the process via required steps and paperwork, with vague guidance. Recommend Interim Authority to Operate be allowed at completion of Phase I vice Phase III.

Question 6: IA policy between DoD and the separate services sometimes parallels or conflicts, particularly in locations where there are multiple policy makers.

Little Authority over Subordinates/Organizations

Have NO authority over service component organizations - they have their own reporting lines - the Title 10 issue all over again.

Page 1085 of 3957

As a CINC who must respond for their respective Components, we have little say when the reporting structure and infrastructure is based upon a Service-centric model. That's why we face difficulties with the real C2 of the networks, as evidenced with disparities in INFOCON levels, as just one example.

The IA organization at DSS has no real authority over subordinates/organization. IA's role is more an advisory/oversight function without true authority to control systems or system owners.

Limited Financial Resources

We are not funded adequately for that protection to be maximized to the extent necessary to protect our infrastructure. Our CO is very supportive but funding limits and sets our priorities.

NCIS is currently not funded for this mission. We have made extraordinary strides in meeting this challenge, which are not being replicated within DoD, and are maximizing the limited resources we have.

While there is guidance from above with respect to IA policy/guidance, limited resources constrain programs to a (illegible) that could be deemed unacceptable. There are several DoD mandates that DSS is not in compliance with.

A strong commitment of "resources" and "will" is required by leadership at all levels to be the warfighter's IA agency of choice!

Limited Human Resources

Finding qualified people is difficult, more so on the GS side than on the contractor side.

Accreditation is a big obstacle for us because we have so many systems and so few people.

Suggestions for Change

IA should be budgeted as a separate program to ensure you get the required resources (personnel, training and tools).

I recommend having an area IA assigned to an IG area that provides full time support and overwatch to all IG offices within a pre-determined geographic location / area support. Responsibility for all IG offices within the assigned sector or geographic locations.

Page 1086 of 3957

Page 1087 of 3957

Attachment B: Organization's Coordination and Interface

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
Air Force	AFCIC	All Air Staff functionals; OSD, Joint Staff, NSA, DISA, DIA, IC, Army, Navy, USMC, MAJOR COMMANDS, JTF-CND, CINCs, NSTISSC,	Various government contractors	All of the above.
Army	DAIG	None.	None.	DAIG, V Corps, 3d Corps Support Command
Army	Office of Inspector General-West Point	DAIG, DoDIG, OSC	None	DAIG, DoDIG, OSC
Army	n/a	JCAHO (Joint Commission on Accreditation of Healthcare Organizations)	Japanese Healthcare System, US Healthcare Insurance Firs	TIMPO (Tri-Service Information Management Program Office), DoD Health Affairs, USAMISSA, TMSCC
Army	DISC-4	NSA, DISA, ASD C3I, DCSPS, DCSINT, CECOM, ISEC, NSSTISIC	ISS, STS, Sytec, GSA, Mitre	NSA, CECOM, ISEC
Army	n/a		NAI, ISS, Harris Corp Smartforce	
Army	DISC-4	Assistant Secretary of Defense for C3I, National Security Agency, Defense Information Systems Agency, US Air Force, US Navy, US Marine Corps, Defense Intelligence Agency, General Services Agency, National Institute of Standards and Technology, Joint Staff		National Security Agency, National Institute of Standards and Technology, Defense Information Systems Agency, Joint Staff
Army	n/a	DISA CID, MI (CI), NSA	CERT (Carnegie Melon)	MI, NIPC, JICPAC (USCINCPAC), DISA
Army	Space and Information Superiority Directorate	None	MPRI; Mitre; TAMSCO; COLEMAN Research and others	TRADOC Schools and Centers; CECOM; DISC4; DISA; ARL/SLAD; ATEC; and others

Page 1087 of 3957

Page 1088 of 3957

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
Army	n/a	Microsoft and other software vendors.	Services and Products contractors	Microsoft, DISA Cert, ACERT
Army	n/a	USAFE, NAVEUR, DISA, DISC4, ASC, EUCOM, NATO, CND JTF, LIWA ACERT-CC, 202nd MP Group (CID)	Cisco, ISS, Network Associates, Symantec, Microsoft	Army Signal Command, DISC4, EUCOM, USAFE, NAVEUR, USAREUR, LIWA, DAMO-ODI
Army	Field Security Operations	DISC4, PEO STAMIS, PEO GCSS, PEO AMD, PEO AVIATION, PEO IEW&S, CECOM, DARPA, LIWA, ASC, NSA,	IEEE, SANS, AFCEA,	All of the above
Army	n/a	Members of Federal CIO Council, and subordinate offices of the members.	Most any company in the US.	ASD(C3I), DoD Defense Information Assurance Program.
Army	SAF/IG	INS, Official Passport Office, DFAS-Charleston and Denver ETC.		7th ATC, USAREUR and DAIG
Army	n/a	ANSOC, ACERT, CIAC, MEDCOM, TRICARE, OSD HA, ANSOC	NORTN AND MCAFEE, GOVERNMENT COMPUTER NEWS, FEDERAL COMPUTER WEEK, INFORMATION SECURITY, CHIPS	ACERT, MEDCOM, OSD HA, CIAC, TRICARE, NARMC MEDDACS
Army	SAF/IG			
Army	DISC4		Vendors providing IA products and services	DoD ASD C3I, CECOM, ARL, ASC, LIWA
Army	n/a	EUCOM, DISA, USAFE, MARFOR-Europe, NAVFOR-Europe, ACERT	None	EUCOM, DISA, USAFE, MARFOR-Europe, NAVFOR-Europe, ACERT, Army RCERTs, AFWIC, SHADOW
Army	RCERT-E		ISS	ARIN, RIPE
Army	n/a	congress (rarely), FBI, CIA, NSA	Sun Systems, MicroSoft	too far down the org. to respond
Army	n/a	U.S. Air Force, U.S. Navy,	Microsoft, Remedy,	ACERT,
Army	n/a			
Army	n/a	VA	numerous contractors	MEDCOM
Army	DAIG	White House, Congress, Justice Department,	Various vendors (Microsoft, CISCO, 3COM, etc.)	DISA, ANSOC, DISC4 and installation DOIMs
Army	SAF/IG			DAIG IRMD Fort Campbell DOIM
Army	DISC4		We interface on a routine basis with vendors. Many vendors are selling their products. Other vendors hold IA tool contracts.	NSA for EAL standards -- Army CERT -- Army Signal Command (ASC) theater Network Operation Centers (NOC) -- Army Regional CERTs -- JTF-CND.

Page 1088 of 3957

Page 1089 of 3957

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
Army	n/a	NIST, NAVCIRT, AFCIRT, NSA, DISA, ARMY DOIM, ARMY PORTAL, CIO IA TEAM, USAPA, USASC IASE, DTIC	Computer Science Institute, SAN, MICROSOFT, ISC2, Rootshell, ICSA, IEBT	Computer Science Institute, SAN MICROSOFT, Rootshell, security focus, whitehats, antionline
Army	SAM	Defense Information Systems Agency (DISA), Air Force Pentagon Communications Agency (AFPCA), Army Information Management Support Center (IMCEN), Office of the Secretary of Defense, Information Technology Directorate (OSD/ITD), Department of the Navy, Info	Major Network Vendors, i.e., Cisco, Cabletron, Alcatel,etc., Major Information Technology Consultants, i.e., Gartner Group, MITRE, etc.	Defense Information Systems Agency (DISA), Air Force Pentagon Communications Agency (AFPCA), Army Information Management Support Center (IMCEN), Office of the Secretary of Defense, Information Technology Directorate (OSD/ITD), Department of the Navy, Info
Army	SAF/IG			
BMDO	OSD/BMDO	DTRA, DARPA, ARMY, NAVY, Air Force, Marine Corps, DISA, DIAP, OSD (A&T), OSD(C3I), Air Force Office of Special Investigations, Army 902nd Military Intelligence, NSWC Dahlgren, foreign security offices for some programs	IETF, ASIS, and AFCEA	All the ones we interface with are in some ways supporting us.
DISA	DISA	OSD, Joint Staff, CINCs, Services, Agencies, Law Enforcement, Intel Community, NATO, NCS	IT community in general and academia	MITRE, ROME Labs, DARPA, Lawrence Livermore, Carnegie Melon, NSIRC, NIST
DISA	DISA-EUR-RCERT	Regional CERTS in the EUCOM AOR IA representatives from the components in the AOR, EUCOM IA division	Training organizations	HQ DISA
DISA	n/a	NSA, ALL CINCs, GAO	EDS, SAIC, CSC	NSA
DISA	DISA-PAC	FBI, NCIS, NSA, NRO	SANS, Carnegie Mellon, Symantec, MacAfee	DoD-CERT, Regional CERTS, Component CERTS/CIRTS
DISA	DISA-SCOTT-RCERT	NIPC, USJFCOM, USCENTCOM, USSOCOM, USSOUTHCOM, USSTRATCOM, USTRANSCOM, PAC-CERT, EUR-CERT, COL-CERT, CENT-CERT	CERT/CC, SYMANTEC, MACAFEE, SANS, ARIN, RIPE, APNIC	JTF-CND, DOD-CERT, GNOSC FSO
DSS	n/a	See faxed document, "All Agencies with DCII Access". Ask W. Lozano to fax it (lozanw@sainc.com)	Over 2,000 industrial organizations.	Air Force, Army, Navy, Marines, DoD agencies (C3, Policy, Comptroller, General Counsel, Washington HQ Services), DLA, DSW, DISA VA, GSAFEDSIM, OPM, State Department, FBI, CIA, NSA, INS, etc.

Page 1089 of 3957

Page 1090 of 3957

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
EUCOM	n/a	NATO, NSA, State Department	BAH, PRC, ManTech, Motorola, GTE	IATAC, DISA, NSA
Joint Staff	J6K	most of this survey not applicable because the joint staff - J6 does not do some of the items listed above. We interface with nearly all IA orgs within the govt	msoft and most IA vendors	Services, CINCs, Agencies,
Lincoln Labs	n/a	DARPA, AF (AFRL, AF/ESC, AFIWC, Army (Cecom), NSA, FAA, NIST	BBN, Boeing, Telecordia, SRI, RST, Honeywell, SAIC	SEI/CERT, Sandia
Marines	n/a	FBI, NIPC, NSA, CIA, DIA, DISA, NIST, IOTC, JOIC	Carnegie Mellon University, ISS, Symantec, Macaffee, ICSA, CIS, ISSA, IACSS, NCSA, MICROSOFT, Timestep, Dell, Compaq, IBM,	ITFF, AFCEA, ISC2, ISO, IEEE, ANSI, USENET
Navy	NCTAMS	SPAWAR SAN DIEGO, SPAWARSYSCEN CHARLESTON SC, COMNAVCOMTELCOM WASH DC, EUCOM, DISA EUR, NATO, JTF, CNE	SAIC, BBN, CISCO, CABLETRON, DELL CORP, GATEWAY CORP.	SPAWAR SAN DIEGO, SPAWARSYSCEN CHARLESTON SC, SAIC, BBN, DISE EUR
Navy	NCTAMS LANT	CINCLANTFLT AFLOAT AND ASHORE COMMANDS, SPAWAR, CNO, CNCTC, NCTF-CND, FIWC, DCMS, COMANAVBASE, NAVY MID-ATLANTIC REGIONAL COMMANDER, NAVMETOC, JOINT BATTLE CENTER/JTASC, JFCOM, PSD, BUPERS, FISC, CNET, COMNAVTRAGRU, NCIS, DSS, DISA	BOOZ-ALLEN-HAMILITON, SAIC, TDS, LUCENT	CNO, FIWC, SPAWAR, CINCLANTFLT, CNET, NCTF-CND, NCTC, NCIS, DSS, DISA
Navy	NCTAMS PAC			
Navy	OPNAV-N6	DON CIO ; Chief of Naval Operations (CNO); BUPERS; Flt CINCs; Navy Component Task Force-Computer Network Defense (NCTF-CND); Fleet Information Warfare Center (FIWC); Naval Space Command; Space & Naval Warfare Systems Command (SPAWAR); NAV COMPT; NCT		CNO FIWC, NCTF-CND, SPAWAR, NCTAMS EURCENT, NCTAMS LANT, and NCTAMS PAC

Page 1090 of 3957

Page 1091 of 3957

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
Navy	SAF/IG	Defense Criminal Investigative Organizations, Defense Computer Investigations Training Program, DCFL, FBI, NSA, CIA, USSS, DOE, NIPC, JTF-CND, State and Local Law Enforcement, US Dept. of Justice, Various International Law Enforcement Agencies.	Numerous/varied - depending upon investigative requirements	See 10A
Navy	NAVIG			
Navy	NCTAMS PAC	OSD C3I, JS J39/J6, MCEB, IAP, DIAP, JTF-CND, NCTF-CND, DODCERT, service CERTs, NCIS, CINCSPACE, IC CMS, NSA		Same as 'a'
Navy	DONCIO	Federal CIO Council, Federal PKI Steering Committee, NIST, NSA, GSA, GAO, DoD CIO Executive Board, DISA, DLA, DFAS, JECPO, DoD Access Card Office, Other Military Departments, OSD, Joint Staff, OMB, NIPC, US SPACECOM, Treasury, State	Banking Information Technology Secretariat (BITS), RSA, AFCEA	OSD, NSA, FFRDCs, Industry Academia, Joint PMEs, Sandia Laboratories, Gartner Group et al.
NSA	IOTC	National Intelligence Agencies (NSA, CIA, DIA, NIMA, DISA, etc.), Unified Commands, Services (Army, Navy, Air Force, Marine Corps), OSD, DCI.	No direct interface with external industry organizations.	National Intelligence Agencies (NSA, CIA, DIA, NIMA, DISA, etc.), Unified Commands, Services (Army, Navy, Air Force, Marine Corps), OSD, DCI.
NSA	NSA-ISSO	JTF-CND, SPACECOM, NIPC, Other CINCs, Service Certs, NSTISSC members GSA, DTRA, OSD, DISA, NRO	Mitre, CMU-SEI, Cert-CC, SANS and support contractors	NSTISSC members, NIPC, JTF_CND, Service CERTS, etc
OSD	OSD/BMDO	None	None	DoD WHS, C3I ITD
SOCOM	SOCOM-J6	JTF-CND, DISA GNOSC, DoD CERT, Scott RNOSC, other C/S/As, NIPC, NSA, DIA, DISA, JIOC, US Army CECOM, SPAWAR,	Carnegie-Mellon CERT, SANS, CSI,	JTF-CND, USSPACECOM, DISA, NSA,
SOCOM	Army Special Operations Command	ANSOC, ACERT, HQDA, AFSOC, NAVSOC, JSOC, USSOCOM, NSA, NAVCIRT,		Listed in Item A

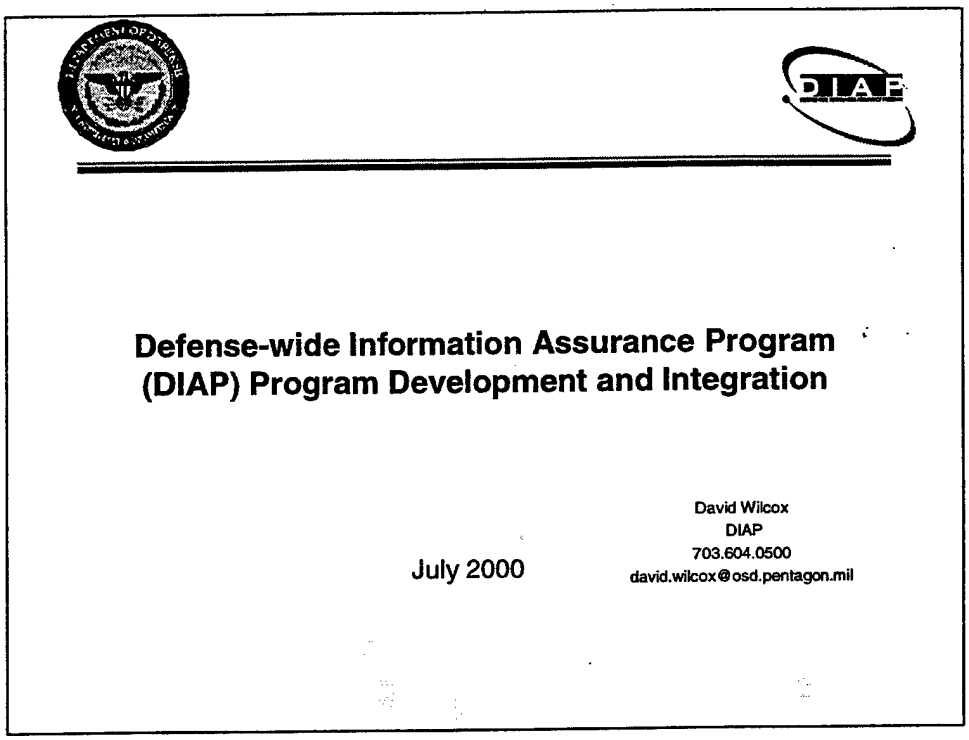
Page 1091 of 3957

Page 1092 of 3957

Component	Unit Acronym	Government Interface	External Industry Interface	Organizational Support
SPACECOM	SPACECOM- J2	USCINCJFCOM NORFOLK VA//J2//, USCINCPAC HONOLULU HI//J2/, USCINCSOC MACDILL AFB FL//J2//, USCINCEUR VAIHINGEN GE//ECJ2//, USCINCTRANS SCOTT AFB IL//J2//, USCINCSTAT OFFUTT AFB NE//J2//, USCINCCENT MACDILL AFB FL//CCJ2//, USCINCSO MIAMI FL//DR/J2//, USCIN		same as 10(a).
STRATCOM	STRATCOM-J3	DISA, NSA, DIA, CERTs, JTF-CND, CINCs, JIOC, AFIWC, IOTC, Services	Various S/W vendors: Symantec, Norton, & Microsoft	DISA, NSA, DIA, CERTs, JTF-CND, CINCs, JIOC, AFIWC, IOTC, Services

Page 1092 of 3957

APPENDIX E. DIAP PROGRAM DEVELOPMENT AND INTEGRATION TEAM (PDIT) BRIEFING



Defense-wide Information Assurance Program (DIAP) Program Development and Integration

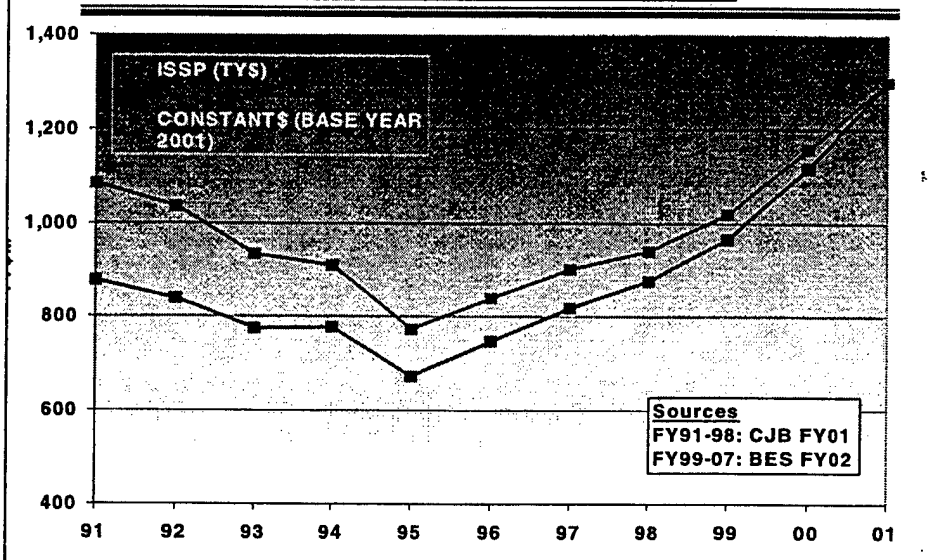
July 2000

David Wilcox
DIAP
703.604.0500
david.wilcox@osd.pentagon.mil

- How much is the DoD spending on IA?
- How much does a pound of IA cost?
- What is the real IA requirement?

What We Know ($M)

HISTORICAL TREND OF ISSP RESOURCES

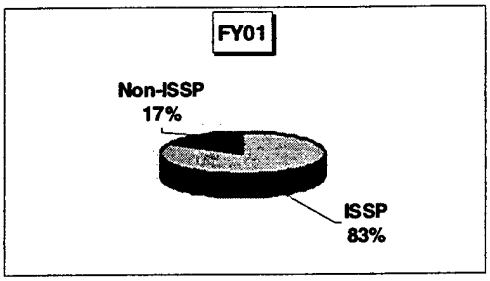


What We Don't Know

- IA costs embedded within acquisition programs/initiatives
- IC Community
- Services use post, camp, station/base operating support funds for IA
- DOD law enforcement (computer crimes, computer forensic lab)

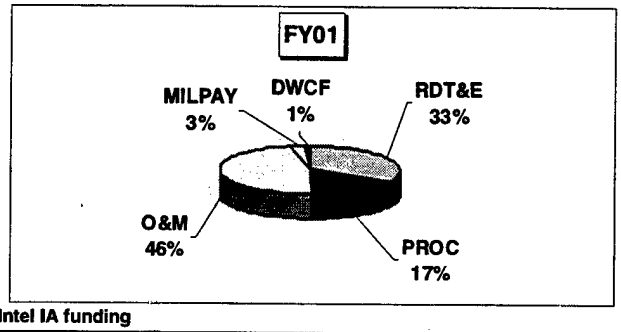
What We Know ($M)

Program	FY99	FY00	FY01
ISSP	966.0	1,115.9	1,299.5
Non-ISSP	113.6	185.9	269.5
TOTAL	1,079.6	1,301.8	1,569.0



What We Know ($M)*

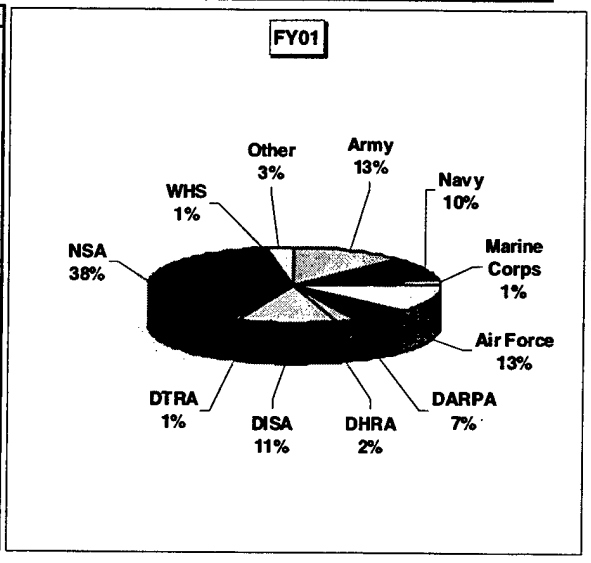
Appropriation Cat	FY99	FY00	FY01
RDT&E	392.4	405.0	517.7
PROC	178.1	226.3	263.7
O&M	462.8	611.6	725.2
MILPAY	42.6	44.7	45.8
DWCF	3.7	14.1	16.0
Surcharge	0.0	0.1	0.6
TOTAL	1,079.6	1,301.8	1,569.0



* Does not include Intel IA funding

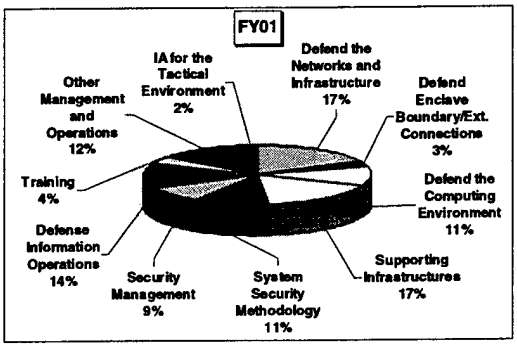
What We Know ($M)

Component	FY99	FY00	FY01
Army	113.4	142.0	196.2
Navy	93.7	140.2	161.4
Marine Corps		12.3	20.3
Air Force	116.8	134.3	196.5
BMDO		0.8	1.1
DARPA	77.7	97.5	105.5
DCAA		0.0	0.0
DCMA	2.1	4.1	4.0
DeCA		0.7	1.3
DFAS	1.3	2.5	5.0
DHP	1.7	4.8	6.4
DHRA		13.0	31.8
DIA	0.4	0.4	0.4
DISA	105.0	134.7	173.3
DLA	1.9	7.1	6.8
DSS	0.1	1.1	1.2
DTRA	4.0	6.3	9.4
NIMA		0.9	3.0
NSA	545.0	570.5	607.8
OIG	0.8	3.0	4.9
OSD	4.2	3.2	3.1
USSOCOM	2.0	2.9	6.6
USTC	0.4	2.7	2.3
WHS	9.4	16.7	20.8
TOTAL	1,079.6	1,301.8	1,569.0



What We Know ($M)

Defense-in-Depth Category	FY99	FY00	FY01
Defend the Networks and Infrastructure	282.3	238.8	282.6
Defend Enclave Boundary/External Connections	32.4	51.3	39.6
Defend the Computing Environment	64.4	135.4	168.9
Supporting Infrastructures	145.2	184.7	268.1
System Security Methodology	135.0	163.1	168.5
Security Management	96.1	118.3	137.7
Defense Information Operations	121.1	152.7	215.4
Training	41.4	49.7	64.0
Other Management and Operations	154.1	185.7	191.6
IA for the Tactical Environment	7.7	22.2	32.5
TOTAL	1,079.6	1,301.8	1,599.0



Industry IA Estimate

• 5% to 8% * of industry Information Technology spending should be Information Assurance.

- This observation is for network centric IT and does not take into account systems such as the DoD's Strategic and Tactical Weapons/Space Systems (i.e. GPS, NC2, NMD) nor IA Research and Development

• Applied to the DoD
- $267B Total DoD
- $ 15.8B DoD IT - (Avg. FY02-07)
- 5-8% = **$.8 - 1.3B**

* Source(s) Gartner Group, others

1997 DSB IW-D Recommendation 6.1

- Designate ASD(C3I) as the accountable focal point for all IW issues.
- Establish DASD(IW)

FY99	FY00	FY01
+5	+5	+5

July 2000 Update

OASD(C3I) Information Operations Strategy & Integration chartered as DoD focal point for IO

OASD(C3I)(I&IA) and DIAP Office focal point for IA

FY99	FY00	FY01
+1.5	+2.5	+ 2.6

For intel-related IA

FY99	FY00	FY01
unable to obtain associated resources		

1997 DSB IW-D Recommendation 6.2

- 6.2.1 **SECDEF request DCI to establish a Center for Intelligence Indications & Warning, Current intelligence, and Threat Assessment at NSA with CIA and DIA support**

FY99	FY00	FY01
+60	+35	+30

July 2000 Update

NSA's National Security Incident Response Center

FY99	FY00	FY01
2	2	2

Intelligence Resources

FY99	FY00	FY01
unable to obtain associated resources		

1997 DSB IW-D Recommendations 6.2.2 & 6.

- **6.2.2 Establish a Center for IW-D Operations**

FY99	FY00	FY01
+60	+60	+60

- **6.2.3 Establish a Center for IW-D Planning and Coordination**

FY99	FY00	FY01
+10	+10	+10

July 2000 Update

JTF CND / DISA GNOSC / DoD CERT

FY99	FY00	FY01
9.8	12.1	22.0

USCINCSPACE assumed CND role for DoD in Oct 1999

FY99	FY00	FY01
--	3.9	14.5

1997 DSB IW-D Recommendation 6.2.4

- **6.2.4 Establish a Joint Office for System, Network, and Infrastructure Design within DISA**

FY99	FY00	FY01
+55	+50	+50

July 2000 Update

OASD(C3I) Architecture & Interoperability Directorate established in 2000

FY99	FY00	FY01
-	~3.0	~3.1

DISA D6 Engineering & Interoperability/Joint Information Engineering Organization (JIEO)

FY99	FY00	FY01
unable to obtain associated resources		

NSA Information Assurance Technical Forum

FY99	FY00	FY01
5	3	3

Page 1099 of 3957

1997 DSB IW-D
Recommendation 6.2.4 (cont'd)

- **6.2.4 Establish a Joint Office for System, Network, and Infrastructure Design within DISA**

FY99	FY00	FY01
+55	+50	+50

July 2000 Update

Joint IA Architecture Working Group -- IA Info Exchange Requirements

FY99	FY00	FY01
-	<1.0	<1.0

DARPA Info Assurance and Survivability R&D Project

- Research efforts include fault tolerant and survivable network architecture development (*see Recommendation 6.9 for DARPA resources*)

1997 DSB IW-D
Recommendation 6.3

- **Increase Awareness**
  - Establish IW-D awareness campaign for public, industry, CINCs, Services, Agencies
  - Expand IW Net Assessment in 1994 Summer Study
  - Review Joint Doctrine for IW-D Emphasis
  - Large scale IW-D demos, understand cascading effects
  - Develop simulations to demonstrate IW-D effects
  - Implement Policy to include IW-D realism in exercises

FY99	FY00	FY01
+85	+135	+135

July 2000 Update

See next 3 slides for update

Page 1100 of 3957

1997 DSB IW-D
Recommendation 6.3 (cont'd)

- **Increase Awareness**
  - Establish IW-D awareness campaign for public, industry, CINCs, Services, Agencies

July 2000 Update

IA awareness raised to highest levels throughout DoD
- DepSecDef strong IA proponent
- OASD(C3I)(I&IA) and DIAP active advocates of IA
- Eligible Receiver 97 demonstrated IA impact on operations
- Continuous series of attacks/probes on DoD networks
- USSPACECOM assigned CND/CNA operational mission
- Quality and degree of DoD IA Training/awareness significantly raised
- DoD and Services have "IA Awareness" days and conferences
- Awareness processes exist that engage with industry and academia

FY99	FY00	FY01
14	16	19

1997 DSB IW-D
Recommendation 6.3 (cont'd)

- **Increase Awareness**
  - Expand IW Net Assessment in 1994 Summer Study
  - Review Joint Doctrine for IW-D Emphasis
  - Large scale IW-D demos, understand cascading effects

July 2000 Update

Status and efforts to expand 1994 IW Net Assessment are unknown

OASD(C3I)(Info Ops Strategy & Integration)
- Conducting IO Broad Area Review with DoD Components, including IA
- Services and JS, in conjunction with IO review, are reviewing IO and IA doctrine

Joint Warrior Interoperability Demonstration (JWID)
- Ongoing right now, some IA technologies to be demonstrated

Page 1101 of 3957

1997 DSB IW-D
Recommendation 6.3 (cont'd)

- **Increase Awareness**
  - Develop simulations to demonstrate IW-D effects
  - Implement Policy to include IW-D realism in exercises

July 2000 Update

Components have some modeling and simulation efforts to demonstrate IA effects and to collect data. Most of these efforts reside at NSA

JS is staffing CJCSI 6510.01 to:
- include integration of CND (IA) into joint exercises and wargames
- instruct components to exercise CND in realistic scenarios
- task J7 to ensure IA and CND operations are exercised and coordinated

Components are implementing IA (to varying degrees) into exercises
- INFOCON 99, Blue Flag 00-2, 00-3, UFL, Steel Puma, Power Sweep...

1997 DSB IW-D
Recommendation 6.4

- **Assess Infrastructure Dependencies and Vulnerabilities**

prior FY99	FY99	FY00	FY01
+90	+0	+0	+0

July 2000 Update

DoD Critical Infrastructure Protection (CIP)

CIP Office with staff of nine

FY99	FY00	FY01
<1	<1	<1

CIP Analysis and Assessments

Joint Program Office Special Technologies Countermeasure (Navy)

FY99	FY00	FY01
14	14	14

Balanced Survivability Assessments (DTRA)

FY99	FY00	FY01
-	-	10

ASD(C3I) Y2K/CIP

FY99	FY00	FY01
20	-	-

Page 1102 of 3957

1997 DSB IW-D

Recommendation 6.5

- **Define Threat Conditions and Responses**

FY99	FY00	FY01
+0	+0	+0

July 2000 Update

INFOCONs
- VJCS signed memo March 10, 1999 on INFOCON procedures and policy
- JS revising CJCSM 6510.01 to include INFOCON, hopefully this Fall

1997 DSB IW-D

Recommendation 6.6

- **Assess IW-D Readiness**
  - Establish standardized readiness assessment system
  - Incorporate IW preparedness assessments in Joint Reporting systems and Joint Doctrine

FY99	FY00	FY01

July 2000 Update

CJCSI 6510.04 *IA Readiness Metrics* issued May 15, 2000
- Provides standardized IA metrics and supplemental policy IA guidance to support DoD components self-assessment of IA status for consideration in Joint Monthly Readiness Report (JMRRs)
- Future guidance/policy on incorporation into SORTS type reports is under consideration

Page 1103 of 3957

1997 DSB IW-D
Recommendation 6.7

- **"Raise the Bar" with high-payoff, low-cost items**
  - Improve access control (get rid of fixed passwords)
  - Identification and authentication
  - Examine products, use approved products

FY99	FY00	FY01
+10	+10	+10

July 2000 Update

DoD Public Key Infrastructure program (managed by NSA)

FY99	FY00	FY01
20	56	127

Enabling of applications to utilize a public key infrastructure
- PKE to be resourced from components' programs
- PKE study estimates total resources to PK-Enable 690 applications will be around $175M

National Information Assurance Partnership (NIAP)

FY99	FY00	FY01
3	7	4

1997 DSB IW-D
Recommendation 6.8

- **Establish and maintain a minimum essential information infrastructure**
  - Define options with associated costs and schedules to determine MEII such that infrastructures can failsoft to support critical functions while under attack
  - Define minimum essential conventional *force structure* and supporting *information infrastructure* needs
  - Prioritize critical functions and infrastructure dependencies
  - Design a Defense MEII and a failsafe restoration capability
  - Direct Components to fence funds for Defense MEII and restoration capability

FY99	FY00	FY01
+100	+100	+100

July 2000 Update

Separate & limited efforts ongoing to define MEII.
- CIP office analyzes defense sectors and identify MEIIs, but not all.
- OASD(C3I) is working to define supporting info infrastructure.
- The National Security Telecommunications Advisory Committee (NSTAC) coordinates with industry to assess telecommunications interdependencies for Governmental critical mission operations and may address MEIIs.

Page 1104 of 3957

1997 DSB IW-D
Recommendation 6.9

- **Focus the R&D on following areas:**
  - Robust survivable system architectures
  - Techniques and tools to model large scale distributed network systems
  - Tools for synthesizing & projecting performance of survivable distributed systems
  - Testbeds and simulation-based mechanisms for evaluation of emerging technologies
  - Research in US Computer science and engineering programs
  - Educational programs for curriculum development at undergrad and graduate levels

FY99	FY00	FY01
+125	+160	+160

July 2000 Update

See next slide for update

1997 DSB IW-D
Recommendation 6.9 (cont'd)

- **Focus the R&D effort**

FY99	FY00	FY01
+125	+160	+160

July 2000 Update

NSA IA Research and Development

FY99	FY00	FY01
49	57	60

DARPA Info Assurance and Survivability R&D Project

FY99	FY00	FY01
78	99	115

Page 1105 of 3957

1997 DSB IW-D
Recommendation 6.10

- **Staff for Success**
  - Establish career paths, training & certification of systems administrators
  - Establish a skill specialty for IW-D
  - Develop specific IW awareness courses with focus on DoD's professional schools

FY99	FY00	FY01
+55	+50	+50

July 2000 Update

IA mobile training teams

DoD wide training and certification of military, civilian, and contractor:
- IS Administrator/Security Manager/Security Officer
- IS Professional technician

FY99	FY00	FY01
18	24	26

IA & IT Training, Certification, and Personnel Management Report
- With DEPSECDEF for review and signature
- Estimates $77.5M over FYDP to implement all recommendations

What We Should Know

- DOD's total IA resources
- What it buys us
  - Risk return on investment
- What is the total requirement

Page 1106 of 3957

APPENDIX F. ACRONYMS

AFIWC	Air Force Information Warfare Command
BIOSG	Bilateral IO Steering Group
CERTs/CIRTs	Computer Emergency or Incident Response Teams
CIP	Critical Infrastructure Protection
CJCS	Chairman of Joint Chiefs of Staff
CNA	Computer Network Attack
CND	Computer Network Defense
COMSEC	Communications Security
CONOPS	Concepts of Operations
COOP	Continuity of Operations Plan
COP	Common Operational Picture
CORT	Cyber Operations Readiness Triad
DepSecDef	Deputy Secretary of Defense
DIAP	Defense-wide Information Assurance Program
DIO	Defensive Information Operations
DoD	Department of Defense
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
ETA	Education Training and Awareness
ETS	Education and Training for Service
FEA	Front End Assessments
FIWC	Fleet Information Warfare Command

Page 1107 of 3957

FOC	Full Operational Capability
GAO	Government Accounting Office
GCCS	Global Command and Control System's
GIG	Global Information Grid
GNOSC	Global Network Operations and Security Center
IA	Information Assurance
G&PM	Guidance & Policy Memo
IA/IT HR IPT	Information Assurance/Information Technology Human Resources Integrated Process Team
IC	Intelligence Community
IDM	Information Dissemination Management
IO/IA/CIP	Information Operations, Information Assurance, and Critical Infrastructure Protection
IPT	Integrated Process Team
ISSP	Information Systems Security Program
I&W	Indications and Warning
JMRR	Joint Mission Readiness Review
JPO-STC	Joint Program Office for Special Technology Countermeasures
JRDC	Joint Requirements Oversight Council
JTF-CND	Joint Task Force-Computer Network Defense
JTS	Joint Training System
MCB	Marine Corps Base
NETOPS	Network Operations
NOIWON	National Operations and Intelligence Watch Officer Network

Page 1108 of 3957

NORAD	North American Air (later) Aerospace Defense Command
NSTISSC	National Security Telecommunications and Information Systems Security Committee
OMB	Office of Management & Budget
OPM	Office of Personnel Management
ORA	Operational Readiness Assessment
OT&E	Operational Test and Evaluation
PA&E	Program Analysis and Evaluation
PE	Program Element
PPBS	Planning Program and Budgeting System
PRG	Program Reviews
RC	Reserve Component
RDT&E	Research Development Test and Evaluation
ROE	Rules of Engagement
R&D	Research & Development
SecDef/OSD	Secretary of Defense/Office of the Secretary of Defense
SBU	Sensitive-but-Unclassified
SOP's	Standard Operating Procedures
TCCC	Theater C4 Coordination Center
TPI	Two-person Integrity
TTP	Tools, Tactics, Techniques, Procedures
USCINCSPACE	Commander in Chief, U.S. Space Command
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology & Logistics

Page 1109 of 3957

USD(P)	Under Secretary of Defense Policy
USMC	United States Marine Corps
VA	Vulnerability Assessment
VE	Vulnerability Evaluation
WMD	Weapons of Mass Destruction

Page 1110 of 3957

ANNEX D

Defense Science Board Task Force
on
Defensive Information Operations

Panel Report on Policy Implications

REPORT OF FINDINGS, DISCUSSION/OBSERVATIONS AND RECOMMENDATIONS

TABLE OF CONTENTS

Executive Summary 1
1. Low Entry Cost 2
2. Blurred Traditional Boundaries 2
3. Expanded Role For Perception Management 2
4. Lack Of Strategic Intelligence 3
5. Difficulty Of Tactical Warning And Attack Assessment 3
6. Difficulty In Building And Sustaining Coalitions 3
7. Vulnerability of the United States Homeland 3
Conclusions 6

I. Toward a Common Terminology 7
Findings 7

II. Requirement for Government-Wide Coordination 9
Findings 11

III. Critical Infrastructure Protection 13
Findings 15

VI. Security Standards 17
Findings 19

Appendix A. Acronyms 21

Annex B. Panel Membership 23

Page 1112 of 3957

Page 1113 of 3957

EXECUTIVE SUMMARY

"We can't solve problems by using the same kind of thinking we used when we created them."

Albert Einstein

The American homeland is becoming increasingly vulnerable to non-traditional attack, including information warfare, the focus of this report. Rapid advances in technology have and will continue to create new vulnerabilities and challenges to U.S. security. Recent studies by both the Government Accounting Office (GAO) and the Computer Security Institute found that the number of cyber security threats to both the government and the private sector is on the rise. The damage caused by a successful attack, both to physical infrastructures and to the psychological health of U.S. institutions, could prove immense, and the Department of Defense is not exempt from this danger.

In many circles within the U.S. defense and broader international security community, the term "information warfare" is increasingly being used to encompass a far greater set of information-age "warfare" concepts than was attributed to it in the past. These emerging new warfare concepts are directly tied to the prospect that the ongoing rapid evolution of cyberspace, the global information infrastructure, could bring both new opportunities and new vulnerabilities. At least one of these vulnerabilities, the prospect that the information revolution could put at risk high-value national assets outside the traditional battlespace boundaries, will affect U.S. national security strategy, and thus U.S. military strategy. The fact that assets that are critical to the conduct of military operations would also be put at risk compounds this problem.

There is an emerging element of information warfare, one that appears to be common to almost all currently evolving uses of the term, which warrants identification and definition. Strategic information warfare, in essence, the intersection of evolving information warfare and post-cold war "strategic warfare" concepts, warrants special recognition and attention as a legitimate new facet of warfare, one with profound implications for both U.S. military strategy as well as overall U.S. national security strategy and policy.

A fundamental aspect of strategic information warfare is that *there is no front line*. Strategic targets in the United States may be just as vulnerable to attack as in-theater command, control, communications, and intelligence targets. As a result, there exists a need for broadening strategic understanding beyond the single traditional regional theater of operations to four distinct separate theaters of operation: 1) the battlefield, 2) the allied or regional zone of the interior, 3) the intercontinental zone of communication and deployment, and 4) the U.S. zone of the interior.

The post-cold war "*over there*" focus contained in the persistent emphasis on the regional component of U.S. military strategy has been rendered incomplete and is of declining relevance to the likely future international strategic environment. When responding to information warfare attacks of this character, military strategy can no longer afford to focus on conducting and supporting operations only in a region of concern.

Page 1114 of 3957

What are the basic features of strategic information warfare as best we understand them today? The following represent a synthesis of observations about these basic features. There is, most definitely, a cascading effect inherent in these observations; each helps to create the enabling conditions for subsequent ones.

1. Low Entry Cost

Interconnected networks may be subject to attack and disruption not just by states but also by non-state actors, including dispersed groups and even individuals due to the low cost of entry. Potential adversaries could also possess a wide range of capabilities. Thus, the threat to U.S. interests could be multiplied substantially and will continue to change as ever more complex systems are developed and requisite expertise is ever more widely diffused.

Cyber attacks have moved beyond the realm of the mischievous teenager and are now being learned and used by terrorist organizations as the latest weapon in a nation's arsenal. In June 1998 and February 1999, the Director of the Central Intelligence Agency testified before Congress that several terrorist organizations believed information warfare to be a low-cost opportunity to support their causes. Both *Presidential Decision Directive 63* (PDD-63) issued in May 1998 and the *President's National Plan for Information Systems Protection*, version 1.0, issued in January 2000, call on the legislative branch to build the necessary framework to encourage information sharing to address cyber security threats to our nation's privately held critical infrastructure.[1]

Effective attribution and swift response to attacks would nullify the appeal of the low cost of entry by making the chances of "getting caught" much higher. Perceived increased risk by the attacker should be an added deterrent to preventing information warfare attacks.

2. Blurred Traditional Boundaries

Given the wide array of possible opponents, weapons, and strategies, it becomes increasingly difficult to distinguish between foreign and domestic sources of information warfare threats and actions. We may not know who is under attack by whom, or who is in charge of the attack. This greatly complicates the traditional role distinction between domestic law enforcement, on the one hand, and national security and intelligence entities on the other.

Not only are borders becoming more porous, but they are increasingly irrelevant in cyberspace. According to a long-time CIA operative and FBI consultant, "Globalization and technology were lowering traditional boundaries between what constitutes an international or domestic threat, and terrorists, drug cartels, spies, and hackers were all leaping those boundaries with impunity."[2]

3. Expanded Role For Perception Management

Opportunities for information warfare agents to manipulate information that is essential to public perceptions may increase. For example, political action groups and other non-government organizations can use the Internet to galvanize political support, as the Zapitistas in Chiapas,

---

1 Statement of Representative Tom Davis on the Introduction of The Cyber Security Information Act of 2000, April 12, 2000.

2 John McGaffin, in Covert Counterattack, by James Kitfield, National Journal, September 16, 2000, pg. 2858.

Mexico, were able to do. Furthermore, the possibility arises that the very "facts" of an event can be manipulated via multimedia techniques and widely disseminated. Conversely, there may be decreased capability to build and maintain domestic support for controversial political actions. One clear implication is that future U.S. administrations may include a robust Internet component as part of any public information campaign.

4. Lack Of Strategic Intelligence

For a variety of reasons, traditional intelligence-gathering and analysis methods will be of limited use in meeting the strategic information warfare challenge. Collection targets will be difficult to identify using existing national technical means; allocation of intelligence resources will be difficult because of the rapidly changing nature of the threat; and vulnerabilities as well as target sets will not be well understood. In sum, the United States may have great difficulty identifying potential adversaries, their intentions, and their capabilities.

5. Difficulty Of Tactical Warning And Attack Assessment

Warning and attack characterization and assessment involving information warfare presents fundamentally new problems in a cyberspace environment. A basic problem exists: distinguishing between attacks and other events such as accidents, system failures, or hacking by thrill seekers. This challenge is exacerbated by the speed of events in cyberspace. The main consequence of this feature is that the United States may not know when an attack is underway, who is attacking, or how the attack is being conducted.

6. Difficulty In Building And Sustaining Coalitions

Many allies and coalition partners will be vulnerable to information warfare attacks on their core information infrastructures. For example, the dependence on cellular phones in developing countries could well render telephone communications in those nations highly susceptible to disruption or deception. Other sectors in the early stages of exploiting the information revolution, such as the energy or financial sectors, may also present vulnerabilities that an adversary might attack to undermine coalition participation. Such attacks might also serve to sever weak links in the execution of coalition plans.

Conversely, tentative coalition partners who urgently need military assistance may want assurances that a United States deployment plan to their region is not vulnerable to information warfare disruption.

7. Vulnerability of the United States Homeland

As stated earlier, information warfare has no front line. Potential battlefields are anywhere networked systems allow access. Current trends suggest that the United States economy will rely on increasingly complex, interconnected network control systems for such necessities as oil and gas distribution management, electric grids, telephone service, air traffic control, and much, much more. The vulnerability of these systems is currently poorly understood. This lack of understanding and recognition inhibits a thorough assessment of the vulnerabilities that may exist in both the technology-driven control systems and in the fiscal marketing processes that can directly affect energy distribution. In addition, the means of deterrence and retaliation are uncertain and may rely on traditional military instruments in addition to information warfare

threats. In summary, the United States homeland may no longer provide a sanctuary from outside attack.

The U.S. concept of national security must adapt to this changing world. The existing national security decision-making and execution apparatus is not well suited to ensure this type of security. Among other things, the apparatus that is needed must be able to:

- Act quickly, avoiding the delays of inter-agency processes, yet represent appropriate concerns
- Deal with threats functionally instead of geographically
- Bring law enforcement, national defense, and intelligence functions to bear on a threat seamlessly without endangering civil liberties
- Engage with the private sector

Rebuilding the national security apparatus cannot be done in one step. The bipartisan Commission on National Security in the 21st Century has begun to address this problem. It must evolve and adapt as the world changes. The key will be to create a flexible, agile, adaptive apparatus that embraces experimentation and keeps what works.

In the interim, this panel submits a series of recommendations, grouped into four areas, the implementation of which would go a long way to meet the emerging information warfare threat. The panel believes that actions taken in the near term would materially benefit the effective execution of Defensive Information Operations (DIO) within the Department.

RECOMMENDATION 1

Create an Executive Order (EO) on Common DIO Terminology

Multiple definitions for the same DIO-related terms are in wide usage within DoD, DOJ, and the Intelligence Community (IC). The absence of common definitions produces differing interpretations of authorities and knee-jerk reactions in both the private sector and the legal community, e.g., monitoring, attack, armed attack, etc. This decreases the likelihood of coordination and increases the potential for confusion and turf battles. We believe the problem can be solved by using existing mechanisms without changing current laws, policies; and regulations. The recently signed Presidential Review Directive (PRD) will institute an Interagency Working Group (IWG) process that will help.

The SecDef and the Director of the Critical Infrastructure Assurance Office (CIAO) should jointly sponsor an effort to produce an authoritative document (perhaps an EO) containing the maximum number of DIO-related terms, which would be useful to Information Assurance (IA) in a national, DoD, civil agency, and civil context.

Page 1117 of 3957

RECOMMENDATION 2

Establish a National DIO Coordinator

The nation has no means of providing either tactical Indications and Warning (I&W) of a widespread cyber attack on critical infrastructures or a coordinated response to it. No one is assigned the clear responsibility for rationalizing law enforcement and national defense equities when a cyber attack is detected. There is currently a bias in favor of law enforcement procedures, even if their use impedes response and recovery. There is no governing authority with the responsibility to make response-and-recovery decisions effective across stovepipes. Moreover, coordination often depends on the personalities of those involved.

The SecDef should propose creation of a national DIO coordinator. Initial responsibilities and authorities would be limited to policy and planning, but would increase as the job matures and Congress engages, to potentially include: oversight, direction and control, responsibility for information resource policy and strategic planning and adjudication among agencies.

RECOMMENDATION 3

Identify Critical Infrastructure Dependencies

Critical infrastructures are those systems that are essential to the minimum operations of the economy and government. The critical infrastructures of the United States are predominantly owned by the private sector, and the DoD is extremely dependent upon them. Industry has indicated a willingness to share information with the DoD, but will not necessarily be motivated by the same factors that motivate government. Industry fears regulation and unfunded mandates and will not go beyond what makes financial sense.

DoD must make a concerted effort to identify what is critical in terms of its private sector infrastructure dependencies. The DoD effort to produce sector Critical Infrastructure Protection (CIP) plans was a step in the right direction; however, lack of funding is hindering this action. DoD must energize its local outreach by local DoD installation commanders to build the relationships necessary and to identify dependencies on local commercial and municipal infrastructures.

Page 1118 of 3957

RECOMMENDATION 4

Gain Consensus on DIO Security Standards

There are few information security technical standards to which DoD program managers can turn. Moreover, Global Information Grid (GIG) Information Assurance Technical Architecture Framework (IATF) Standards and Protocols for providing security are inconsistent with the Joint Technical Architecture (JTA).

A clarification memorandum should be issued making it clear the JTA will be adhered to for all GIG implementations, especially in the IA domain. The JTA is the better reference on IA standards and protocols, and it should be referenced as such in all GIG IA policy documents.

CONCLUSIONS

Following the end of the Cold War, and the subsequent changes in the geopolitical climate, the United States now faces a different kind of threat. This threat is characterized by the ability of numerous potential adversaries to engage in an information attack upon the United States, enabled by the lower entry costs associated with such an attack. Further, an attack could be at a lower threshold as a concerted effort to undermine or gradually erode our strategic or tactical position, our economic strength and fiscal processes, societal confidence in our government's ability to respond to crisis, or other less traditional targets. America's ability to attribute and respond is woefully insufficient to pose a significant deterrent to would be-attackers. And on the other end of the spectrum, early tactical indications and warning capabilities are virtually non-existent in cyberspace. These factors converge to create a newly and differently vulnerable United States homeland.

It is our contention that immediate actions can work to decrease the threat and potential damage to United States national security, including infrastructures, institutions, and individuals. The United States national security apparatus must continue to evolve over time to deal with these emerging trans-national threats, including trans-boundary threats where the differences between law enforcement and national defense, between foreign and domestic, between national and transnational, and between government and civilian are increasingly irrelevant. In the interim, there are a few discrete policy related actions we as a nation and military institution should take:

- We all need to be able to speak the same language and should take action toward a common DIO-related lexicon.
- Someone needs to be in charge to ensure government-wide coordination.
- We need to identify our dependencies on and protect our critical infrastructures.
- DOD systems developers need a single source for DIO security standards.

Page 1119 of 3957

I. TOWARD A COMMON TERMINOLOGY

New technologies and new concepts inevitably require new terminology. Unfortunately, terminology and definitions related to DIO vary widely throughout government and the private sector. DoD has expended considerable effort to standardize Information Operations (IO) related definitions, but differences and controversy remain. The Intelligence Community (IC) and DoD, in spite of a great incentive to share definitions, have managed to formally agree on only about a dozen. Industry and the private sector use a wide variety of definitions depending on convenience and circumstance, and these often differ from those within the IC and DoD.

How one defines a concept or an action has a direct bearing on which laws may be applicable to a situation and which authorities may hold sway. It may also affect how actions are funded. Consequently, definitional issues often masquerade as surrogates for deeper struggles over turf and resources.

The situation is made more complicated by the fact that some terms arrive on the scene laden with semiotic baggage. For example, "monitoring," means one thing to the National Security Administration (NSA) in a foreign intelligence context, another to the FBI in its law enforcement role, and something quite different to the ACLU when discussing the Fourth Amendment. Likewise, the term "attack" may mean to destroy, to penetrate for purposes of monitoring, to trace back for purposes of defense, or to temporarily disable, depending on who is conducting the "attack" and the intent of his or her actions.

Fortunately, the law does not need to be changed to create a common lexicon and direct its use throughout government. Most, if not all, of the problems associated with definitions can be solved using existing processes and organizations. However, a necessary precondition of such a lexicon would be an improved consensus on authorities, roles, and responsibilities to perform DIO. The process of building a common lexicon would force many such issues into the open for discussion and resolution. Additionally, if such a lexicon were developed with utility to the civil sector in mind, it might have the added benefit of helping industry consolidate its efforts to defend critical infrastructures.

A Presidential Review Directive (PRD) has recently been signed, which calls for an Interagency Working Group (IWG) to reach consensus on several matters important to IO in general and DIO in particular. Doing so will do much to clarify roles and responsibilities. The subject of definitions is among the matters to be discussed, but the PRD stops short of calling for a comprehensive common lexicon to be used throughout government.

FINDINGS

- Multiple definitions exist for common DIO-related terms. This is so within both DoD and the IC. The law enforcement community, the private sector, and the rest of government use either their own terms for DIO-related concepts or create new ones as the need arises.
- Within DoD and the IC, the use of multiple definitions for the same concept has the potential to cause operational confusion. Outside of DoD and the IC, the use of

Page 1120 of 3957

multiple terms can exacerbate problems associated with overlapping authorities and complicate efforts to coordinate a response to an attack.

  - The absence of common definitions produces differing interpretations of authorities and differing ideas about the purpose of an action. This can be particularly troublesome when particular words (e.g., monitoring) have widely accepted meanings in the private sector and legal communities, which are based on case law or popular misconceptions.

- A common lexicon would not only facilitate mutual efforts to defend infrastructures, but it would help clarify authorities, roles, and responsibilities as well.
- Creating a common lexicon of useful DIO terms would not require changes to law, policy or regulation. Existing mechanisms and organizations are sufficient to mandate and develop such a lexicon.
- The challenge will be to reach out beyond DoD and the IC to include the private sector, the law enforcement community, and the rest of government in the process. For this reason, the effort requires sponsorship at the National Security Council (NSC), National Economic Council (NEC), or Executive Office of the President (EOP) level.

RECOMMENDATIONS

- SecDef and the Director of the CIAO should jointly sponsor an effort to produce an authoritative document (perhaps an Executive Order) containing DIO-related terms, which would be useful in both the national security and civil sectors of government. This effort should draw upon the work of the IWG established by the PRD on IO.
- To assist this effort, the following Office of the Secretary of Defense (OSD) actions should be undertaken:
  - DOD & IC General Counsels (GCs) should work with the DOJ to develop a common concept for and set of terms to be used when conducting "investigations" in cyberspace.
  - The Bilateral IO Steering Group (BIOSG) should create a joint DOD/IC working group to produce the largest possible set of common IO-related definitions. The term DIO should be included.
  - USD(P) should initiate a dialogue with the State Department and the Office of Management and Budget (OMB) regarding common DIO definitions. The goal of these talks would be to encourage the use of common DIO-related terms throughout top levels of government, the international community, and the DoD.

Page 1121 of 3957

II. REQUIREMENT FOR GOVERNMENT-WIDE COORDINATION

Prior to the Information Age, protecting the nation from external attack was clearly the province of the DoD, supported by the IC. Law enforcement assisted with counter-intelligence efforts and other domestic responsibilities. The situation is more complex today. An attacker in cyberspace may do harm to our critical infrastructures without our knowing his identity or location. The infrastructures he is attacking may be private property and not clearly under the purview of the national security apparatus. Similarly, uncertainty about the origin, severity, and target of an attack may lead to confusion over whose authorities are preeminent in responding to it. Obviously, coordination becomes critical in such circumstances.

Warning is another issue that will be seen through different lenses in the Information Age. Traditional intelligence collection and analysis methods might provide some measure of *strategic* warning of an IO attack, but the nation has no means of providing *tactical* Indications and Warning (I&W) in cyberspace. In fact, there is no reliable means of even detecting a widespread, subtle, "slow and low" attack, let alone warning of it. Some would argue that such an attack is already ongoing. Even if an attack were detected, there is no consistent, widely understood process for reacting to it or recovering from its effects. Furthermore, there are no formal mechanisms for balancing equities between law enforcement and national security when reacting to it.

Any cyber I&W effort will require visibility into a large number of domestic networks, if not for content, at least to characterize the health of their operations. Obviously, the IC is limited in its ability to perform such a function. Likewise, law enforcement is proscribed from monitoring actions in the absence of compelling legal grounds. Nevertheless, there is much that can be done within existing law, policy, and regulation. (For a more complete discussion of this subject, see the legal section of the report.)

A few systems in government and industry (e.g., monitored command networks and Telecommunications Service Providers) have limited capabilities to detect an attack within their own "stovepipes," but reaction options are limited and local. Coordination and "spreading the word" generally falls to Computer Emergency Response Teams (CERTs) and individual initiative. In no case is there a robust means of characterizing diverse attacks occurring in separate segments of government and industry or of rationalizing large-scale reaction and recovery. The National Information Protection Center (NIPC) was originally created to help coordinate information on such attacks, but has devolved primarily into a cyber-crime investigation body. In fact, the predominant FBI (law enforcement) culture of the NIPC has made information sharing difficult in a practical sense, within government or with industry. As always, well-meaning individuals with initiative have built informal coordination mechanisms, but these are personality dependent.

Since the NIPC, by default, considers a cyber intrusion to be a crime, rules of evidence and strict investigative procedures are applied and information sharing is restricted. This practice, which appears to have little justification in law, biases reactions in favor of law enforcement and

Page 1122 of 3957

stands in the way of effective information sharing and the coordination that would be necessary to mount an effective national defense. Finally, no one is assigned the responsibility or the authority (other than through Cabinet level cooperation) to make the decision that an ongoing attack has progressed from a law enforcement case to a national security matter.

A similar vacuum is seen when one looks for someone in authority to coordinate a recovery from a nationwide or large-scale cyber attack. Obviously, some activities would be covered under standing contingency plans for disaster recovery or continuity of government. Likewise, many segments of industry, (e.g., banking and the stock markets) have elaborate backup and recovery plans. On the other hand, if an attacker were to mount a carefully coordinated assault on several segments of our infrastructure simultaneously, it would be difficult to recover without massive dislocation. For example, if phone service and the power grid were lost at the same time gas lines were disrupted during winter, the combined effect could be catastrophic. Even worse would be a scenario combining such cyber attacks with traditional bomb blasts or the release of a biological agent. It does not take much imagination to see that coordinating a recovery would require difficult tradeoff decisions about whose infrastructure should be recovered first. Questions of liability aside, these hard choices must be made by someone with visibility across infrastructure stovepipes and the authority to compel actions that will affect lives and finances.

As matters stand today, a declaration of martial law might be required to answer the demands of the desperate situation described above. However, a more palatable, more effective, and less costly recovery could be made using the offices of a standing official charged with the responsibility for national critical infrastructure protection. It is true that there is a coordinator for counterterrorism, security and critical infrastructure protection, but realistically his authorities are constrained to his powers of persuasion. Likewise, CINC, Joint Forces Command is charged with homeland national defense, but confusion may arise from the fact that CINCSPACE is responsible for Computer Network Defense. Realistically, neither CINC can do much to prepare for homeland cyber defense without asking hard questions about posse commitatus, the legal aspects of dealing with private industry, and public perceptions of the military taking on such a role in peacetime.

Finally, there is the question of international allies and corporations with close ties to U.S. firms. Geographic boundaries mean little in cyberspace. Effective reaction to and recovery from a serious cyber attack almost certainly will require coordination with allies and foreign partners. Consequently, the State Department must engage on these issues in the immediate future. In fact, State is already involved in several DIO-related matters, such as a Russian proposal to limit work on Information Warfare. As matters progress, State will have to join more fully with the DoD, the IC, and law enforcement communities in coordinating responses to cyber issues.

In sum, the nation needs a well-staffed, designated official with direct access to the principals of the National Security Council (NSC) who is charged to plan for and respond to the type of crisis described above. Perhaps the growing discussion about creating a Federal CIO within the Executive Office of the President will answer these concerns, provided that the position is given the required authorities and that national security matters are coordinated through the NSC. Such an official will require explicit authorities that can only be granted in law by Congress. Consequently, anyone appointed to fulfill these duties will require Congressional confirmation.

Page 1123 of 3957

FINDINGS

- We have no means of providing tactical I&W of a widespread, well-coordinated cyber attack, other than reporting within a few stovepipes (e.g., local telcos and DoD networks).
- There is no clear responsibility for rationalizing law enforcement and national defense equities when certain types of cyber attack are detected.
- There is currently a bias toward using law enforcement authorities and procedures when a cyber incident is detected. Although this will be satisfactory in the vast majority of cases, no formal means exists to review cases to determine if national security procedures might be more appropriate.
- No one has the responsibility or authority to make response and recovery decisions and take actions across stovepipes. Coordination depends on personalities.
- The State Department is potentially very important to DIO, but is not sufficiently engaged.
- A great portion of government does not understand DIO issues or appreciate the potential impact of information technology vulnerabilities on their operations.

RECOMMENDATIONS

- The SecDef should propose the creation of a national DIO coordinator. Prior to congressional action, the Coordinator's authorities will be limited. In the interim, he could serve as the nexus of DIO policy development. Eventually, this individual should sponsor the development of national-level, coordinated DoD/IC/law enforcement mechanisms to provide I&W of a cyber attack, respond to it, and recover from its effects.
- To support this effort the SecDef and DCI should:
  - Create a joint DoD/IC panel to work with the DOJ, NSC, and OMB staffs to draft a DIO Executive Order (EO). The EO should clearly establish the preeminence of the national security response over the law enforcement response in cases having a national security impact.
  - Create a panel to examine EO12333 and other law, policy, and regulations in light of emerging DIO realities.
  - Create a standing GC's working group to monitor legal precedents for decisions useful and inimical to DIO efforts and to explore the latitude available for DIO under existing law.
  - Task the Bilateral IO Steering Group (BIOSG) to propose mechanisms for the military services and the IC to deconflict DIO (especially related to Computer Network Operations).

Page 1124 of 3957

Page 1125 of 3957

III. CRITICAL INFRASTRUCTURE PROTECTION

The Defense Department is increasingly reliant on a broad range of vital infrastructure services provided by the private sector, municipal utilities, and other non-DoD sources. While DoD's communications, energy, transportation, logistics, and supporting requirements grew significantly over recent decades, DoD has become far more dependent on non-DoD-owned and -operated systems and networks. The underlying private sector infrastructures have undergone an explosion in technical capability, complexity, and integration, adopting new technologies and processes, particularly evident in communications and energy infrastructures. This revolution in technology and system interoperability has empowered infrastructure owners and operators to better serve their customers while expanding capabilities and building corporate strength. Technological interoperability, a feature inherent in these infrastructures, was market economy driven, and thus the infrastructures are exceedingly interdependent. As the infrastructures advanced in capability, capacity, and complexity, DoD took advantage of their availability.

Private sector dependencies have direct implications for the availability and reliability of DoD's Global Information Grid (GIG) – leased private sector systems incorporating our nation's fiber optic network, twisted wire, and wireless systems provide the GIG's backbone outside DoD's information infrastructure gateways. The dependencies go much further than this vital information backbone; the breadth of defense operations requires much more energy, logistics, and other vital services than ever before. For DoD to fully understand its private sector dependencies, it must analyze and assess those dependencies, a process that cannot be done without dialogue and partnering with the private sector or municipal owners and operators of those infrastructures.

DoD's expanded use of private sector infrastructures should logically require a more detailed assessment of potential risks inherent in the interdependent, underlying infrastructure. The private sector built and operated these infrastructures while using a very different risk model than those used within DoD. Private sector risk analyses are based on economically driven models, focusing on profitability and customer service, with modernization reliant on anticipated returns on investment. Threats and risks are plausible in peacetime scenarios, where the threats may be backhoes and risks considered are seen as natural disasters or competitive business practices. DOD risk models focus on more sinister threats – where a bad actor or nation state could purposefully deny infrastructure to degrade our global projection of force or otherwise undermine the national security of the United States.

The *Presidential Decision Directive on Critical Infrastructure Protection* (PDD-63, 1998) focused national efforts to implement critical infrastructure solutions, including expanded partnership between government and the private sector. Many national initiatives began, including establishment of the National Infrastructure Protection Center at FBI and the initiation of Infrastructure Sector Analysis Centers (ISACs), attempting to expand partnership between government and the private sector within individual infrastructure sectors. Arguably, though much has been done to advance national CIP efforts, the broad ranging initiatives have not seemed to gel into the desired partnerships, including interagency coordination and partnerships between government and the private sector. Similarly, many agencies and departments have not

Page 1126 of 3957

funded CIP efforts consistently across government. DoD began recognizing its need to consider critical infrastructure issues and proceeded somewhat independently and separately from other government agencies to focus on vital aspects central to DoD.

In 1997, DoD accelerated its exploration of dependencies on non-DoD infrastructures, standing up individual infrastructure sector teams and coordinating them through organizational processes such as the Critical Infrastructure Protection Integration Staff (CIPIS). Administrative and organizational efforts within OSD and the services were supplemented by operational initiatives, such as Joint Service Integrated Vulnerability Assessment (JSIVA) efforts, accelerated Red Teaming, DoD readiness exercises such as Eligible Receiver, and expanded infrastructure initiatives at the Joint Program Office for Special Technology Countermeasures (JPO-STC) and the Defense Threat Reduction Agency (DTRA). Most infrastructure vulnerability assessments focused on our key defense sites and facilities.

The risk environment, especially as it pertains to the critical infrastructures on which DoD relies, has changed. Threats to our homeland are becoming far more real, leading to important explorations of new risks: information warfare, biological and chemical warfare, and unconventional nuclear risks. While the risk environment has evolved, the infrastructures on which we rely, both domestically and in forward-deployed areas, have become more technologically advanced, concentrated in increasingly critical nodes, with complex distribution that DoD may not fully understand. Further, these infrastructures are less within the government's and DoD's control. Market pressures drive technological advancement within these networks, with fiscal realities no longer shaped by government needs.

The potential for a smart adversary to undermine the reliability or availability of our critical infrastructures is increasingly real. In the context of DoD's evolving Global Information Grid backbone, protecting information architectures and their content does not necessarily protect the underlying cyber and physical infrastructures. Similarly, protecting DoD's GIG within the gateways that connect it to private-sector-owned and -operated information infrastructures does not guarantee GIG availability should the leased connectivity outside those gateways be denied.

DoD should accelerate its efforts to identify its private sector dependencies and vulnerabilities, for DoD's information backbone as well as for other infrastructure dependencies that support energy requirements, logistics and transportation, water, and other critical infrastructure reliances. Without broad-based consideration of the full scope of critical infrastructure dependencies, mission constraints are unknown but potentially significant.

Relationship building and the resultant trust takes time. It is likely that both the government and private sector leaders at a localized level have multiple overlapping requirements and interests that contribute to both national security and the corporate prosperity of the infrastructure provider. For the purposes of critical infrastructure protection, it is important that these relationships advance toward the mutual benefits of government interests, including those of national security, and those of the critical infrastructure providers. Accordingly, it is important that efforts taking place at the local DoD installation level to define local dependencies on private infrastructures be explored and assessed in depth. More work needs to be done to identify vulnerabilities outside the lifelines of DoD, yet within the infrastructures on which DoD is very reliant.

Partnership between government and the private sector remains a vitally important yet elusive goal. Efforts to expand partnership with the private sector are hampered in many ways.

Page 1127 of 3957

The private sector sees a lot of the government wrangling and interagency squabbles (some of these indicate the shortfalls in PDD-63 implementation), confusing the infrastructure owners and operators and making it easier to question the government's seriousness in partnering. Further, especially in the context of information sharing among government and the private sector, the owners and operators need relief from Freedom of Information Act (FOIA) to protect their proprietary data and interests and their competitive position.

Industry has indicated a willingness to help, but will not necessarily be motivated by the same things that motivate government. Industry fears regulation and unfunded mandates and will not go beyond what makes financial sense in the market economy. The private sector level of trust in government is low. In particular, the public is least trusting of three specific government sectors. They are law enforcement in particular, and to a lesser degree, the intelligence community and DoD. Government must be willing to openly respond to industry concerns if it hopes to overcome the hurdles in achieving partnership. While the government and the public perceive that industry has the answers, true partnering with industry remains the prime challenge. Best practices within the private sector and within government should be shared, not only as an element of trust and partnering, but to enhance the security and economic implications of infrastructure operability and assurance issues. Partnership challenges will become even more difficult in the future, as companies grow even more global.

FINDINGS

- There is a lack of understanding that it is not enough to simply protect one's own information systems. The DoD depends enormously on the commercially owned and operated telecommunications, transportation, electric power, and gas and oil industries, and on the financial sector.
- The level of trust in government is low. The outreach efforts by the government in the aftermath of PD-63 have not produced an outpouring of trust of government in the private sector.
- Industry has indicated a willingness to help, but will not be motivated by the same things that motivate the government. Industry fears regulation and unfunded mandates and will not go beyond what makes financial sense in the market economy.
- DoD is extremely reliant on private sector systems, networks, and infrastructures. Increased analysis is needed to pinpoint and assure vital reliances on the private sector.
- DoD must partner with the private sector to better protect networks and enhance national security.

RECOMMENDATIONS

- DoD should accelerate actions to identify critical infrastructure dependencies on the private sector – the DoD effort to produce sector CIP plans is a step in the right direction, but we would note that it is not moving along very quickly, primarily due to lack of funding.
- DoD must expand its interactions with the private sector and municipal providers of critical infrastructure services. This is best achieved on a localized level, between

Page 1128 of 3957

base commanders (or other DoD leadership) and the infrastructure owners and operators. Direct DoD installation commanders (with support of JPO-STC) to identify critical infrastructure vulnerabilities, assess mission impact, and take corrective action with private sector service providers.

- DoD should work with Sector Lead Agencies to ensure that its requirements are incorporated into the information-sharing processes with the owners and operators of critical infrastructure.
- Advocate FOIA and other related legal relief to remove impediments to private sector information sharing.
- Fund and resource JPO-STC appropriately to support critical infrastructure assessments. As a minimum starting point, increase funding for such focused efforts to at least $25M per year.
- DoD should modify or develop a process to assess the fiscal impact of infrastructure impact.

Page 1129 of 3957

VI. SECURITY STANDARDS

During the course of this DSB Task Force, it became increasingly clear that, as with the definitional issues addressed earlier, understandings regarding use of information technology standards for desktop, system, and network security mean different things to different people--so much so that in the same organization responsible for promulgating the JTA, a new document, the Information Assurance Technical Architecture Framework (IATF), was developed for the purpose of setting forth guidance with respect to IA standards for the Global Information Grid (GIG).

The IATF document is a tutorial and collection of useful generic information on Information Assurance (IA). It should be noted, however, that the section of the IATF associated with standards and protocols for providing security to system applications is incorrect and inconsistent with the JTA.

The IATF, unlike the JTA, is not a standards setting or selection activity. Rather, the IATF Forum has been organized to encourage participation by vendors of largely commercial off-the-shelf (COTS) IA products and services. The major focus of the IATF is the development of protection profiles (under the Common Criteria [CC]) that will be used to evaluate products, e.g., under the National Information Assurance Partnership (NIAP) program operated by the National Intelligence Support Team (NIST) and the National Security Administration (NSA). There is no unified architectural underpinning for the IATF. This is to be expected, i.e., security evaluation criteria such as the CC (and product profiles based on the CC) tend to be architecture independent. As a result, the collection of standards cited by the IATF in their briefing to our panel lacks architectural continuity and it is not an appropriate alternative to the work of the JTA.

Many of the standards that are lumped together are experimental or dead. For example, S-HTTP is not implemented in any commercial browsers or servers; it lost the protocol battle to SSL/TLS. SPKI is not a standard, but rather is the experimental output of a failed Internet Engineering Task Force (IETF) working group, not supported in commercial products. The PKIX WG of the IETF produces standards based on X.509, which are implemented in a wide variety of products. Moreover, the other IETF security protocol working groups make use of the PKIX standards, not SPKI.

The IATF referenced a wide range of security labeling standards that are a mix of redundant and/or superceded documents. The IATF thus suffers from the same problems associated with the TAFIM; it is a collection of history and general information--not a document that can be used to implement interoperable, secured information systems for DoD. Figure 1 shows the numerous protocols issued as guidance in the IATF, most of which are inconsistent with the JTA.

Page 1130 of 3957

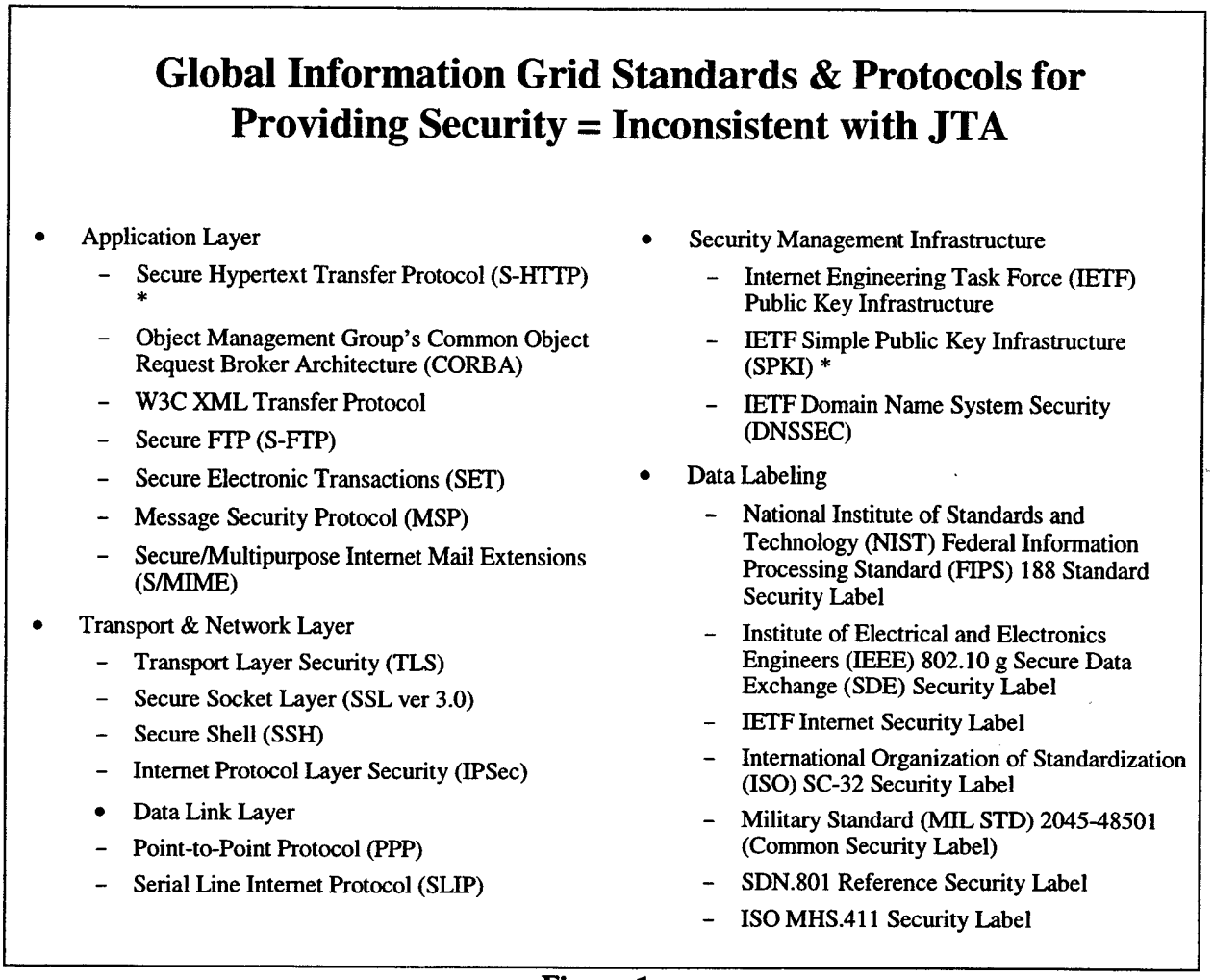


Figure 1.

DoD policy requires that the Joint Technical Architecture (JTA) be used as the "building code" for the DoD information infrastructure. On the other hand, the recent document from the Deputy Secretary of Defense, "Department of Defense Chief Information Officer Guidance and Policy Memorandum no. 68510," Department of Defense Global Information Grid Information Assurance (ASD/C3I), suggests that the IATF and published Common Criteria Protection Profiles be consulted "for guidance, and IA solutions to be considered to counter attacks." A major concern is the apparent confusion these two policy statements could cause within the IA community.

There is an urgent need to provide JTA education to all personnel working with the GIG architecture. Though the IATF effort may be viewed as being helpful in several ways, such as documenting what is available in the commercial sector and what has not survived the "test of time," the JTA should be positioned as the compelling document for guiding the use of standards within the GIG. Commercial standards should be used for security in the GIG wherever practical; however, there will be DoD-unique requirements for certain security implementations not available from the commercial sector. For this reason, we support the R&D/technology

initiatives documented in the Technology chapter of the DIO Task Force report as well as the recommendations put forth by the Architecture Panel of the DIO Task Force.

FINDINGS

- The IATF suffers from the same problems associated with the TAFIM; it is a collection of history and general information—the IATF is not a document that can be used to implement interoperable, secured information systems for DoD.
- The IATF standards are incorrect and inconsistent with the JTA and private sector practice.

RECOMMENDATIONS

- A clarification memorandum should be issued making it clear that the JTA will be adhered to for all GIG implementations, especially in the IA domain.
- The JTA is the better reference on IA standards and protocols, and it should be referenced as such in all GIG IA policy documents.

Page 1132 of 3957

Page 1133 of 3957

APPENDIX A. ACRONYMS

BIOSG	Bilateral IO Steering Group
CC	Common Criteria
CERTs	Computer Emergency Response Teams
CIAO	Critical Infrastructure Assurance Office
CIP	Critical Infrastructure Protection
CIPIS	Critical Infrastructure Protection Integration Staff
COTS	Commercial off-the-shelf software
DIO	Defensive Information Operations
DTRA	Defense Threat Reduction Agency
EO	Executive Order
EOP	Executive Office of the President
FOIA	Freedom of Information Act
GAO	Government Accounting Office
GC	General Counsel
GIG	Global Information Grid
I&W	Indications and Warning
IA	Information Assurance
IATF	Information Assurance Technical Architecture Framework
IETF	Internet Engineering Task Force
IC	Intelligence Community
IO	Information Operations
ISACs	Infrastructure Sector Analysis Centers
IWG	Interagency Working Group
JPO-STC	Joint Program Office for Special Technology Countermeasures
JTA	Joint Technical Architecture
JSIVA	Joint Service Integrated Vulnerability Assessment
NEC	National Economic Council
NIAP	National Information Assurance Partnership
NIPC	National Information Protection Center
NIST	National Intelligence Support Team
NSA	National Security Agency
NSC	National Security Council
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PDD63	Presidential Decision Directive
PRD	Presidential Review Directive

Page 1134 of 3957

Page 1135 of 3957

ANNEX B. PANEL MEMBERSHIP

Chairman:

Mr. Richard Wilhelm	Booz-Allen & Hamilton

Members:

Mr. Brenton Greene	Sandia National Laboratories
Mr. David Henry	Scitor
Mr. Owen Wormser	C3I

Page 1136 of 3957

ANNEX E

Defense Science Board Task Force
on
Defensive Information Operations

Panel Report on Legal Implications

REPORT OF FINDINGS,
DISCUSSION/OBSERVATIONS
AND RECOMMENDATIONS

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

The Overlapping of National Security and Law Enforcement Missions 1

Why Information Sharing Is So Important 2

Why Information-Sharing Is So Hard 2

Recommendations for the Defense Department and the Justice Department 3

Recommendations for Congress 4

I. Introduction: Why Sharing Information About Network Attacks Is Important – and Hard to Achieve 7

II. Recommendations 11

APPENDIX A. Acronyms A-1

APPENDIX B. Task Force Members B-1

Page 1138 of 3957

Page 1139 of 3957

EXECUTIVE SUMMARY

"Yesterday, December 7, 1941 – a date which will live in infamy – U.S. forces in Pearl Harbor suffered numerous criminal trespasses. I have mobilized a team of prosecutors and FBI agents to investigate and take action."

In 1941, FDR never even considered giving that speech. Today, he might have to.

If critical U.S. information networks were attacked tomorrow in an "electronic Pearl Harbor," FBI agents and Justice Department prosecutors would in fact be on the front lines. Unfortunately, this report concludes, law enforcement and national security agencies have not learned to work together well to defend against attacks on U.S. information networks. Legal and cultural roadblocks have made it difficult for the Defense Department to rely on the FBI and Justice for full information about potentially dangerous attacks. This report proposes an agenda for new leadership and new compromises to break through these roadblocks.

THE OVERLAPPING OF NATIONAL SECURITY AND LAW ENFORCEMENT MISSIONS

Why have Justice Department entities like the FBI assumed such a large role in defending against network attacks? In a word, because attacks on American networks are typically the work of hackers, not foreign states. They are crimes, nothing more.

But that will change, and soon. Hackers' tools will become weapons in the hands of hostile nations, because U.S. information systems are a tempting target, especially for countries that cannot confront our armed forces directly. Network attacks are anonymous – or at least deniable. They are asymmetric. They allow hostile nations to pick a battlefield that minimizes American strengths in conventional and nuclear forces – indeed, one that turns strength into weakness by exploiting the United States' unique dependence on computer networks. The next Saddam Hussein – or the current one, for that matter – could win a symbolic victory just by tying up Manhattan traffic for a day. But some believe network attacks will soon be able to cause deaths and chaos across the country – especially if offensive capabilities continue to outpace our defenses.

In short, network attacks have a national security as well as a law enforcement dimension. DoD must be involved, both because it has a responsibility to defend the country and because it depends so heavily on a civilian infrastructure that is particularly vulnerable to network attacks. But DoD cannot act alone; it may not be possible to tell at the start of an attack whether the matter can be treated as a crime or an act of war or something in between. This means that the defense, intelligence, and law enforcement communities must be prepared to work together in a smooth and coordinated way.

Based on what the task force has seen, that day is a long way off. While they have been quick to take the lead in protecting information networks, the Justice Department and the FBI

Page 1140 of 3957

have been slower to recognize the need for cooperation with the Defense Department and other national security agencies.

WHY INFORMATION SHARING IS SO IMPORTANT

This tendency toward limited information sharing has harmed the country's preparations for attacks on U.S. critical information infrastructure. The first order of business in preparing to defend against network attacks is to gather information about the attacks now being mounted against U.S. information systems. The more we know about today's attacks, the better prepared we will be to deal with tomorrow's. Information warfare cannot be launched blindly. Like any weapon, it must be tested. Indeed, to be most effective, information warfare should be planned and preliminary intrusions should be launched years before an overt attack – defenses must be probed, vulnerable systems reconnoitered, logic bombs planted. To judge the extent of the danger, we should be watching intently for just such activities – sifting those patterns from the noise of "script kiddy" hackers. We should be alert for the subtle signals that governments and terrorists are in fact beginning to turn the theory of information warfare into practice.

Thus, gathering information about the kinds of attacks now being launched is the crucial first step of any defensive effort. Unfortunately, this task has become the subject not of effective initiative but of continuing political and bureaucratic conflict. Although it has responsibility for national defense, the Defense Department must rely on law enforcement agencies such as the FBI and the Justice Department to gather information about network attacks and then decide what DoD needs to know. Thus far, however, the FBI and the Justice Department have been far too focused on their own missions to provide the kind of information sharing that DoD needs.

WHY INFORMATION-SHARING IS SO HARD

The FBI is the principal "intake point" for information about network attacks, in large part because it is easy to use the tools of criminal investigation to gather information about an attack, especially in its early stages. That is why the National Infrastructure Protection Center (NIPC) was housed within the FBI. Although staffed by defense and intelligence personnel as well as FBI agents, it relies heavily on criminal investigative tools that could not easily be deployed by other agencies.

But the effectiveness of NIPC in protecting national security depends on sharing information about attacks, and the FBI has a remarkably bad reputation on that score. A wide range of different communities – local police, intelligence analysts, civilian agencies, and business executives – all complain with regularity that however much information they share with the Bureau, the Bureau never reciprocates.

The NIPC has struggled to avoid the same reputation, but the culture of reticence cannot be turned on and off, particularly when the Justice Department, for its own reasons, has raised additional barriers to information sharing with defense and intelligence agencies. To some extent, the atmospherics surrounding the dialogue between the NIPC and the agencies it supports has made it difficult to arrive at ground truth, but the task force believes that what it has found warrants action. Without substantial improvement, the NIPC cannot live up to its initial promise.

As things now stand, DoD cannot count on NIPC, Justice, or the FBI for a free flow of information about network attacks. On the contrary, the task force identified numerous policies and legal interpretations at NIPC, the FBI, and the Justice Department that have prevented

Page 1141 of 3957

effective information sharing about potential national security risks. The task force concludes that these barriers must be swept away, and soon, if DoD is to continue to support and rely upon NIPC. Unless NIPC, FBI, and Justice overcome their narrow crime-fighting perspectives – in a formal high-level agreement with the Defense Department – then DoD and the intelligence community should pull out of NIPC and create an independent center for gathering and sharing information about the most serious network attacks. This should, however, in the view of the task force, clearly be a measure of last resort.

RECOMMENDATIONS FOR THE DEFENSE DEPARTMENT AND THE JUSTICE DEPARTMENT

Rather than splinter the government's limited resources further, the task force recommends several specific changes in the policies and legal interpretations that have prevented NIPC from achieving its full potential as an information-sharing center. It is the view of the task force that the necessary changes cannot be achieved without leadership from the very top of both departments, and that the issues raised below should form the agenda for a series of talks that will, we hope, culminate in a new agreement over information sharing between the law enforcement and national security communities.

- First, all information available to NIPC should also be available to defense and intelligence analysts (who are already trusted with rather more sensitive information) unless there is an express legal bar on sharing or an *interagency* consensus that sharing the information is imprudent. The task force found that there may be misperceptions about the "law enforcement sensitive" label that is placed on information flowing from the NIPC to the Department. The Justice Department should clarify for the department that the label is attached to sensitize its readers rather than to prevent its flow to those requiring the information within the department. Likewise, the task force also believes that DoD agencies (including NSA) should share all available information on events with the NIPC.

- Second, the Justice Department has blocked NIPC from easy and natural communication with the National Security Council (NSC) about infrastructure attacks, despite the NSC's central role in national security decision making generally and infrastructure protection in particular. The DoJ is plainly reluctant to share information about criminal investigations with White House personnel, but DoJ's general policy, should not be applied to information about network attacks.

- Third, DoD should have access to information about network attacks gathered under Title III (the wiretap statute). The Justice Department opinion refusing to provide this access shows little appreciation of the need for interagency cooperation on national security matters and should be reconsidered.

- Fourth, concerns about grand jury secrecy have made it difficult to know what material in a criminal investigative file may be shared with DoD and what may not. These concerns are mostly derived from very conservative readings of the rules on grand jury secrecy (readings adopted in part to serve the prosecutors' interest in avoiding public disclosures of their investigative priorities). They are also derived in part from the Justice Department's failure to discipline investigators of infrastructure attacks. These investigators could gather information without using grand jury

subpoenas and thereby avoid later information sharing difficulties, but the FBI and Justice Department do not require their investigators to use these less problematic tools in the first instance. The rules on sharing grand jury information should be clarified to permit sharing for national security purposes; until this is accomplished, computer crime investigators should be prohibited from using grand jury subpoenas without interagency approval. While the amount of grand jury material that has been withheld is disputed, and may be relatively small, the failure to address this issue continues to create tension.

- Fifth, NIPC is buried so deep in the Justice and FBI bureaucracy that it cannot perform its interagency role effectively because it cannot assure its counterparts in other agencies that decisions can be rapidly referred to high levels in the bureau and the Justice Department. NIPC should report directly to the Office of the Director FBI as well as the Office of the Deputy Attorney General.

- Sixth, DoD has not taken all the steps necessary to ensure a large and strong contingent of DoD detailees at NIPC. Assuming a successful resolution of the issues raised in this report, DoD should upgrade its contribution to NIPC, both in numbers and in quality, and it should treat NIPC service as a "joint" appointment for purposes of military promotion.

- Seventh, NIPC has much to offer DoD on questions such as when to block a particular hacker from further access and when to let the hacker continue in an effort to learn more about his techniques and purposes. DoD should agree on a role that clarifies NIPC's purely advisory position while guaranteeing that NIPC has a voice in such decisions. DoD should further clarify the commander's decision-making authority in this area so that responsibility is unambiguous.

- Eighth, NIPC and the Justice Department's computer crime experts have exceeded their jurisdiction in trying to limit what information intelligence agencies may receive; neither NIPC nor the Justice Department's Criminal Division should have a role in deciding whether and how DoD entities share information with NSA or other intelligence agencies.

- Finally, the task force notes that "red team" exercises, though vital, have been slowed in the past by multiple legal signoffs and supervision at DoD. This concern is diminishing as red teaming becomes more common, but it remains true that a standardized and simple set of procedures should be adopted to allow unannounced "red team" attacks on all DoD networks without excessive high-level intervention by DoD officials.

RECOMMENDATIONS FOR CONGRESS

All of the recommendations above could be implemented without changing any statute. That is the preferred solution. Nonetheless, there are areas in which U.S. laws have failed to anticipate the need for effective critical infrastructure protection. For that reason, the task force

Page 1143 of 3957

recommends that the Defense Department support a variety of relatively limited changes in existing law.

- Most important, DoD should have its own civil authority to seek information about network attacks with national security implications. Under existing law, network service providers may give away information about hacking attacks on street corners, but they are legally prohibited from giving the information to a government agency unless the agency begins a criminal investigation. This is unfortunate for all. It forces hacker investigations into a criminal posture, which is likely to be bad for the hacker as well as for the opportunity to share information among agencies. The government should justify any request for information about its citizens, but it should not have to launch a criminal investigation before it can gather information needed to protect national security.

- Second, the task force encountered a disturbing limitation in the ability of the government to maintain wiretap coverage of persons engaged in long-term hacking campaigns against government networks. Ironically, the more likely it is that the attackers are sponsored by foreign governments, the less likely it is that wiretap coverage will be maintained, because the likelihood of successful prosecution will decline over time. In the end, criminal wiretap authorities are inadequate for this problem, and a statutory solution should be sought that protects both national security and the civil liberties of Americans. One possibility is a provision denying network trespassers an expectation of privacy for their actions in attacking a victim's information system.

- Third, current law concerning "trap-and-trace" orders often requires that law enforcement agencies seek multiple, sequential orders as they trace a single hacker from system to system. This provision should be modified to allow a single, nationwide order aimed at a single attacker who uses multiple computer systems. In addition, there is currently no statutory provision allowing the government to obtain certain types of information without the requisite order in situations of extreme urgency. This is an oddity, since under the Electronic Communications Privacy Act, wiretaps may be initiated without a judicial order in an "emergency situation." In the interest of enabling law enforcement officials to obtain the crucial information they need for the prompt investigation of critical infrastructure attacks, the provision allowing emergency wiretaps should be extended to court orders and subpoenas as well.

- Fourth, if agreement cannot be reached with the Justice Department concerning the Title III and grand jury rules that currently restrict information sharing with DoD, Congress should clarify its intent that the confidentiality of criminal investigations not trump the national security interests of the United States.

- Finally, though the majority of the problems outlined here focus on information-sharing deficiencies between and among government agencies, greater efforts could be made to encourage voluntary private-sector cooperation in hacking investigations.

Page 1144 of 3957

To this end, the use of nondisclosure agreements in gathering information on network attacks should be expanded, and narrowly tailored legislation that would restrict the Freedom of Information Act disclosure of information shared pursuant to a hacking investigation should be considered.

Page 1145 of 3957

I. INTRODUCTION: WHY SHARING INFORMATION ABOUT NETWORK ATTACKS IS IMPORTANT – AND HARD TO ACHIEVE

Like everyone else in America, the armed forces depend heavily on sophisticated communications networks – not just their own, but those of the civilian industries that support them. U.S. adversaries know this. That is why information warfare attacks on our networks are a near certainty – because they are likely to work. How great is this risk? We do not know, and this panel report focuses on what we don't know, and why.

We do know that attackers have had disturbing success in penetrating sensitive systems essential to carrying out the Defense Department's mission. Worse, the attackers who have succeeded are mostly vandals and petty criminals, and the tools they have used are offshoots of existing technology. But no one estimates the military might of the United States by studying the weaponry of American street criminals, and by the same token, the technology of information warfare will soon bear little resemblance to the viruses and denials of service that currently annoy Internet users. The problem is likely to get worse before it gets better.

Better information about network attacks is the first line of defense. To launch a serious information warfare attack on the United States would likely require considerable preparation – probing defenses, testing tactics, leaving behind logic bombs or back doors. If the government is to have warning of future attacks, it needs to gather information about current attacks in a systematic way and to analyze the information for patterns.

While gathering and sharing information on attacks is the foundation of a defense against information warfare, so far we do it badly. The private sector is reluctant to share information for both competitive and legal reasons. Information sharing comes no more easily to government. Intelligence agencies classify information in order to limit sharing to those with a "need to know." Law enforcement agencies restrict sharing to protect witnesses and keep their targets in the dark. And almost everyone in government treats information as currency, to be offered only sparingly and in return for value.

In short, sharing information does not come naturally. Despite this reluctance, the need to centralize and share information about network attacks is so obvious that an interagency entity, the National Infrastructure Protection Center (NIPC), was created to do just that.

Specifically, NIPC has two primary practical goals. One is to investigate (and, wherever possible, prevent) attacks on critical infrastructure systems. Critical infrastructure systems are the backbones that allow U.S. cities and towns to function; they include the electrical power grid, the water works, and the telecommunications pipelines. Half of NIPC's mission is to coordinate the collection and dissemination of information about the security and defense of these systems. The other part of NIPC's mission is to coordinate the sharing of information on network attacks within the law enforcement and intelligence communities, which includes, of course, DoD.

When NIPC was established, there was some debate about where it should be housed. Agencies like the Commerce Department were rejected because they lacked independent

Page 1146 of 3957

investigative and intelligence capabilities. Intelligence agencies were rejected because their mission is focused on foreign countries, and their capacity to gather intelligence on Americans is rigorously limited. While information warfare itself is an entirely appropriate concern of the intelligence community, most network attacks are not state-sponsored. Indeed, the thousands of hackers whose activities obscure the acts of foreign governments are as likely as not to be Americans. By the same token, while DoD is the proper agency to respond to information warfare, it has little or no authority to deal with simple vandals.

Given those constraints, it seemed that the logical "intake point" for information about infrastructure attacks was the FBI, which has authority to investigate both common criminals and foreign agents. Despite this logic, the FBI was a controversial choice. It was handicapped by a remarkably deep and pervasive reputation – among other law enforcement agencies, in the intelligence community, and in the private sector – as a black hole for information. Everything goes into the Hoover building, according to this view, and nothing comes out.

For that reason, many steps were taken to keep NIPC from falling heir to the FBI's reputation for restricting information. A well-regarded Justice official was transferred to head the office, and detailees from the Defense Department and intelligence agencies were put in charge of information-sharing offices within NIPC. Based on what the task force learned in the course of interviewing numerous DoD, Justice, NIPC, and intelligence sources, however, this was not enough. Putting information-sharing responsibilities in the hands of law enforcement agencies has produced serious problems that were not adequately foreseen when NIPC was established.

Because of legal and cultural restrictions, NIPC staff, even personnel detailed from DoD itself, have found it difficult to share information about network attacks in an easy, cooperative fashion with agencies outside law enforcement. The problems have been many. The National Security Council, for example, has been denied timely information on the status of network attacks under investigation; whole categories of information (Title III intercepts, for example, and materials obtained via grand jury subpoena) have been set aside by the Justice Department as the domain only of law enforcement agencies. Other information has been designated as "law enforcement sensitive" and subjected to dissemination restrictions in a fashion that lacks the safeguards usually relied upon to prevent overclassification.

Of course there are explanations for all of these roadblocks, and in many cases NIPC has worked to overcome them and to establish at least the beginnings of an effective information-sharing facility. The task force does not underestimate that achievement. NIPC has faced pressures from many directions other than defense and the intelligence communities. Businesses, civil liberties advocates, competing law enforcement agencies, and even foreign governments have all claimed the right to help set one or another aspect of NIPC policy, though they have been notably more reticent when resources have to be put into the effort. In these circumstances, to create a functioning entity with its own esprit has proved to be no easy task.

That said, the task force finds it unlikely that NIPC, operating under current constraints, can consistently provide the kinds of information needed by DoD to protect against attacks with a national security dimension. NIPC is still far too dominated by the law-enforcement culture and by legal interpretations by the FBI and Justice Department that tend to reinforce the NIPC's reputation for not sharing information. While NIPC has managed to work around some of these obstacles, the current structure for sharing network attack information still is not responsive enough to the interests of national security and intelligence agencies.

Page 1147 of 3957

This situation is not tolerable, particularly for the Department of Defense. To a very great extent, DoD depends on NIPC for the information it needs to defend itself and the nation. Reliance on law enforcement agencies for such a crucial element of support will only work if those agencies seamlessly share with DoD any and all information likely to have a bearing on DoD's defense mission. Current policies suggest that the FBI and Justice Department are not willing (or perhaps think themselves unable) to share information in this seamless way. The restraints on NIPC have significantly restricted its ability to play an adequate interagency information-sharing role.

The task force provided early drafts of conclusions to NIPC, and NIPC strongly, sometimes stridently, disagreed with task force conclusions on this point. NIPC says that it has managed to find ways to share virtually every useful piece of information about network attacks that has come into its hands. While the doctrines and difficulties laid out in this report are acknowledged as obstacles, NIPC believes that in the end they can all be overcome – indeed that almost all have been overcome – with creativity and care. NIPC urges us to focus on its successes and its need for substantial additional resources from DoD to conduct the necessary analyses of data already being shared.

The task force agrees that there have been successes, and that more analytic resources are needed – at NIPC or elsewhere. But that does not alter the fact that substantial legal and policy roadblocks exist, and that those roadblocks have prevented sharing already. Change will not come quickly. While in some cases NIPC has worked around the problem successfully, we must not wait until there is a catastrophic failure to address these concerns. The legal and policy issues identified here are continuing threats to the effort to build a seamless and effective information-sharing system for network attacks.

The task force recommendations go to the heart of this concern.

Page 1148 of 3957

Page 1149 of 3957

II. RECOMMENDATIONS

RECOMMENDATION 1:

DoD Should Insist on a High-Level Agreement with Justice and the FBI that Reforms NIPC's Role and Structure.

Part of the information sharing problem has been a lack of clear leadership. After the initial cabinet-level activity to establish NIPC, little high-level attention was paid to how preparations for information assurance were actually functioning. In that atmosphere, each agency asserted its prerogatives without much fear of oversight. Issues related to information sharing practices were not readily resolved because political decision makers did not intervene to force reasonable compromises in the interest of NIPC's overall mission.

The task force's central recommendation, therefore, is that this problem be addressed at the highest levels of the Justice and Defense Departments, and that DoD insist on major changes in exchange for augmenting its support for NIPC.

Currently, DoD is the largest contributor to the staffing of NIPC, other than the FBI itself. Present staffing levels at NIPC are roughly as follows:

FBI:	82
DoD[1]:	14
United States Postal Service:	1
CIA:	2
Energy Department Labs:	1
Local Law Enforcement:	1
Foreign Liaisons:	2

There is no high-level agreement between DoD and Justice/FBI about the terms of details to or the information-sharing practices of NIPC. Instead, information-sharing policy is set by a two-page memorandum of understanding (MOU) that is to be signed by DoD, FBI, and each detailed employee. The MOU is an inadequate and entirely one-sided document, essentially imposed on the detailees and their agencies. Some provisions are unexceptionable – such as those making clear that each employee sent from DoD will be tasked exclusively by his or her superiors at NIPC, will be removed from the chain of command in DoD, and will have access to information in FBI files and to other sensitive information.

Unfortunately, the MOU goes further. It requires that dissemination of information from NIPC, including dissemination back to the detailee's home agency, be governed by FBI policy as well as applicable statutes and other guidelines or procedures.[2]

---

1 The DoD elements represented include NSA, NCIS, Air Force OSI, DCIS, air force, army, navy, and OSD.

2 NIPC argues that the MOU is necessary to protect against claims that DoD personnel are acting in violation of *posse comitatus* rules and that NSA and CIA personnel are violating rules governing intelligence agency handling of U.S. person information. This is open to question, and should be more carefully reviewed. In practice, *posse comitatus* is rarely a bar to assistance to law enforcement, and while intelligence agency restrictions may require intelligence personnel on detail to obey the laws governing law enforcement, it is not clear that these personnel must submit to additional and unspecified

Page 1150 of 3957

Those policies are by no means limited to information-sharing restrictions imposed by law. It is of course understandable that anyone handling law enforcement information would be subject to any restrictions imposed by law on the use of such information. But the MOU goes beyond that to impose sweeping restrictions that are not required by law. Such a sweeping approach is inconsistent with NIPC's mission and with the participation of other agencies in that mission. Some restrictions based on law enforcement policy rather than law may well be appropriate, but the burden of identifying and justifying each separate restriction should be on the FBI and Justice. (It is not enough in an interagency context, to say, as NIPC has, that equivalent restrictions are imposed on FBI personnel. The point of an interagency task force is that the personnel bring different skills and traditions to the task.)

Agencies that detail staff to NIPC still pay the salaries of their detailees. It makes no sense to pay those salaries unless the employees' participation in NIPC provides ongoing value to the agency that details them. Potential restrictions on detailees' communications limit their value to the sending agency. Some agencies are already cutting back their participation. The Secret Service, for example, has ended its participation. After initially insisting on sending seven people, it has pulled all of its representatives back, in part because of reluctance to accept FBI information-restriction policies. The Department of Energy has also failed so far to replace one of its detailees; it too has had conflicts with the FBI and NIPC over information sharing.

Although DoD originally planned to send eighteen detailees, only fifteen have ever been assigned to NIPC, and the likelihood of replacement once they rotate to a new assignment is uncertain. Some DoD elements, notably the National Security Agency, have also had conflicts with NIPC over information-sharing policy; NSA's participation in the NIPC, as well as that of the CIA, has been sporadic. With this track record as a backdrop, it is at least fair for the NIPC to make the claim that pulling back detailees by agencies, as well as sporadic participation, will indeed hamper the NIPC's efforts at information sharing.

Currently, the participation of other agencies, including DoD, is dwarfed by the contribution of the FBI itself to the office's staffing and funding. This will soon turn NIPC into an FBI office rather than an interagency office, and that will have a serious impact on all aspects of the operation. (NIPC's preferred solution would be to increase staffing from other agencies. The task force agrees, but this will happen only if information-sharing problems can be solved.)

DoD should not follow the example of the Secret Service and simply decamp – at least not without attempting to negotiate a broader and more reasonable framework agreement with Justice and the FBI. The task force does not believe that NIPC's problems are necessarily fatal, or that a "go it alone" approach is a better solution for DoD. NIPC continues to be the best window into law enforcement information about network attacks. While its reputation in the private sector is decidedly mixed, it does obtain important information from cooperating companies as well. And so many network attacks are ultimately of little practical interest to DoD that it should allow other agencies to take the lead in addressing them. Withdrawing from NIPC would run a risk of weakening both NIPC and DoD. If possible, it would be far better to

---

NIPC and FBI policies on handling law enforcement information. Moreover, the FBI required other law enforcement agencies – such as the United States Secret Service – to abide by the same agreement, even though *posse comitatus* was not an issue. Indeed, the Secret Service balked at signing the MOU, because it was unduly restrictive, believing as we do that there was no sense in agencies detailing personnel if the detailed employee could not share information more freely with his or her agency of origin.

reform NIPC to make it truly interagency in spirit rather than a captive of law enforcement policies.

While information-restricting law enforcement doctrines need to be addressed in any framework agreement, they are not the only issues that should be covered in high-level talks between DoD and Justice. DoD's own practices in sharing information and choosing detailees are appropriate matters for concern on the part of NIPC. So too is the current placement of NIPC within the FBI hierarchy, which hinders the functioning of NIPC as a truly interagency body.[3] Finally, there is no written agreement on NIPC's role in such obvious questions as whether it is better to lock a particularly dangerous intruder out of a system or to let him in and watch him in the hopes of learning what damage he is capable of causing.

Drafting an agreement that covers all of these aspects of NIPC's operations may be the only way to engage the attention of decision makers within DoD and Justice/FBI, and to ensure that NIPC's critical early-warning mission will be given higher priority than each agency's turf concerns.

The remainder of this section recommends specific reforms that the task force believes should be incorporated into a framework agreement between DoD and Justice/FBI.

RECOMMENDATION 1.1:

All information held by NIPC about infrastructure attacks should be available to DoD unless sharing the information would violate a legal prohibition. DoD should provide similar assurances for information in the hands of its agencies.

Neither NIPC nor DoD has been a model of information sharing. Complaints about unnecessary barriers to information sharing can be heard in both camps, and with good reason: in each agency, there are cultural limits to information sharing. Nonetheless, the task force judges the problem to require more attention on the NIPC side, primarily because that is where the information about network attacks is being centralized.

It is easy to understand the sensitivity of some law enforcement information. The name of a suspect, the identity of a source inside a criminal organization, the effectiveness of a particular investigative technique – this kind of information is jealously protected by law enforcement agencies. Indeed, NIPC fears that if FBI agents were told that NIPC intended to distribute such information throughout the government, they would stop talking freely to NIPC, leading to a new wall between the FBI and other agencies – but this time with NIPC on the other side of the wall.

NIPC has tried to satisfy law enforcement concerns while at the same time finding ways to share information with others. In general, it uses two methods. First, it sanitizes its reports to remove the most sensitive law enforcement sources and methods while still providing useful information. Second, it supplies information marked "law enforcement sensitive," a designation

---

[3] Concern has been expressed at DoD that, in the latest reorganization, NIPC has found itself "buried" in the terrorism division of the FBI. Treating NIPC like any other FBI program heightens the impression that it is simply an FBI office that happens to benefit from free labor provided by other agencies. It is also difficult to run an interagency process that, when complete, must climb the FBI and Justice bureaucracies through several levels. This issue is not without its difficulties. Viewed as a "line" office, NIPC is not big enough to be an FBI division by itself, and so giving it a direct report to the Office of the Director would require treating it more like the FBI staff offices, such as Office of General Counsel.

Page 1152 of 3957

that is similar to the designation "Originator Controlled (ORCON)" in the classified world, telling readers that the information may not be further circulated without the approval of the originating agency. According to NIPC, including the CIA detailee in charge of information sharing, these methods have allowed NIPC to share practically everything of value to other agencies.

NIPC sees the use of the "law enforcement sensitive" concept as a valuable tool that favors sharing. The task force is more troubled by it, particularly because the doctrine is both vague and broad. As set forth in a more detailed NIPC protocol on information sharing procedures, dissemination may be limited to shield "a protected source, sensitive method, [or] confidential witness," categories where restrictions might be justified if interpreted narrowly. But the protocol also protects even broader and more questionable categories of information, such as information identifying juvenile suspects, or information about cases that are awaiting trial. Even information in cases that have been closed can be restricted if the investigating agency thinks disclosure would compromise its sources and methods.

Understandable as the concerns of law enforcement may be, they do not justify such a broad set of restrictions – especially if the interpretation is left solely to law enforcement. Such a decision-making process lacks checks and balances. It does not utilize the more recognized (and in the view of the task force, more disciplined) classified information system familiar to national security agencies. And it makes law enforcement agencies the final authority in disputes about information sharing. The task force welcomes NIPC's assurance that the doctrine is rarely used to prevent sharing of relevant information. If so, it should be possible to adopt a default rule that calls for sharing in the absence of specific factors – and that allows DoD to participate in the decision about whether sharing is justified.[4]

In the task force's view, sharing of information about serious attacks should be automatic unless the sharing would violate a specific legal ban (such as Rule 6(e) of the Federal Rules of Criminal Procedure, which prohibits the sharing of grand jury information) or unless there is an interagency determination that the risk of compromising sources and methods requires the restriction. The task force discusses in later recommendations ways to minimize the adverse effects of legal restrictions on sharing. The recommendation that the risk of compromise be weighed against the value of the information bears further discussion here.

It is worth remembering that the principal justification for the "law enforcement sensitive" doctrine is preventing the compromise of a current or future criminal investigation. And it is obvious that this is a severe risk in some criminal contexts: investigations of organized crime, for example, are susceptible to compromise with consequences that can be fatal for the investigators. But the likelihood that sharing NIPC information with DoD will have such effects is vanishingly small, particularly because NIPC will have information mainly, if not exclusively, about criminal investigations of hackers, who are not known for bribing officials to gather intelligence or for adopting the other techniques of organized crime. More importantly, there is no reason to think that sharing NIPC information with DoD officials is more risky than sharing the information with criminal investigators or prosecutors. DoD is entrusted with far more serious secrets than a

[4] NIPC has pointed out that DoD and other agencies do, in fact, have detailees at NIPC, and some of these detailees are already in a position to approve dissemination of information that is law enforcement sensitive. This is a good thing, but it is not the same as giving DoD an institutionalized voice in the decision.

Page 1153 of 3957

handful of investigative details in a hacking case, and its record of protecting secrets is at least as good as the FBI's and the Justice Department's.[5]

In fact, NIPC does not defend its restrictions on strictly law-enforcement grounds. It argues that the risk of compromise extends not only to individual criminal investigations, but also to general investigatory techniques, many of which are likely to be important to DoD as well as law enforcement. In these circumstances, the issue more closely resembles a classic intelligence "sources and methods" problem, and the usual tactics employed by the intelligence community to solve such problems should work.

It is for this reason that the decision as to whether to share information about an investigation should not be made exclusively by prosecutors and investigators. DoD must be given a voice in that decision, perhaps by designating an official from the Office of General Counsel who would always be trusted with investigative information as part of the interagency sharing process. (The task force notes that twenty-five years ago, intelligence agencies objected to the involvement of the Justice Department in their activities because they feared that prosecutors would be unable to protect intelligence sources and methods; those concerns have now been resolved by long practice. That prosecutors and investigators fear for the security of their special secrets is equally understandable -- and equally wrong.) Involvement of decision makers with different perspectives is an important guarantee of objectivity, but in the end the important thing is not just the process itself, but the principle that those who want to restrict information sharing must justify that view to other parts of the government. The default should be that the information is available to DoD and its agencies.

A second reason often advanced for not sharing investigative information is privacy. This report will address statutory privacy protections separately, but even where statutory restrictions do not apply, the task force agrees that protecting privacy is an important value that NIPC and other agencies need to bear in mind at all times. At the same time, it is worth remembering that NIPC can only share information about private citizens that it already possesses – in other words, information that is already in the hands of at least one and probably several government agencies. It is reasonable to question how well privacy is protected by keeping information that has already been widely shared within the law enforcement community out of the hands of Defense Department analysts. A more effective protection would focus on preventing misuse by all the parties that have access to the information.

As stated at the outset, in focusing on the barriers to information sharing that have been erected at NIPC, the task force does not mean to suggest that this practice runs only one way. NIPC has cited its own examples of information withheld arbitrarily by NSA and perhaps other DoD elements. NSA and NIPC are seen as competing for similar missions and resources, and as is typical in such cases, each side has a store of grievances against the other. The task force recommends that DoD and its elements also make binding assurances that information will be shared with NIPC unless it is subject to legal restrictions. Both parties should ensure that NIPC personnel have clearances that are adequate to facilitate this information sharing and that there is a process for resolving disputes about which classified information may be shared with NIPC.

---

[5] In rebuttal, NIPC and Justice point to an occasion on which a high-ranking DoD official briefed an ongoing attack and investigation to Congress only to have details leak to the press. This of course is unfortunate, and it has happened too often to every agency that depends both on secrecy and on Congressional favor. But every agency tends to remember the times when other agencies have been the source of a leak and to forget those in which it was the source. Keeping information away from DoD is not an appropriate solution to the problem of "political" leaks.

Page 1154 of 3957

RECOMMENDATION 1.2:

NIPC should share all information about network attacks with the National Security Council and its staff unless the information is likely to compromise an investigation of a White House official.

If NIPC is to participate in national security planning and decision making, it must obey the same rules as other participants in that process. This includes providing all necessary information to the interagency process administered by the National Security Council (NSC). Currently, NIPC is unable to do so – a serious handicap that should be cured either by agreement between DoD and the Department of Justice or by the President.

Restrictions on FBI communications with the White House were imposed in 1994 in an agreement between the White House Counsel's Office and the Office of the Attorney General. Under that agreement, the FBI may not provide any information to a member of the White House staff except with the approval of the Deputy Attorney General (DAG). The purpose of this restriction is to prevent actual or apparent White House interference with or influence over criminal investigations. The arrangement gives the Deputy Attorney General an assurance that he is fully aware of any communications between the FBI and the White House.

In the context of NIPC, this restriction on sharing information is dysfunctional. During the Clinton Administration, defense against foreign-based infrastructure attacks was coordinated by a senior NSC official. Delaying the delivery of information to the NSC is not good management, and NIPC itself has asked Justice to modify the rule in this context, so far without effect. The NSC is a well-established mechanism for coordination of national security issues with interagency dimensions. In their defense, the Justice Department and NIPC emphasize that in the end practically everything the NSC wanted to know was provided by NIPC. The task force found that, on some occasions, the transfer of information to NSC has gone smoothly – as one official told us, "DAG approval can take 20 minutes." But in other cases, there have been significant delays in delivering information to the National Security Council due to disagreements between Justice and NIPC over what information should be supplied to the national security staff. Justice officials said they sometimes felt forced to choose between having their best technicians respond to attacks and having the technicians respond to what they called "drive-by tasking" from the NSC.

The task force did not try to decide whether NSC had asked for unnecessary or burdensome briefings, although it was noted that this is a widely held view at NIPC and the Justice Department. But even if that view is correct, Justice should not have responded by claiming the legal right to withhold information from NSC. DoD depends on the NSC to address interagency issues that arise when national security is threatened. The NSC process is well-oiled and has functioned predictably in a host of conflicts, and NSC is the logical place to address network attacks with national security implications. If agencies can refuse to provide information to that interagency process, they will always be tempted to withhold information that makes them look bad. Again, the default should be in favor of sharing information. In the long run, busy NSC officials are unlikely to ask for information that is not relevant to their jobs.

What of the concern that led to the no-White-House-briefings rule in the first place? The task force does not denigrate the concern that White House communications can lead to charges

Page 1155 of 3957

of interference in a criminal investigation. For that reason, the task force agrees that NIPC should be free to refuse to provide information that would compromise an investigation of White House staff. But there is little reason to use a broader rule in this context. Criminal investigations of hackers will often have national security dimensions. So far, however, no one has raised the slightest suggestion of political interference. Until the risk of politicization of network investigations is something other than theoretical, this restriction should be lifted.

This change could be accomplished by a blanket approval by the Attorney General for the sharing of information on attacks with national security significance. But such approval has not been forthcoming, and it therefore should become the subject of high-level agreement between DoD and Justice.

Once again, the task force notes that this restriction falls into a pattern, in which FBI and Justice entities that are tasked with interagency responsibilities attempt to justify restrictions by saying that they are simply applying the Justice/FBI rules that usually apply to "criminal investigations." That is precisely the problem: these investigations are not exclusively matters of concern to prosecutors and investigators, and they cannot be treated as though Justice Department policies are the beginning and end of analysis. Unless the "business as usual" mentality at Justice and the FBI can be shaken loose in some form of agreement, DoD will have to create its own, separate capabilities, free of parochial constraints imposed for law enforcement reasons.

RECOMMENDATION 1.3:

Title III intercept information should be shared with DoD for purposes of assisting DoD in preventing attacks on its computer networks.

Sooner or later, usually sooner, any serious investigation of a network attack requires a wiretap. This allows investigators to intercept the communications between an attacker and the sites the attacker uses to launch (or launder) his attacks. Electronic intercepts are a fundamental tool in combating network attacks. But as things now stand, they usually can only be performed as part of a criminal investigation using the authority conveyed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. (Foreign intelligence intercepts can also be used inside the United States, but only if the target is an agent of a foreign power – something that is difficult if not impossible to determine at the outset of a hacker investigation.)

Use of criminal wiretap authority is in some respects easy. Hacking into other people's computers is a crime, so that the prerequisites for a Title III intercept order for data may be quickly met. But there's a catch. Once the data has been gathered under a Title III order, it may not be shared with DoD or other national security bodies. At least that is the view of the Justice Department, which interprets Title III as prohibiting such sharing. In the task force's view, the Justice Department's reading of Title III is at best arguable, and shows far too little concern for national security.

The statutory language in dispute is not lengthy. Under Title III, information derived from an intercept may only be used "to the extent that such use is appropriate to the proper performance of [the] official duties" of the law enforcement officer who has obtained the information. (*See* 18 U.S.C. § 2517 (1) and (2)).) This language would not bar DoD from receiving Title III information if "the official duties" of law enforcement officers include

Page 1156 of 3957

protecting national security and preventing additional crimes. At one time, the Justice Department's Office of Legal Counsel (OLC) took a similarly broad view of the "official duties" language, concluding for example that the Justice Department could provide Title III information to congressional committees on the theory that responding to congressional inquiries is part of a government employee's "official duties." No longer -- after considerable delays, the OLC has recently issued an opinion that overrules its earlier interpretation and concludes that Title III authorizes only sharing of intercept information for official *law enforcement* uses.

The OLC opinion further concludes that this ambiguous intent is not overcome even by the National Security Act, which expressly grants the Director of Central Intelligence "access to all intelligence related to the national security which is collected by any department, agency, or other entity of the United States." (*See* 50 U.S.C. 403-4(a)(1994)). Finally, it dismisses a Reagan-era executive order directing all agencies to give the director of Central Intelligence "access to all information relevant to the national intelligence needs of the United States." (*See* Executive Order 12333 (1981))[6]

In the view of the task force, the OLC opinion is questionable as a matter of statutory construction, and it almost willfully ignores the national security implications of its conclusions. A careful reading of the law, as well as strong public policy concerns, argue in favor of the disclosures at issue here. OLC's contrary decision casts real doubt on the willingness in the Justice Department to give due weight to Defense Department interests when carrying out missions that mix national security and law enforcement.[7]

The OLC opinion suggests that it is appropriate to lean against sharing of Title III data because of privacy concerns. Privacy is indeed important, but as noted earlier one may wonder: will the targets of Title III wiretaps really be comforted by the knowledge that the contents will be provided to prosecutors' secretaries, perhaps even to IRS auditors – but not to defense and intelligence authorities? There is of course an extra bit of privacy in any restriction on distribution of private information, but it is difficult to agree with the Justice Department's decision to treat this relatively minor gain for privacy as more important than the significant loss in terms of national security. The additional privacy benefit is particularly attenuated in the context of hacker intercepts. What makes classic wiretaps so troublesome from a privacy perspective is that they capture often-intimate conversations between parties who trust each other and believe their conversations will remain private. But intercepts of hacker attacks are typically focused on signals sent by the hacker to a victim's computer. The tap simply provides a quick

---

[6] We should note that this opinion was resisted by NIPC on grounds that it is unnecessarily restrictive, while at the same time one of the principal OLC contributors to the opinion is now part of the office of the DoD General Counsel.

[7] Other aspects of the opinion do little to dispel this view. For example, OLC determines that intelligence agencies will be allowed access to intercepts in one circumstance – when they have been firmly subordinated to law enforcement and are simply putting their resources at the disposal of prosecutors and criminal investigators. *Then*, the opinion declares, there is no problem with sharing intercept information. In short, if the Justice Department's interests are served by sharing, the sharing is legal; if not, not.

The opinion also contains a remarkable passage to the effect that if a law enforcement intercept produces urgent national security information, then the President can order that it be shared with intelligence agencies. Given the National Security Act and Executive Order 12333, one might think that Congress had already authorized such an order and that the President had already issued it, but having rejected that obvious conclusion, the opinion is forced to find that the President has retained some inherent authority to order such sharing anyway, but that the authority should only be exercised in desperate circumstances. The opinion takes a convoluted course to arrive at a position that could have been achieved by giving a straightforward reading of the National Security Act.

Page 1157 of 3957

way to capture keystrokes that are themselves part of the crime and that would not qualify under most people's definition of a communication, let alone a communication entitled to the highest possible privacy protection. These keystrokes may well be protected by Title III, but it is difficult to justify expanding their protection in the face of a law and an executive order that clearly require the Justice Department to share any intelligence relating to national security.

An OLC opinion is binding on the executive branch, but interpretations can be overturned, as this one overturned an earlier decision. The task force urges that the opinion be reconsidered in the context of a broader agreement on NIPC's information-sharing policies.[8]

RECOMMENDATION 1.4:

Rule 6(e) on sharing grand jury information should be clarified to permit sharing for national security purposes; until this is accomplished, computer crime investigators should be prohibited from using grand jury subpoenas without the express approval of NIPC, acting with interagency agreement.

Unfortunately, Title III is not the only criminal provision that prevents defense and intelligence agencies from gaining the full benefit of information obtained by criminal investigators about network attacks. Another provision with an impact on information sharing is Rule 6(e) of the Federal Rules of Criminal Procedure, which provides that attorneys for the government "shall not disclose matters occurring before the grand jury, except as provided for in these rules." Specifically, information may only be disclosed when permitted by the court, or to an attorney for the government or to "such government personnel ... as are deemed necessary by an attorney for the government to assist an attorney for the government in the performance of such attorney's duty to enforce federal criminal law". (*See* Rule 6(e)(3) (A) and (C)).

Unfortunately, the Justice Department has taken a narrow view of its authority to share information under this rule. To make matters worse, NIPC has taken an expansive view of what materials are covered by the rule. And, finally, Justice Department prosecutors continue to use grand jury subpoenas where other processes could be equally effective, unnecessarily expanding even further the body of material to be withheld from DoD and other agencies.

This report examines each of these three concerns separately. But first, it may be worthwhile to note that grand jury secrecy, while often praised as a protection for criminal suspects' privacy, actually serves the prosecutors' interests at least as well as the defendants'. The privacy rationale is that grand jury secrecy protects those who are investigated and not indicted, or not

---

[8] If this cannot be done, we suggest that NIPC and the Justice Department maximize "parallel sourcing" of information that might otherwise only be obtained through the use of Title III. For example, some information produced from a wiretap targeting a hacker would also most likely be available directly from the computer of the victim, particularly once monitoring software was installed. We recognize that this is not a complete solution; if all the information produced by a wiretap could be harvested in another fashion, the wiretap would not be approved, since by law an intercept can only be used with necessity. Nonetheless, procedures to automate and make routine such parallel sources are worth considering. (Even this limited solution creates new difficulties, however. While systems administrators have nearly total discretion to install monitoring software to protect their systems, the Justice Department fears that the use of such software at the direction of criminal investigators will lead to legal problems later. The victim of the attack and its system administrator may find themselves deemed to be agents of law enforcement if they cooperate too enthusiastically with the FBI and Justice. This is yet another example of a problem we encountered over and over; while law enforcement authorities provide a quick basis for gathering information about network attacks, they often bring with them so much encrusted criminal law doctrine that in the end the use of law enforcement authorities may not be worthwhile. We discuss later in the report some methods of addressing this problem, including the use of a civil remedy that avoids the need to bring in criminal authorities.)

Page 1158 of 3957

indicted for everything examined in the investigation. In this vein, keeping grand jury proceedings secret prevents the release of derogatory information that ultimately was insufficient to persuade the grand jury to charge a crime. In this context, of course, it is *public release* of the information that is most important to prevent – the information is not kept from investigators, prosecutors, or the grand jurors. Thus, as a matter of policy, this vital privacy interest would seem to be best protected by making sure that any officials who have access to the information are subject to a confidentiality requirement.

It is not clear that barring dissemination of grand jury information to DoD personnel – who may already be subject to more stringent confidentiality disciplines than Rule 6(e) – adds much in the way of privacy protection for those under investigation. This is particularly the case today, when practically any harm to U.S. vital national security interests can also be investigated as a crime. In such investigations, the national security and criminal processes are already intimately coordinated. As a result, the national security agencies know quite well who is being investigated for, say, a major terrorist incident, and they already know what information the criminal investigators hope to obtain from the criminal process. In those circumstances, the suspects' privacy interest in preventing DoD from knowing that they are suspects is already fatally compromised. The case for withholding grand jury information from DoD on privacy grounds in cases where national security is at stake thus seems questionable at best.

Of course, prosecutors have their own reasons for defending the principle of grand jury secrecy, one that has nothing to do with the privacy of the suspect. Grand jury secrecy rules allow prosecutors to keep an investigation secret from the defendant, thus reducing risk of flight, intimidation of witnesses, and premature disclosure. While the commitment of prosecutors to keeping their plans secret is praiseworthy, in the task force's view this commitment must be balanced against the security needs of the nation. Prosecutorial secrecy cannot be absolute, and Rule 6(e) should not be read to protect it absolutely. Again, in almost every case of national security concern, such as terrorism investigations, criminal investigators are likely to reveal all facets of their investigations to the national security agencies and personnel involved in the investigations. Law enforcement already expects national security personnel to protect investigators' secrets as intensely as they protect classified information, with generally good success. Given all that, there is no obvious policy reason why the fruits of one particular investigative technique – grand jury subpoenas – should be kept from DoD to protect the prosecutors' interest in confidentiality.

A. Dissemination of grand jury information to DoD should be permitted

Given the weakness of the policy reasons for not sharing grand jury information, and the vital importance of allowing DoD access to information with a bearing on national security, the Justice Department should have taken a broad view of the dissemination authority already provided in Rule 6(e). As mentioned above, the rule allows dissemination to "such government personnel ... as are deemed necessary by an attorney for the government to assist an attorney for the government in the performance of such attorney's duty to enforce federal criminal law". (*See* Rule 6(e)(3)(A) and (C).) If the "duty to enforce federal criminal law" includes preventing or deterring assaults on networks of national security concern, sharing 6(e) information with DoD for that purpose is completely permissible. Since the rule also seems to leave the final decision to the attorney for the government and what he or she has "deemed necessary," one would have thought that a broad interpretation was eminently sustainable. After all, courts have allowed

Page 1159 of 3957

prosecutors to share 6(e) information with state bar grievance committees, judicial councils investigating a judge's misconduct, and congressional committees considering impeachment. It is not unreasonable to conclude that protecting DoD networks from what may be state-sponsored attacks would be at least as important to the enforcement of federal law as disciplining private members of the bar.

In 1997, however, the Office of Legal Counsel once again adopted a position that does little to accommodate the concerns of national security bodies. Despite the sweeping language of the National Security Act, which commands all federal agencies to provide all intelligence-related information to the Director of Central Intelligence, OLC gives conclusive weight to one line from a 1983 Supreme Court decision, *Illinois v. Abbot & Associates, Inc.* In that case, the court refused to give state attorneys general access to federal grand jury testimony despite a federal law requiring the Attorney General to disclose information to state authorities in joint antitrust enforcement matters. In that context, the court declared that "we will not infer that Congress has exercised [its power to override grand jury secrecy] without affirmatively expressing its intent to do so." (*See Illinois v. Abbot & Associates, Inc.*, 460 U.S. 557, 572-73 (1983))

In the light of the Supreme Court's language, OLC's reasoning here is more justifiable than its opinion on Title III, but it is still highly questionable. One may reasonably doubt that the Court would have applied the same reasoning in the context of legislation on national security – a field where Congress speaks only rarely and then in the most general terms. But OLC saw no reason to hesitate; it applied the Court's language without regard for context. This application would be moderately persuasive if OLC had been willing to accept the logical consequences of its position. But OLC faced the obvious risk that such a strict rule would lead to disaster in the real world – where criminal and national security concerns overlap ever more often. What would happen, OLC was asked, if grand jury testimony uncovered vital matters of national security that then could not be disclosed to intelligence authorities (e.g., a plot to bomb an allied government facility abroad)? In the face of this concern, OLC faltered. If such information was uncovered, OLC declared, the President would have "inherent" authority to receive and order the sharing of information covered by Rule 6(e). This of course is the only responsible answer. But if the President has that authority, it is unconvincing to suggest that the President did not exercise it when he issued Executive Order 12333, which already requires all agencies to share intelligence information of any kind with the Director of Central Intelligence.

In short, the 1997 opinion is internally inconsistent and deserves reconsideration in the context of a broader agreement on information sharing about network attacks.

B. Materials obtained by grand jury subpoena should be shared with DoD.

The restriction on sharing grand jury information raises a second question: what is the scope of this restriction? Clearly, testimony given before a grand jury is a "matter occurring before the grand jury." If that were the full scope of the Rrule, it probably would not be worth discussion here; such testimony rarely figures in investigations of the sort that NIPC conducts. (Moreover, if the same statements are made in the grand jury and in interviews to agents prior to grand jury testimony, as is often the case, the interview notes can almost always be divulged without running afoul of Rule 6(e).)

The problem is that Rule 6(e) can be read as extending not simply to testimony, but to documents and other information obtained by means of a grand jury subpoena. If Rule 6(e) is

Page 1160 of 3957

read as barring DoD access to such information, it will impose significant barriers to prompt and easy sharing of information about network attacks with national security significance.

This task force is not in a position to canvass all of the case law about how Rule 6(e) might apply to subpoenaed materials, except to note that there is some divergence in the courts on this point. Prosecutors have successfully argued in some cases that disclosure of subpoenaed materials might disclose the direction of the grand jury's inquiries.[9] Given this tactical value to prosecutors of grand jury secrecy, it is understandable that the FBI and Justice Department have reason to give Rule 6(e) a broad scope. Even so, there is reason for concern that NIPC's information-sharing protocol goes well beyond the requirement of Rule 6(e). For example, it expressly states, "For purposes of this Protocol, Grand Jury information also includes any material obtained pursuant to a grand jury subpoena." It is not limited to testimony or even to materials that would disclose the grand jury's lines of inquiry.

Whatever the reasons, it is difficult to see why the FBI or Justice should insist on this broad interpretation in the context of sharing information with DoD. Privacy concerns are particularly limited in this context. First, confidentiality agreements can be used to prevent DoD personnel from publicly releasing data in question. Second, whether subpoenaed information is protected by Rule 6(e) is often a matter of mere chance. Information identical to that obtained through a grand jury subpoena may usually be obtained by means of other criminal process that is not subject to Rule 6(e) – grand jury subpoenas are often used simply because they are faster or simpler to obtain than court-ordered discovery. Privacy is tenuous at best when it depends on the form that an investigator happens to fill out in the course of gathering evidence. And information should not be withheld from national security agencies simply because law enforcement used the path of least resistance to obtain it.

C. Investigators' use of grand jury subpoenas should be more effectively disciplined.

If it proves impossible either to limit Rule 6(e) to grand jury testimony or to give full effect to the executive order already requiring intelligence sharing, the difficulties arising from Rule 6(e) can still be minimized. Justice and the FBI could take internal action to greatly reduce the impact of Rule 6(e) on NIPC's ability to share information.

While it is legally necessary for the government to use some form of criminal process to obtain subscriber information from Internet Service Providers, investigators often have a choice of methods. They can obtain the information through grand jury subpoena or through an order under 18 U.S.C. § 2703(d). Information gathered under section 2703(d) is not subject to Rule 6(e) or its restrictions. The practical problem is that grand jury subpoenas are easier and faster to obtain – prosecutors need only show that the information sought is relevant to a criminal investigation. In contrast, obtaining a court order under section 2703(d), which would make a broader range of information available to investigators than that released pursuant to a subpoena, requires that the prosecutor state specific and articulable facts showing that evidence relating to a crime will be obtained, and present the proposed order to a judge.

A prosecutor or investigator in a hurry is likely to use a grand jury subpoena without worrying much about the problems it will later cause to other agencies in need of the

[9] Again, it is worth noting that this consideration is of doubtful weight in a context where investigators' non-grand-jury inquiries are already thoroughly coordinated with national security agencies.

Page 1161 of 3957

information. Current Justice Department policy encourages prosecutors to consider alternatives to grand jury subpoenas, but it is not clear that this suggestion is enforced by more than suasion. NIPC and Justice should establish rules prohibiting investigators and prosecutors from using grand jury subpoenas in investigating network attacks unless no other form of process will be as effective. Furthermore, investigators and prosecutors who persist in the use of grand jury subpoenas should be disciplined. The task force recognizes that sometimes speed is essential, and a grand jury subpoena is the fastest option. In that event, a second form of process should also be used to obtain the information in shareable form.

D. Legislative and executive solutions should be explored.

In the absence of (or in addition to) any other action, the position taken by OLC on sharing of grand jury information with DoD could be corrected, either by Congress or by executive order. Congress could make it clear that the National Security Act does indeed allow sharing of grand jury information with national security authorities. And the President could make it clear that Executive Order 12333 is intended to have the same effect. (In the context of national security, where the executive's authority is great, an executive order expressly requiring the sharing of Rule 6(e) information would very likely meet the "express statement" requirement set by the Supreme Court in *Illinois v. Abbot*.)

Before turning to the next recommendation, it should be noted that Justice and NIPC both take the view that Rule 6(e) has not often been a serious obstacle to information sharing in the context of network attacks. The task force agrees that a properly administered interpretation of Rule 6(e) should resolve most of the concerns. At the same time, no one asserts that Rule 6(e) never has or never will cause difficulties in the context of national security or network attacks. Moreover, Rule 6(e) is one of the obstacles to information sharing that is invariably raised by law enforcement as an essentially unsolvable legal problem. Coincidentally, this "unsolvable" problem also prevents complete openness with non-law-enforcement personnel, and ultimately forces a sharp distinction between the groups. In the task force's view, this insistence on separate regimes is itself likely to be a source of continued conflict and inefficiency. Every effort should be made to reduce or eliminate legal and cultural barriers to a seamless interaction of DoD and law enforcement personnel in the area of critical infrastructure protection.

RECOMMENDATION 1.5:

NIPC should report directly to the Director of the FBI and the Deputy Attorney General.

NIPC is – or could be – a vitally important interagency office. Assuming it can overcome the information-restricting policies criticized above, it has a large role to play in identifying and helping to respond to critical infrastructure attacks.

At present, however, NIPC is buried deep under a heavy FBI bureaucratic structure. It must pass through several levels of review before it can reach a Presidential appointee of any kind. This of course has unfortunate consequences for the office itself, but the concern is for the interagency process. It simply is not credible for the head of NIPC to perform an interagency coordinating function if his decisions must clear through three or four levels of FBI review before they reach the Director (let alone the Justice Department). Other agencies with flatter hierarchies will be discouraged from participating in NIPC's interagency coordination process if

Page 1162 of 3957

the decisions reached in that process are subject to reconsideration at the insistence of mid-level FBI officials.

Indeed, some of the information-sharing disputes described to us festered longer than necessary because there was no ready way to escalate and resolve the issue at a level where some perspective could be achieved.

The task force recognizes that offices the size of NIPC rarely report directly to the Director of the FBI. For administrative and budgetary purposes, it may make sense for NIPC to be subsumed into a larger whole. But for policy and interagency matters, it should have a direct line, at least to the Director. Because resort to a political appointee may often be necessary to resolve interagency disputes, the task force also believes that NIPC should have direct access to the Deputy Attorney General.

RECOMMENDATION 1.6:

As part of a satisfactory framework agreement, DoD should upgrade its contribution to NIPC.

Although DoD's contribution to NIPC staffing is the largest outside the FBI itself, DoD has not sent as many detailees as it could, nor has it taken all possible steps to make a detail to NIPC as attractive as possible. In part, this may reflect doubts about whether detailees will be able to provide value to DoD while serving at NIPC. Assuming that problem is solved satisfactorily, DoD should take action to make sure that it sends a larger contingent of experts and properly supports them while on detail.

In general, this means that tours at NIPC should be two years, something toward which DoD now strives with only partial success. In addition, DoD should strongly consider making service at NIPC a "joint" assignment of the sort necessary for promotion to the higher ranks of the armed services. This would increase its attractiveness as a posting for military officers, and would help to ensure that NIPC is staffed with the highest quality detailees possible.

RECOMMENDATION 1.7:

DoD should clarify the role of NIPC in deciding how to respond to intrusions into DoD networks.

Any institution faced with a hacker, especially a persistent and successful hacker, has to make difficult judgments about whether to give top priority to blocking the attack or to observing the attacker's *modus operandi* in the hope of learning enough to identify or neutralize him. Locking the attacker out stops the immediate hemorrhage, but it may simply teach the hacker to switch to tactics that are less visible to the defenders, making the situation worse rather than better. Additionally, blocking out the hacker eliminates virtually any possibility of identifying the attacker and ascertaining his motives. But watching and waiting means that the hacker will continue to exploit the system.

The question for the government is: who should make the decision as to whether an attack should be blocked or watched? Within DoD the "block v. watch" decision is supposed to be in

Page 1163 of 3957

the hands of the commander whose system is attacked. If more than one commander has information on the systems being attacked, the decision is evidently made by the Joint Task Force – Computer Network Defense (JTF-CND). At least one DoD element has made the decision to deploy tools that could tip off attackers, despite concerns expressed by law enforcement and perhaps other DoD elements about the "noisiness" of such tools. In the course of the debate over how to respond in that case, at least some DoD officials felt that NIPC and Justice were asserting the authority to influence the final decision. NIPC and Justice both deny any intent to assert such authority. Whether or not they did, the fact that neither should make this decision should be clarified in any agreement over NIPC's role in critical infrastructure decision making.

At the same time, assigning responsibility for the decision is not the same as concluding that other agencies have nothing to offer the decision maker. NIPC has established a process for addressing "block v. watch" decisions. NIPC's structure calls for a "senior group" review at which all interested agencies are represented. The senior group is a consensus body. Although NIPC may convene meetings, the head of NIPC is not supposed to have any more authority than any other participant. The senior group review process apparently has been useful in some circumstances, producing consensus decisions about how to handle sensitive investigations.

There are nonetheless some difficulties with this structure. It is not part of any formal understanding with any of the agencies involved. Thus, in the absence of a clearly defined decision path, it would be easy for people to believe that NIPC had assumed unilateral authority over a particular decision. In addition, it is difficult for NIPC's interagency process to truly be a "senior" group when NIPC cannot speak for Justice or the FBI without clearing several internal levels of review.

There needs to be more clarity about the role of NIPC and the senior group in providing advice and making decisions about network attacks, including the "block v. watch" decision.[10] Neither this task force nor NIPC finds fault with the current DoD rule that this decision lies with the commander whose system has been attacked. This allocation of responsibility should be recognized in the agreement between DoD and NIPC. It might also be dealt with by a broader interagency agreement or Presidential directive. But it is crucial that the authority to make the decision be clearly assigned, and recognized by all concerned parties.

RECOMMENDATION 1.8:

NIPC should not make independent judgments about what information intelligence agencies may and may not receive; in particular, it should no longer rely on its erroneous view of NSA's authorities as a reason for restricting distributions to NSA's information security organization. Additionally, neither NIPC nor the Justice Department's Criminal Division should have any role in deciding how DoD entities should share information with NSA or other intelligence agencies.

The final area that should be clarified relates to information sharing with the National Security Agency (NSA). NSA has great resources and experience in this field. In addition to its

[10] It is also important to note that, at least at the outset of an attack, it may be difficult to determine with any precision which systems are involved in the attack and whether the attack is state sponsored.

Page 1164 of 3957

well-known intelligence-gathering mission, it has direct responsibility for the security of DoD information systems. Its experience and analytic capabilities on both the offensive and defensive sides make it a valuable participant in any effort to defend against network attacks. Depriving NSA of information about network attacks should therefore require substantial justification.

In actual practice, NIPC and Justice officials have shown considerable reluctance to give NSA information about network attacks, a reluctance that has often been justified by reference to legal concerns. But the need for clarification goes well beyond NIPC. In fact, even DoD itself has shown confusion about what information may lawfully be shared with NSA.

NIPC in particular frequently suggested that information sharing with NSA should be restricted to prevent an intelligence agency from gaining access to information about U.S. persons. There are two problems with this approach.

First, NIPC, the FBI, and indeed most of the Justice Department simply lack the expertise necessary to determine what limits apply to intelligence agencies' use of information. In general, intelligence agencies are barred from targeting Americans for surveillance, but they are not barred from reviewing information gathered elsewhere about Americans. (Any other rule would call into question the distribution of U.S. newspaper clips at intelligence agencies.) As a general rule, legal restrictions on intelligence agencies are grounded in the conviction that the fearsome capabilities of these agencies should not be aimed at U.S. citizens. But information in the hands of NIPC has not been gathered by intelligence agencies. Thus, allowing intelligence agencies to examine such information for analytic purposes does not point U.S. intelligence capabilities at American citizens.

Second, there is no reason to think that the usual intelligence oversight mechanisms are not functioning, or that NIPC or the Justice Department's computer crime experts should act as an intelligence oversight body. NIPC in particular should not seek to act as NSA's watchdog in a context where its actions might be construed as simply defending turf. In general, if there are questions about the lawfulness of intelligence agency access to particular information, NIPC's job should be limited to raising the issue with the relevant agency's general counsel, the Justice Department's Office of Intelligence Policy and Review, or both.

Along the same lines, the Justice Department's Criminal Division has encouraged a much-too-narrow view of when DoD may share with NSA information that it acquires in the course of administering security measures. The Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) has argued that a DoD systems administrator should not share information about attacks on DoD systems with intelligence agencies. This is a harsh limit, since it prevents NSA from analyzing hacker tactics even when the hackers are attacking DoD's own computers. The origins of this notion lie deep in Justice Department lore. But in the task force's view, that lore has little relevance in other contexts.

Broadly speaking, Title III and its progeny make all intercepts of electronic communications illegal in the absence of a statutory exemption. This creates a potential problem for network operators and systems administrators, who often are exposed to the contents of communications over their networks and who sometimes actively monitor those communications to protect against security breaches. To make sure that this activity was not outlawed, Congress provided that the agents of a service provider may monitor communications "while engaged in any activity which is a necessary incident to the ... protection of the rights and property of the provider." In

Page 1165 of 3957

reliance on this provision, system administrators may record every keystroke a hacker makes while on their systems.

Sooner or later, instead of just watching the attacker, systems administrators may decide to call in the police. But unlike the systems administrator, the police may not simply record all of the communications of a criminal suspect, unless they have a court order. Faced with such a burden, the police are naturally tempted to ask the system administrator to continue monitoring for purposes of gathering evidence. To avoid this result, courts and the Justice Department have sought to prevent investigators from "tasking" service providers or otherwise turning systems administrators into agents of law enforcement.

At some point however, the Computer Crime and Intellectual Property Section came to believe that, if police and prosecutors could not work closely with systems administrators, then neither could intelligence agencies like NSA. The theory was that Title III only allowed monitoring of networks for security purposes, not for purposes of law enforcement or intelligence gathering.

There are two problems with this conclusion. First, it mischaracterizes NSA as simply an intelligence agency. While NSA does indeed gather signals intelligence, it also has another and quite separate mission – information security. This is carried out by a large office devoted entirely to providing information security for DoD. This office is not part of the intelligence community, it has no intelligence role, and for that reason it is not subject to the intelligence-targeting restrictions that apply to the intelligence side of NSA. In short, there is no reason to deny NSA's information security office access to information on the basis of intelligence agency limitations.[11]

Second, there is reason to doubt the Justice Department's assumption that if the police and prosecutors may not work closely with systems administrators monitoring a hacker, then no one may. In fact, police and prosecutors are subject to strict, court-enforced rules about how they gather evidence against criminals, and any deviation from those rules is likely to draw careful scrutiny. Therefore, for reasons having to do with public policy and judicial oversight, prosecutors are not allowed to circumvent those restrictions by "laundering" their evidence-gathering through systems administrators.

This is the most reasonable reading of the system administrator exception to Title III. For many reasons, systems administrators need broad authority to conduct monitoring, and as long as that monitoring has a plausible relation to a security concern, their actions must be lawful. Any other rule would require systems administrators to walk a knife edge each day, with the constant threat of felony prosecution if their subjective motives were deemed to fall over the fine line between proper monitoring (for a security purpose) and improper monitoring (for some other purpose). If the monitoring has been performed lawfully, Title III gives systems administrators virtually unlimited authority (under Title III) to disclose the results of the monitoring.

---

[11] To be fair, DoD has not always been clear on this point either. For example, doubts have been expressed about whether DoD logs showing the tactics of intruders can be shared with NSA analysts, since the nationality of the intruders cannot be known, though in many cases they hack in from U.S. hosts. The answer appears clear enough. First, the information security side of NSA is part of the DoD computer security apparatus. Anything that a systems administrator can review for security purposes can be shared with NSA's information security office. Since it is clear that doubts on this point remain even within DoD, it should be made plain both inside the DoD and in any framework agreement with NIPC.

Page 1166 of 3957

On that reading, there is little or no basis for the Justice Department to question the sharing of DoD system administrator logs with NSA – or other intelligence agencies for that matter. The ultimate goal of that sharing is better network security, and the role of the intelligence agencies in analyzing and circulating information about attacks is in many ways similar to that of the Computer Emergency Response Team (CERT), which also circulates intelligence gathered from systems administrators about attacks on their systems.[12]

RECOMMENDATION 2:

A Standardized and Simple Set of Procedures Should be Adopted to Allow Unannounced "Red Team" Attacks on All DoD Networks Without Excessive High-Level Intervention by DoD Lawyers.

The task force does not mean to leave the impression that all of the legal difficulties that have hindered DoD's preparations for information attacks can be traced to NIPC, the FBI, or the Justice Department. Some have been home-grown.

The effectiveness of "red team" operations in uncovering vulnerabilities in government computer networks is undisputed. Indeed, these simulation attacks have done much to show just how unprepared the United States is to defend itself against a significant information warfare offensive. In the past, however, conducting a red team attack on a DoD element has required extensive internal approvals, climbing up both the tested and testing agency command structure, and culminating in DoD General Counsel and Secretary of Defense approval on a case-by-case basis. This was because DoD took a belt-and-suspenders approach to the legality of red team intrusions. To ensure that there were no legal questions about the red team's right to gain access to DoD computer files, DoD sought assurances that all users had consented to red team access, which could only be determined after a review of each system. Since DoD users receive consent notices regularly both in hard copy and through system banners, this should not have been difficult to establish, but in the early days of the program, great care was taken to double- and triple-check the consents for each system and each exercise.

The task force believes that this degree of care is no longer necessary. The task force noted that DoD has made real strides lately in reducing the complexity of the red team approval process without any adverse consequences – and with real advantages in terms of security. The approval process is more streamlined, and red-teaming is no longer seriously constrained by determinations of consent. Nonetheless, the Secretary of Defense is still being asked to review individual red team exercises and certify consent. This is an unnecessary burden on the secretary and on the red-team process. Now that red-teaming is becoming a standard part of DoD security measures, the task force recommends that instead of reviewing individual exercises the Secretary simply certify periodically that DoD systems and users have consented to network monitoring.

[12] The fact that some of the information is circulated in classified form makes no difference; systems administrators themselves could choose to centralize corporate security information and circulate it to a limited number of trusted employees, and they could do so without worrying that gathering information for such purposes is somehow outside the scope of their legal authority.

RECOMMENDATION 3:

Specific Legislative Revisions Should Be Made to Facilitate Interagency Information Gathering and Sharing.

The proposals listed above focus on matters of agency policy and procedure that should be revised in order to facilitate more effective defensive information operations. The task force concentrated its attention on reforms that lie, at least in part, within the power of DoD. Of course, nothing would prevent Congress from acting to require a charter for NIPC, or from incorporating any or all of these recommendations for such a charter. But the task force sought to avoid issuing a report that was dependent on legislative action for its implementation.

Nonetheless, it became clear in the course of task force discussions that the current legal framework for defending against information warfare is flawed in several ways that only Congress can cure. The task force did not proceed from the assumption that this framework requires a complete overhaul. Quite the contrary, we resisted recommendations for legislative action whenever we thought the problem could be resolved by a more reasonable administrative interpretation. Despite this resistance, the task force became convinced that some changes in existing law are appropriate if a unified and effective response to information warfare is to be mounted. The task force's proposals for a legislative agenda in this field are contained below.

RECOMMENDATION 3.1:

DoD should have the authority to seek information about network attacks through a civil investigative order, specifically to combat attacks on systems of national concern.

Time and again, efforts to streamline information sharing have struggled with the structure of rules that has grown up around the class of information that is gathered in a criminal investigation. So long as information about attacks is gathered primarily through criminal investigative methods, that information will carry with it a set of legal and cultural rules that are hostile to the sharing needed to respond effectively to network attacks.

Perhaps the most egregious example of forcing all information gathering into a criminal law straitjacket is 18 U.S.C. § 2703(c). This provision of law limits the circumstances in which a service provider may disclose information about customers or subscribers to a governmental entity. For basic subscriber information (name, address and the like), the government must produce an administrative, grand jury, or trial subpoena. For more detailed "transactional" data about customers, the government must: (1) present a search warrant under the Federal Rules of Criminal Procedure or equivalent state warrant, (2) obtain a criminal investigative order under § 2703(d), (3) have the consent of the subscriber or customer, or (4) submit a formal written request for name, address, and place of business when relevant to a law enforcement investigation of a telemarketer. *See* 18 U.S.C. 2703(c)(1)(C).[13]

Even the most minimally competent cyber attacker uses multiple "hops" between computers to launch attacks. This permits the attacker to cover his or her tracks much more effectively. In consequence, tracking hackers requires a series of investigations, essentially tracking backward from one host computer to another. Typically, authorities will be able to use a victim's own logs

[13] Subparagraph (D) of the same section allows the gathering of certain information about subscribers using administrative, grand jury, and trial subpoenas. None of these subpoenas is suitable for most DoD inquiries, since one is criminal, another requires that a trial be imminent, and the third requires some administrative authority that is not obviously granted to DoD.

Page 1168 of 3957

to identify the initial source of an attack; they then contact the system administrator for the computer that is the source of the attack, ask for access to the logs of that host, and try to determine who was logged onto the computer at the time of the attack so as to determine the second "leg" of the hacker's travels. Once the second leg has been identified, the process is repeated, often many times. At every stage in this process, section 2703(c) limits the information that can be provided to government agencies.

It is worth noting that the restriction imposed by section 2703(c) applies only to requests for information made by government agencies. Internet service providers (ISPs) may hand out subscriber information on street corners to all comers without violating any provision of law; they may sell subscriber information to pornography spammers without violating any provision of law. (As a practical matter, of course, most ISPs have instituted privacy policies that voluntarily restrict distribution of customer data.) More realistically, they may share information about network attacks with other ISPs and hosts on a real-time basis without having to stop and invoke the judicial process at all. But they will violate the law if they provide information to a defense agency – even in the midst of a serious attack – without first seeing a criminal investigative order.

This is a remarkable state of affairs, and not one intended by the drafters of section 2703(c), or so one would hope. In general, if a government site is attacked and seeks information about the source of the attack from the first "hop" in the chain, the ISP with that information runs a slight risk that section 2703(c) will be violated if he simply tells the government what he knows about the intruder. That is because at this stage no one knows who the hacker is. He could be a subscriber or customer of the ISP. Chances are that he isn't, but why should the ISP risk civil liability? The prudent thing is to demand a criminal investigative order. Thus, in the name of protecting customers and subscribers, the current law actually puts a significant barrier in the way of protecting those who use government systems.

What's more, the provision essentially forces the government to treat all intrusions that require investigation as criminal matters. This serves no one's interests. If the culprit is a juvenile, prosecution is unsatisfying for the government and damaging for the defendant. Both might be better off if, instead of always relying on criminal investigations, the government could also gather necessary information while pursuing only civil remedies, such as fines, compensatory payments, or tailored injunctive relief. Indeed, some of the most important hacking investigations have not produced significant criminal penalties – at least not in the United States. (One investigation that consumed vast amounts of government resources finally tracked the exploits to two California teenagers and a young Israeli. No significant criminal penalties were imposed in the United States, and the Israeli proceedings have not yet produced a final result. Similarly, a 15-year old boy in Canada is the only person arrested thus far in the celebrated denial-of-service attacks in early 2000. The perpetrators of the "ILOVEYOU" virus will not be prosecuted in the United States.)

Allowing civil discovery in these circumstances is an option that deserves consideration. It is not without risks: ISPs and portals will not welcome any expansion of electronic communications discovery. At the same time, for DoD, there are advantages to information gained in a civil action. First, of course, it can be shared much more readily among agencies and through NIPC. It is not subject to grand jury secrecy concerns, nor to the Justice Department's restrictions on sharing information with NSC, nor is it likely to be "law enforcement sensitive." Indeed, since it would be gathered by DoD, it could be shared freely without even the restraints

Page 1169 of 3957

imposed by FBI culture on NIPC. This factor becomes extremely important when the target of an attack is a computer or network that is crucial to civil and national defense.

Second, being able to move from a purely internal defensive response to a civil investigative response will resolve another problem that has dogged DoD system administrators from the beginning of their work with Justice. This is the "prosecutorial agent" problem discussed above. In general, systems administrators may monitor as closely as they like those who intrude into their networks, without any legal prerequisites. DoD security officials have taken advantage of this fact, but they have complained that bringing criminal investigators into the matter often complicates their efforts to monitor an attacker. This is for the reasons described above – criminal investigators are acutely aware that they must have independent legal authority for intercepts and cannot turn a systems administrator into an agent of law enforcement. This is less of a risk if systems administrators are gathering information for a civil action.[14] Thus, network security officers could move from purely defensive monitoring to a civil investigation, including requests for information from third parties, without ever running the risk that a court would treat those actions as showing that the investigation is "really" a criminal investigation.

There are some drawbacks to the use of civil investigative authority. First, gathering data for the purposes of a civil investigation is complicated if, as with network attacks, there is a possibility of criminal prosecution. Second, DoD would need an appropriate civil discovery authority. And without some incentive to the ISP in question (such as an offer by DoD to pay the cost of expedited processing), the civil process could be significantly slower than a criminal one. Finally, many ISPs have instituted policies to provide notice to customers when law enforcement officials request data pertaining to them, a practice that effectively eliminates the secrecy of an investigation. Still, these are all issues that could be ironed out legislatively for the sake of protecting a nationally sensitive computer system.

A final issue that will undoubtedly be raised in this context concerns privacy. Should DoD be able to obtain subscriber information in network attack investigations without meeting the requirements for a criminal investigation? One may begin by asking whether investigating attacks on national security networks are as important as investigating telemarketers, since Congress has already exempted telemarketing investigations from the criminal subpoena requirements. What's more, a civil discovery authority limited to network attacks would not expose hackers to any greater risk of investigation than they now face; almost all network attacks can be investigated as crimes using criminal process. If necessary, Congress could require precisely the same standard for the civil discovery order as for a criminal order. If so, only two things would be different. First, the government would not be required to begin every investigation as though it was destined to end in indictment, and the authorities would be able to shape their legal response more sensitively in the light of the intruder's age, motives, and status. Second, the information would be gathered directly by DoD rather than the FBI and Justice. Whether that raises privacy concerns depends on which agency is considered more of a privacy threat. Certainly, there is no reason to think that DoD should be barred as a matter of principle from discovery aimed at civilians; defense investigators already serve a variety of civil processes on DoD employees and contractors, as well as ordinary discovery orders in garden-variety civil

[14] No one thinks that private companies may not lawfully ask their system administrators to gather information about hacker intrusions that they intend to use to sue the hackers. If there are real fears that current law somehow prevents the government from following this example, the statute authorizing the civil suit could no doubt also authorize the use of such information in support of the suit and for other network defense purposes.

Page 1170 of 3957

litigation. Properly structured, a civil discovery authority for network attacks would pose no greater threat to civilian privacy than the government's existing powers.

Network security would be greatly advanced, and the privacy status quo would be preserved, by a legislative provision overriding section 2703(c) and permitting the collection of data under a civil investigative order when the target of attack is a system of national security importance.

RECOMMENDATION 3.2:

The gap between law enforcement and foreign intelligence authorities to intercept hacker attacks should be closed, by enacting a "network trespasser" exception to Title III or otherwise.

Another somewhat surprising limitation on the ability of the FBI to gather information under criminal authorities has emerged of late. Under the Foreign Intelligence Surveillance Act (FISA), once a factual predicate has been established – that the target of an investigation is an agent of a foreign power – intercepts may be maintained for relatively long periods of time.[15] A Title III intercept, however, must be renewed every thirty days, with the Justice Department obligated to persuade the presiding judge that the tap is crucial to an ongoing criminal investigation.

But hacking investigations may take years without bringing investigators significantly closer to actually indicting a particular human being. Continuing the intercepts may be crucial to gathering information about the techniques used by the hacker and gathering clues about the hacker's identity and motives, but the process can be a slow one.

Sometimes a Title III intercept shows that the hacker is probably based abroad, and in such cases, over time, a criminal investigation will begin to appear futile. Hacking may not be a crime in the suspected country of origin, or the hacker may not be extraditable, or it may be impossible to get the cooperation of the local police. Gradually, the intercept begins to have less and less value as a criminal investigative tool, even though maintaining the tap may be highly important from an intelligence point of view. Sooner or later, then, prosecutors (at least the prosecutors in the Computer Crime and Intellectual Property Section (CCIPS) which is the source of this concern) are likely to reach the conclusion that the legal standard for continuing the wiretap is no longer satisfied. At that point, the prosecutors will refuse to seek additional wiretap authority – even though a criminal intrusion is still occurring, and even though the evidence may suggest that the intrusion is sophisticated enough to be state sponsored. The CCIPS view is that Title III is not an intelligence-gathering authority; unless a criminal case is in the offing, the tap must end, notwithstanding the value of the intelligence to national security. Of course, if it is clear that a foreign government is involved, a foreign counterintelligence tap can be initiated, but this is rarely clear. The result is that important intelligence about network attacks will be lost. In short, there is a very real possibility that foreign hackers will be able to attack DoD systems without any wiretap monitoring because both existing law enforcement and counterintelligence authorities are too narrow.

---

[15] FISA permits the surveillance of the agent of a foreign power under a court order, which must be renewed every ninety days. The foreign power itself may be targeted for an entire year under a court order pertaining to FISA.

Page 1171 of 3957

For this and other reasons (e.g., statutory information-sharing restrictions), Title III intercepts are an unappealing way to gather information about hacking efforts. That said, it is unclear what alternatives exist unless Congress addresses the problem. In that regard, two approaches should be considered.

First, the Justice Department, or at least CCIPS, would welcome DoD support for a "trespasser" exception to the protections of Title III. In essence, this would deny any statutory expectation of privacy to persons who are trespassing on another person's computer network. This is indeed an appealing approach, as hackers should not have any expectation that the signals they send to the systems of victims will be free from monitoring. This proposal has circulated within the Justice Department but has not been advanced officially. DoD should support such a measure.

A second possibility is to seek amendments to FISA that would allow the courts to presume that a foreign power is involved when attackers hop through hostile countries, attack critical systems, and/or use techniques that are thought to be particularly sophisticated or otherwise characteristic of foreign powers. There is some room for making this argument in the context of existing law, but it would obviously be easier if such considerations were part of FISA.

In so saying, the task force does not underestimate the difficulties of such a modification. The nation will not – and should not – tolerate long-term intelligence surveillance of Americans; no one wants to authorize FISA intercepts that turn out to be aimed at the activities of California teenagers. While it is likely that that result can be avoided if sufficient care is exercised in defining the events that justify such surveillance, any such amendment to FISA would need to be carefully drafted, vetted, and debated. Before making a change, it would be appropriate to ask (as task force members could not, being limited to a secret clearance) whether it is possible to utilize overseas intelligence collection resources to gather information on the attack, thus avoiding the need to invoke FISA at all. Intelligence collection efforts outside of the United States face fewer restrictions on gathering information relating to attacks than do domestic law enforcement investigations. For a variety of reasons, the task force thinks it unlikely that this is a complete answer, but it should be examined with care by DoD before making a final decision on the kinds of legislative changes that are appropriate to address the pressing problems that have been identified above.

RECOMMENDATION 3.3:

Procedural improvements should be made to streamline the "trap-and-trace" process and to allow emergency data requests under Electronic Communications Privacy Act (ECPA).

A. Trap-and-trace improvements.

When a network attack is being investigated, it is normal to obtain, first, a § 2703(d) order for information already in the hands of the first ISP in the chain of attacks, and, second, a trap-and-trace order authorizing future information collection for law enforcement purposes.

The use of trap-and-trace orders, however, has not been free from difficulty. Trap-and-trace orders are ordinarily obtained in the jurisdiction where the trap-and-trace device is to be placed (i.e., in the jurisdiction of the service provider). Since the Internet has little interest in

Page 1172 of 3957

geography, it is typically the case that every leg of a hacker's journey terminates in a different city, and with a different service provider. Often these providers are located in different jurisdictions, and obtaining the requisite orders can cause delays. Delay is the enemy of any investigation, but particularly of hacking investigations, as hackers often change their patterns regularly, sometimes as frequently as every few hours or minutes.

Delays in obtaining trap-and-trace orders for facilities in particular jurisdictions disrupt the ability of investigators to trace back along a hacker's attack chain. In particular, if there is a live connection, tracing back an attack quickly is difficult because each step in the chain may require a new order (because the carriers may be in different jurisdictions), each based upon the information discovered in prior orders. Moreover, the review by multiple courts does not substantively protect any rights, since the court in the victim's jurisdiction has already determined the appropriateness of the trace, and other courts are merely effectuating the order of the first court. Timing is also critical where the investigation concerns an attack that has already taken place, as the investigating agency must obtain a court order to trace the attack through activity logs before the service providers whose networks are used in the attack overwrite their records.

In response to this concern, investigators have expressed interest in obtaining a single national trap-and-trace order that could be served progressively on each service provider who has been the inadvertent host of a hacker on his journey.

In general, such authority would reduce the time it takes to track hackers, though there are many reasons for delays in tracking hackers from one computer to the next. Obtaining trap-and-trace orders is a contributor to those delays, but it is not the only contributor. For example, even with a nationwide order, it will still be necessary for the authorities to go from provider to provider in an achingly sequential fashion. This "one step at a time" approach is an unquestionable source delay in some hacking investigations.

Given these limitations, a nationwide trap-and-trace authority is not a panacea. But it would have some value to Justice and DoD in seeking to find network attackers as quickly as possible. For that reason, it deserves support – so long as that support does not detract from the other, higher priority, legislative reforms set forth earlier.

B. Emergency authority under ECPA.

A second revision also deserves consideration. Currently, there is no statutory provision for government to obtain information quickly under the ECPA in situations of extreme urgency. This is an oddity, since wiretaps, presumably much more intrusive, may be initiated without a judicial order in "emergency situations."[16] In such cases, where a communication must be intercepted "before an order authorizing such interception can, with due diligence, be obtained" (and where there are sufficient grounds to assume that an order would ultimately be granted), an intercept may be conducted in absence of authorization, provided that approval of the intercept is requested within forty-eight hours after "the interception has occurred, or begins to occur." (*See* 18 U.S.C. § 2518 (7))

---

[16] Emergencies are defined as involving:

(i) immediate danger of death or serious physical injury to any person;

(ii) conspiratorial activities threatening the national security interest; or

(iii) conspiratorial activities characteristic of organized crime

Page 1173 of 3957

The information that can be obtained through a subpoena or section 2703(d) order is sometimes equally essential to the investigation of a hacker attack, and providing specifically for emergencies would be useful. It would also protect the interests of ISPs and those under investigation. As things now stand, the lack of a statutory emergency provision means that in an emergency law enforcement agencies put heavy pressure on ISPs to release information even before the authorities can produce an order. The release of this information (which almost always happens) can expose the ISP to liability for violation of its privacy policy, and can cause law enforcement authorities to come to rely on the emergency justification (even in cases where the emergency isn't all that clear). In the long run, as customer privacy becomes the subject of greater scrutiny in state and federal legislatures, ISPs may discontinue their current practice and refuse to release any information in the absence of an order. The current provision in Title III allowing emergency wiretaps should be extended to court orders and subpoenas as well.

RECOMMENDATION 3.4:

Federal Rule of Criminal Procedure 6(e) should be modified to allow sharing of grand jury information relating to national security.

The task force has already discussed (see **Recommendations 1.3 and 1.4**) information-sharing burdens that are created by the use of grand jury subpoenas or Title III intercepts to gather information about network attacks. The task force recommended several ways in which these problems could be solved through reasonable accommodations of the national security by Justice and NIPC. In the event that these agencies are not prepared to make those accommodations, it may be necessary to overcome these obstacles legislatively. No one believes that either Title III or Rule 6(e) was written deliberately to exclude sharing for national security purposes. Very likely, it simply did not occur to the drafters to include a national security provision. Curing this oversight legislatively, perhaps simply by clarifying the existing National Security Act, ought to be a live option.

RECOMMENDATION 3.5:

Legislation should be enacted to encourage voluntary private-sector cooperation in hacking investigations, specifically to quell concerns that sensitive or proprietary information might be disclosed publicly.

Much has been made above of the legal barriers that prevent the government's access to or sharing of information when conducting hacking investigations. These are by far the most significant obstacles to efficient defensive information operations. They are not the only barriers, however, as even information that investigators could lawfully acquire is sometimes kept out of reach.

The investigation of cyber attacks need not be a one-way event, with law enforcement issuing various orders for information and service providers consequently handing it over. An ISP that falls victim to a hacker attack may justifiably hand over information about the attack, at the very least to prove that a crime has taken place. All too often, however, the private sector resists such voluntary cooperation with law enforcement. There are a number of reasons for this

Page 1174 of 3957

reluctance, most notably a fear that the information shared may be released under the Freedom of Information Act (FOIA).

So much of the nation's critical infrastructure is based in private hands that the importance of that sector's voluntary cooperation in investigations on network attacks should not be underestimated. This being the case, the government should adopt reasonable measures to encourage this cooperation. Agencies should be encouraged to expand the use of nondisclosure agreements in gathering information on network attacks. In addition, it would be worthwhile to consider supporting legislation that would restrict from FOIA disclosure any information that a service provider shares in conjunction with a hacking investigation (legislation to this effect was introduced in the last Congress and will likely be reintroduced). Such legislation should be narrowly tailored, so as to avoid creating an exemption behind which companies could conceal evidence of unlawful business practices from public discovery. Even with these limits, the provision could have significant benefits for investigators of network attacks.

Page 1175 of 3957

APPENDIX A. ACRONYMS

CCIPS	Computer Crime and Intellectual Property Section
DAG	Deputy Attorney General
ECPA	Electronic Communications Privacy Act
FISA	Foreign Intelligence Surveillance Act
FOIA	Freedom of Information Act
ISPs	Internet service providers
JTF-CND	Joint Task Force – Computer Network Defense
MOU	Memorandum of Understanding
NIPC	National Infrastructure Protection Center
NSA	National Security Agency
NSC	National Security Council
OLC	Office of Legal Counsel
ORCON	Originator Controlled

Page 1176 of 3957

Page 1177 of 3957

APPENDIX B. PANEL MEMBERS AND GOVERNMENT ADVISORS

Chairman:

Mr. Stewart Baker	Steptoe & Johnson

Members:

Ms. Elizabeth Banker	Yahoo! Inc.
Mr. Bill Burrington	AOL Europe
Mr. Roger Callahan	Bank Of America
Mr. Scott Charney	Pricewater-HouseCoopers LLP
Mr. Steven DeGeorge	AT&T Law Division
Mr. Lawrence Greenberg	The Motley Fool, Inc.
Mr. Jonathan Spear	MCI Telecommunications Corporation

Page 1178 of 3957

ANNEX F

1996 DSB Report on Defensive Information Operations

STATUS OF RECOMMENDATIONS

Page 1181 of 3957

Current Assessment of Recommendations from the *Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)*

(November 1996)

1996 Recommendation	Current Status	Current Shortfalls
1. Designate an accountable IW focal point. The SECDEF should:		
1a. Designate ASD(C3I) as the accountable focal point for all IW issues.	DoD Directive S-3600.1 "Information Operations," 9 Dec 96, designates ASD(C3I) as the responsible authority for IW/IO.	
1a(1). Develop a plan and associated budget beginning in FY97 to obtain the needed IW-D capability.	Components were required to address IA budgets beginning with FYDP 1999-2002. The DIAP was established by DEPSECDEF to better coordinate and align IA budgets and assure adequate funding. – this effort has provided better visibility for overall DoD IA budget.	• There are no specific line items for IA. • Shortfalls identified by DIAP have been faced with a shortage of additional funds.
1a(2). Authorize ASD(C3I) to issue IW instructions.	DoD Directive S-3600.1 "Information Operations," 9 Dec 96, designates ASD(C3I) as the responsible authority for IW/IO. In addition, the DoD implementation of the Clinger-Cohen Act designates the ASD(C3I) as the DoD CIO and assigns the responsibility for IA to the DoD CIO.	
1a(3). Consider establishing a USD(Information).	No longer required; the ASD(C3I) has been designated the DoD CIO.	
1b. Establish a DASD(IW) and supporting staff to bring together as many IW functions as possible.	The June 1998 reorganization within OASD(C3I) resulted in the creation of a DASD for Security & Information Operations, a position that includes responsibility for Information Assurance, Infrastructure Assurance, Security, Counterintelligence, and Information Operations Strategy and Integration.	This organizational structure resides within OASD(C3I) and primarily includes those activities currently within the purview of OASD(C3I). This structure does not readily accommodate the corresponding DIO-related requirements/issues within OUSD(A&T), including related R&D within DARPA and the Military Departments.

Page 1181 of 3957

1996 Recommendation	Current Status	Current Shortfalls
2. Organize for IW-D.		
2a. Establish a center to provide strategic indications and warning, current intelligence, and threat assessments. The SECDEF should request the DCI to:	NSA established the National Security Incident Response Center (NSIRC).	This organization is primarily focused on tactical activities rather than strategic activities, although in some cases, tactical level incidents may yield strategic insights.
2a(1). Establish an I&W/TA center at NSA with CIA and DIA support.	The DIA and JWAC are involved in this area.	There appears to be no overall DoD orchestrated approach to providing a strategic capability for DIO.
2a(2). Task and resource the Intelligence Community to develop the processes for Current Intelligence, Indications and Warning, and Threat Assessments for IW-D.	There are numerous activities within the Intelligence Community to address the intelligence requirements.	It is unclear as to how well these various activities are coordinated.
2a(3). Encourage the Intelligence Community to develop information-age trade craft, staff with the right skills, and train for the information age.	The DCI established the Advanced Research and Development Technology activity under NSA to focus on information technology as a multidisciplinary capability to the Intelligence Community.	The available skill set continues to fall well below the need.
2a(4). Conduct comprehensive case studies of U.S. offensive programs and a former foreign program to identify potential indicators – collection, funding, training, etc.	The DTRA "Chessmaster" case study is an example of the type of activity currently ongoing. Assessments continue as the capabilities and intentions of potential opponents change.	
2a(5). Establish an organization to examine and analyze probable causes of all security breaches.	NSA established the Network Incident Analysis Cell (NIAC) within the NSIRC to perform post network intrusion, forensic-style analysis of data received from incident response centers.	Analytical results and lessons learned are not effectively disseminated.
2a(6). Develop and implement an integrated National Intelligence Exploitation Architecture to support the organization and processes.	Intelligence Community activities in this area are ongoing.	Efforts are disparate and not integrated into a well-described plan.
2a(7). The SECDEF should direct the development of IW Essential Elements of Information (EEI).	Intelligence Community activities in this area are ongoing and JTF-CND is providing input into development of EEIs.	No final product or publication date has been set.

Page 1182 of 3957

1996 Recommendation	Current Status	Current Shortfalls
2b. Establish a center for IW-D operations to provide tactical warning, attack assessment, emergency response, and infrastructure restoration capabilities. The SECDEF should:	The DoD established the Joint Task Force – Computer Network Defense (JTF-CND) and the DISA Global Network Operations Center (GNOSC).	Concepts of Operations (CONOPS) for DIO mission execution are immature or do not exist. Where mission assignments have been made, lack of resources inhibits execution (e.g., USSPACECOM, JPO-STC).
2b(1). Establish a DoD IW-D operations center at DISA with NCS, NSA, and DIA support.	The DoD established the DISA Global Network Operations Center (GNOSC).	DoD does not universally collocate its Network Operations Centers with Information Assurance (IA) / Computer Network Defense (CND) activities.
2b(2). Develop and implement distributed tactical warning, attack assessment, emergency response, and infrastructure restoration procedures.	Currently, JTF-CND does distribute tactical warning, but has minimal attach assessment capability. Emergency response is primarily coordinated through the various CERTS/CIRTS of the Services / Agencies. JTF-CND also assists in establishment of restoration priorities with DISA and other activities.	Recommended improvements in GIG architecture and security could provide a technology baseline to permit creation of a tactical/time-sensitive information attack warning sensor grid. Such a network would also support goals of assigning attacker attribution confidently and rapidly. However, any plan to achieve this outcome must span the domains of policy/law, technology and organization, and would require actions in several sectors of government, as well as private industry.
2b(3). Interface the operations center with Service and Agency capabilities and I&W/TA support.	This requirement is stated in the JTF-CND Concept of Operations; JTF-CND interfaces with these organizations continue to strengthen.	DoD CERT/CIRT activities vary in their execution and are not inclusive of all DoD CINCs/Services/Agencies.
2b(4). Establish necessary liaison (e.g., with military and government operations centers, service providers, intelligence agencies, and computer emergency response centers).	This requirement was completed as a result of the JTF-CND Concept of Operations.	
2c. The SECDEF should establish an IW-D planning and coordination center reporting to the ASD(C3I) with interfaces to the intelligence community, the Joint Staff, the law enforcement community, and the operations center.	The Defense-wide Information Assurance Program (DIAP) was established in 1998. It serves primarily as a facilitator for the gathering and sharing of IA-related information. In that role, the DIAP has accomplished much in identifying what is being done throughout DoD, and continues to focus on unifying/integrating various IW-D activities.	• The DIAP has no real authority to direct the Military Departments or Agencies, and does not control or impact any IW-D aspects of Service/Agency budgets. • Internal staffing and funding shortfalls have further hampered the DIAP's ability to accomplish the mission.

Page 1183 of 3957

Page 1184 of 3957

1996 Recommendation	Current Status	Current Shortfalls
2d. Establish a joint office for system, network and infrastructure design.	There are current activities to develop, promulgate and implement Joint Technical Architecture (JTA), Joint Operational Architecture (JOA) and Joint Systems Architecture (JSA). Many recent efforts have centered on development of GIG architecture.	• There is no joint office to coordinate these various activities. • The GIG IATF standards and protocols for providing security are inconsistent with the JTA.
2d(1). Establish a joint security architecture/design office within DISA to shape the design of the DoD information infrastructure.	OASD(C3I), DISA, NSA, Joint Staff and Service representatives participate in the activities cited in 2d.	• There is no joint office to coordinate these various activities. • The IATF is a collection of history and general information; it is not a document that can be used to implement interoperable, secured information systems for DoD.
2d(2). Establish a process to verify independently and enforce adherence to these design principles.	The DoD established the Defense Information Technology System Certification and Accreditation Process (DITSCAP), as well the Secret And Below Interoperability (SABI) and Top Secret And Below Interoperability (TSABI) processes. Processes within the GIG governance arena are also being established to enforce adherence to GIG architecture requirements.	There are insufficient resources to implement DITSCAP, SABI, and TSABI at a pace that meets the demands within the DoD. Temporary waivers or work-arounds can prove counterproductive to the process.
2e. Establish a Red Team for independent assessments.	Some Red Team capabilities exist within the Services, NSA, and DIA.	Due to lack of clear policy and resources, aggressive, comprehensive, effective operational Red Team activities are lacking across DoD.
2e(1). Establish a Red Team which is accountable to SECDEF/DEPSECDEF and independent of design, acquisition, and operations activities.	No Red Team has been established to be directly accountable to the SECDEF/DEPSECDEF, independent of design, acquisition, and operations activities.	Without such an independent Red Team capability, current Red Team results may be questionable because of organizational affiliation/loyalties.
2e(2). Develop procedures for employment of the Red Team.	Thus far, the DoD has developed the Defensive Information Assurance Red Team (DIART) Manual.	Due to the lack of clear Red Team policy, there is no formal requirement for DIART to be implemented DoD-wide, and it is often ignored. This Red Team Manual provides the standardized procedures for any DoD Red Team, but absent a DoD Directive, there is no way to mandate their use. Additional, guidance needs to be provided on how results of the Red Teams (and any other assessment) are collected and analyzed to determine trends and lessons learned.

Page 1184 of 3957

1996 Recommendation	Current Status	Current Shortfalls
3. Increase awareness. The SECDEF should:		
3a. Establish an internal and external IW-D awareness campaign for the public, industry, CINCs, Services, and Agencies	In June 1998 the ASD(C3I) and the USD(P&R) jointly issued a memorandum that required IW-D user awareness and training. There are currently numerous IW-D training activities throughout the DoD.	Conflicting definitions and usage related to IO, IA and CIP within the DoD and Intelligence Community causes resource and equity fights within the federal National Security Community and inhibits progress in resource management, training, and other important areas.
3b. Expand the IW Net Assessment recommended by the 1994 Summer Study to include assessing the vulnerabilities of the DII and NII.	Over the past five years, OSD - Net Assessment made several attempts to assess various aspects of IO. In each case, the assessment's value was limited by a lack of meaningful metrics. While the assessment could catalog and relate interesting anecdotal information, it would not provide the Secretary with the factual information necessary to make programmatic decisions. Accordingly, Net Assessment shifted its focus toward developing metrics by which the value of information under differing circumstances could be measured.	The IW Net Assessment has not yet been accomplished.
3c. Review joint doctrine for needed IW-D emphasis.	Joint Pub 3-13 (Defensive IO) was issued on October 9, 1998. CJCSI 6510.01B (Defensive IO Implementation), issued 26 August 1998, is currently under revision, with the new version expected to be issued in January 2001.	Doctrine and implementation instructions need to be adequately tested in exercises and integrated into mission planning and execution.
3d. Explore possibility of large-scale IW-D demonstrations for the purpose of understanding cascading effects and collecting data for simulations.	The Joint Staff and CINCs have sponsored exercises in which IW-D was a component.	It is unknown as to whether there have been large scale IW-D demonstrations conducted solely for the purpose of understanding the cascading effects and for collecting data for simulations. The modeling and simulation community lacks maturity in tools to assess these effects.
3e. Develop and implement simulations to demonstrate and play IW-D effects (USD(A&T) lead)	Current status is unknown.	Current status is unknown.

Page 1185 of 3957

1996 Recommendation	Current Status	Current Shortfalls
3f. Implement policy to include IW-D realism in exercises.	The Joint Staff and CINCs have sponsored numerous exercises in which IW-D is a component. Exercise plans are increasing in sophistication to address these issues.	IW-D demonstrations do not effectively reflect cascading effects for collecting data for simulations.
3g. Conduct IW-D experiments.	DARPA and the C4I Joint Battle Center have conducted IW-D experiments.	It is unknown as to whether there have been large scale IW-D experiments conducted for the purpose of understanding cascading effects and collecting data.
4. Assess infrastructure dependencies and vulnerabilities. The SECDEF should:		There appears to be no overall DoD orchestrated approach to providing a strategic capability for DIO.
4a. Develop a process and metrics for assessing infrastructure dependency.	CIP (physical & cyber) analytical methodology has been identified and prototyped to link OPLANS / TPFDDs / Defense sector assets to analyze interdependencies	Prototype methodologies require thorough testing.
4b. Assess/document operations plans infrastructure dependencies.	CIP (physical & cyber) analytical methodology has been identified and prototyped to link OPLANS / TPFDDs / Defense sector assets to analyze interdependencies	Prototype methodologies require thorough testing.
4c. Assess/document functional infrastructure dependencies.	Defense infrastructure sectors are in the initial stages of performing sector characterization which will include intradependencies and interdependencies with other sectors	
4d. Assess infrastructure vulnerabilities.	DoD and JPO are beginning to develop protocol to include/integrate CIP (physical & cyber) assessments of defense infrastructures into existing assessment processes/procedures.	
4e. Develop a list of essential infrastructure protection needs.	Work in this area is currently ongoing.	No anticipated delivery date has been set for a final product/report.
4f. Develop and report to the SECDEF the resource estimates for essential infrastructure protection.	Estimates have been generated for initial CIP (physical & cyber) requirements to perform limited analysis and assessment.	Estimates must be refined, documented, and formally reported in order to promote appropriate action.

Page 1186 of 3957

Page 1187 of 3957

1996 Recommendation	Current Status	Current Shortfalls
4g. Review vulnerabilities of hardware and software embedded in weapons systems.	Not yet addressed. Recent changes in the DoD 5000 series and a Memo from USD(AT&L) adding security as an equal element to cost, schedule and performance for acquisition programs will assist in accomplishing this task. Reviews of some weapons systems were performed as a part of the Y2K effort and lessons learned should be incorporated.	• Lack of a formal requirement inhibits incentive to integrate these assessments into system development plans. • This area remains significantly vulnerable.
5. Define threat conditions and responses. The SECDEF should:		
5a. Define and promulgate a useful set of IW-D threat conditions which is coordinated with current intelligence community threat condition definitions.	INFOCONS have been established. CJCSI Memorandum of March 1999 served as vehicle for dissemination throughout the DoD. USSPACECOM is in the process of reviewing and revising the INFOCON process to make it more usable and ensure appropriate establishment and promulgation throughout DoD.	Interpretation of the INFOCONS varies within organizations, which can adversely impact their collective implementation.
5b. Define and implement responses to IW-D threat conditions.	Rules of engagement are currently undergoing legal review at Secret level.	DoD implementation of responses is hampered by existing and conflicting governing authorities and related rules of engagement.
5c. Explore legislative and regulatory implications.	Legislative and regulatory implications are currently being addressed through various activities within the federal government, as well as the DoD.	Current legislation and conflicting roles/responsibilities/authorities with the Department of Justice are impediments to the process.
6. Assess IW-D readiness. The SECDEF should:		
6a. Establish a standardized IW-D assessment system for use by CINCs, MilDeps, Services, and Combat Support Agencies.	CJCSI 6510.04 (Information Assurance Readiness Metrics), 15 May 2000, provides a standardized information assurance list of items to consider when preparing the information assurance portion within the JMRR C4 functional area.	There is no adequate system for assessing DIO readiness across DoD. CJCSI 6510.04 is relatively unknown within the Military Departments and, buried within the C4 functional area, has relatively little impact on assessing readiness. Although it establishes a baseline, it is neither mandatory, nor does it apply to all DoD activities.

Page 1187 of 3957

Page 1188 of 3957

1996 Recommendation	Current Status	Current Shortfalls
6b. Incorporate IW preparedness assessments in Joint Reporting System and Joint Doctrine, for example.	CJCSI 6510.04 (Information Assurance Readiness Metrics), 15 May 2000, provides a standardized information assurance list of items to consider when preparing the information assurance portion within the JMRR C4 functional area.	DIO is not adequately integrated into mission planning and execution. CJCSI 6510.04 is relatively unknown within the Military Departments and, buried within the C4 functional area, has relatively little impact on assessing readiness.
7. "Raise the bar" with high-payoff, low-cost items. The SECDEF should:		
7a. Direct the immediate use of approved products for access control as an interim until a MISSI solution is implemented and for those users not programmed to receive MISSI products.	NSTISSP No. 11, January 2000, requires that by 1 January 2002, acquisition of all COTS IA and IA-enabled IT products must be evaluated through the NIAP process. The NIAP provides a mechanism for certification of security products. NIST Special Publication 800-23 provides additional guidance in this area. In addition, the Defense in Depth strategy requires several levels of protection of networks and systems. Related security products include access control mechanisms (password control, PKI, biometrics), firewalls, intrusion detection devices, secure routers, etc.	
7b. Examine the feasibility of using approved products for identification and authentication.	The DoD PKI policy memorandum of May 1999 (replaced by the August 2000 Memo), establishes the DoD Public Key Infrastructure policy and Program Management Office (PMO). It establishes the desire to seek maximum use of COTS technology.	
7c. Require use of escrowed encryption for critical assets such as databases, program libraries, applications, and transaction logs to preclude rogue employees from locking up systems and networks.	Current DoD PKI policy addresses the use of escrowed encryption. The "insider threat" issue is being addressed by various efforts, one of which is through the Insider Threat IPT, which is looking at a spectrum of technical, policy, training, and other options to address this issue.	Systems Administrators have the "keys to the kingdom," yet often require no special "reliability" investigations, such as those in the Personnel Reliability Program.

Page 1188 of 3957

Page 1189 of 3957

1996 Recommendation	Current Status	Current Shortfalls
8. Establish and maintain a minimum essential information infrastructure. The SECDEF should:	Through the Y2K efforts, the DoD identified its minimum essential information systems ("thin-line"). This effort serves as a starting point for the CIP (physical & cyber) activities.	The critical infrastructures that are essential to the minimum operations of the economy and government are predominantly owned by the private sector. The DoD is extremely dependent upon these private sector systems, networks and infrastructures, but industry is not motivated to share information on their vulnerabilities with the government.
8a. Define options with associated costs and schedules.	Processes for defining and resolving associated funding requirements are under development.	
8b. Identify minimum essential conventional force structure and supporting information infrastructure needs.	Addressed, in part, in JV2010 and JV2020.	Significant personnel resource shortfalls impact execution of the DIO mission at all levels in DoD.
8c. Prioritize critical functions and infrastructure dependencies.	Under development.	No final product/report or due date has been defined or funding applied.
8d. Design a Defense MEII and a failsafe restoration capability.	The CIO organization is applying lessons learned from the Y2K experience in registering applications, determining mission critical/mission support and policies concerning NIPRNET access.	
8e. Issue direction to the Defense Components to fence funds for a Defense MEII and failsafe restoration capability.	No guidance issued to date.	The DoD continues to remain vulnerable.
9. Focus the R&D. The SECDEF should focus the DoD R&D program on the following areas:	The DIAP Research & Technology (R&T) functional area was established to provide focus in the DoD IA R&D areas. This functional area works primarily with the InfoSec Research Council (IRC), a voluntary member organization of a number of activities (DoD and non-DoD), doing IA research.	

Page 1189 of 3957

1996 Recommendation	Current Status	Current Shortfalls
9a. Develop robust survivable system architectures.	DARPA sponsored major program in this area.	• The DoD is managing its current information assurance R&D in a fragmented way that is not sufficiently focused on the information assurance requirements of the GIG. • The current DoD network architecture calls for a secure network with authorized access via tokens (i.e., PKI). The scope of this security apparatus is enormous, and PKI has not been modeled and tested under extreme requirements.
9b. Develop techniques and tools for modeling, monitoring, and management of large-scale distributed/networked systems.	Previous and ongoing IA R&D efforts are addressing this area.	Development and deployment of new network technology has greatly outpaced information assurance technology, thereby increasing the vulnerability of DoD systems.
9c. Develop tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks.	Previous and ongoing IA R&D efforts are addressing this area.	• One of the weakest aspects of U.S. DIO is our extremely limited ability to detect, assess, and understand both hostile IO capabilities and precursor indications and warning of attack. • No methods exist for automated or assisted discovery of existing or novel attack patterns or signatures, particularly for those attacks which are distributed across many computes or networks. • Intrusion detection technologies curently produce only moderately reliable results in simple environments, and even less reliable results in complex environments.
9d. Develop tools for synthesizing and projecting the anticipated performance of survivable distributed systems.	Previous and ongoing IA R&D efforts are address this area.	DoD does not have a methodology for restoring integrity in its systems.
9e. Develop tools and environments for IW-D oriented operational training.	The Joint Battle Center is chartered to perform this work and has a number of on-going activities to address issues in this area.	The DoD is not aggressively or innovatively addressing its IA R&D personnel requirements, which will likely lead to more serious problems in the next few years as more personnel leave the department and fewer high caliber R&D managers remain.

Page 1190 of 3957

Page 1191 of 3957

1996 Recommendation	Current Status	Current Shortfalls
9f. Develop testbeds and simulation-based mechanisms for evaluating emerging IW-D technology and tactics.	Previous and ongoing IA R&D efforts are address this area.	Progress in defending and protecting the GIG will require a far greater ability to model and simulate the performance of information infrastructures than we have today.
9g. The SECDEF should work with the NSF to develop research in U.S. computer science and computer engineering programs.	NSA's Information System Security Engineering program is working with 7 universities in this area.	This NSA program is independent and not implemented with NSF.
9h. The SECDEF should work with the NSF to develop educational programs for curriculum development at the undergraduate and graduate levels in resilient system design practices.	NSA's Information System Security Engineering program is working with 7 universities in this area.	The degree to which the NSA program, which is implemented independent of NSF, is addressing curriculum development is unknown.
10. Staff for success. The SECDEF should:		
10a. Establish a career path and mandate training and certification of systems and network administrators.	An IT/IA Human Resources IPT was established to examine issues associated with the establishment of an IA/IO career path. An OSD memorandum in June 1998 addressed mandatory training.	The shortage of DoD IT professionals is serious and growing.
10b. Establish a military skill specialty for IW-D.	Skill specialties have yet to be established. The Joint Staff has a tasking to develop common skill sets for specific functions in this area. The military Services have all undergone major restructuring of their military skill sets to identify, recruit and retain professionals in this area.	The appropriate staffing of DIO positions continues to be severely hampered.
10c. Develop specific IW awareness courses with strong focus on operational preparedness in DoD's professional schools.	There are numerous activities in this area. IA awareness products and activities, and IA/IO courses, are provided at all professional military education facilities.	The DoD workforce at all levels is ill prepared to execute the DIO mission because current training efforts are fragmented, inadequately scoped, and poorly documented.

Page 1191 of 3957

Page 1192 of 3957

1996 Recommendation	Current Status	Current Shortfalls
11. Resolve the legal issues. The SECDEF should:		
11a. Promulgate for Department of Defense systems: • Guidance and unequivocal authority for Department users to monitor, record data, and repel intruders in computer systems for self protection. • Direction to use banners that make it clear the Department's presumption that intruders have hostile intent and warn that the Department will take the appropriate response. • IW-D rules of engagement for self-protection (including active response) and civil infrastructure support.	• Legal guidance has been promulgated and policies are under review regarding the monitoring and auditing of network activities. • Intrusion Detection Systems perform a portion of this function. • Guidance on configuration of the various devices is provided as technology changes. • Additional mechanisms to identify and warn intruders are being investigated, as well as a general announcement of DoD policy and intent through the normal media channels. • Rules of engagement issues, including active defense are being investigated to determine possible actions.	The use of banners can only address the "insider issue." Intruders into systems generally bypass standard entry routes and it is virtually impossible to set up mechanisms for banners to be present on all entry points.

Page 1192 of 3957

Page 1193 of 3957

1996 Recommendation	Current Status	Current Shortfalls
11b. Provide to the Presidential Commission on Critical Infrastructure Protection proposed legislation, regulation, or executive orders for defending other systems.	OBE, since PDD 63 was signed. However, there are a number of ongoing legislative activities being addressed among the NIPC, Federal CIO Council, and the CIAO.	• The DoD is suffering under existing legislation. Although it has the responsibility for national defense, it has been forced to rely on law enforcement agencies such as the FBI and the Justice Department to gather information about attacks. • Under existing law, network service providers may give away information about hacking attacks to the public, but they are legally prohibited from giving the information to a government agency unless the agency begins a criminal investigation. • There is no clear guidance as to which takes precedence: the confidentiality of criminal investigations or the national security interests of the United States. • Criminal wiretap authorities are inadequate for the government to maintain wiretap coverage of persons engaged in long-term hacking campaigns against government networks. • Current law concerning "trap and trace" orders often requires that law enforcement agencies seek multiple, sequential orders as they trace a single hacker from system to system.
12. Participate fully in critical infrastructure protection. Regarding the activities of the President's Commission on Critical Infrastructure Protection, the SECDEF should:		
12a. Offer specific Department capabilities to the President's Commission.	OBE, since PDD 63 was signed. However, there are a number of activities in the CIP area that are working with the CIAO to address the spirit of this recommendation.	

Page 1193 of 3957

1996 Recommendation	Current Status	Current Shortfalls
12b. Advocate the Department's interests to the President's Commission.	OBE, since PDD 63 was signed. However, there are a number of activities in the CIP area that are working with the CIAO to address the spirit of this recommendation.	• No one has the responsibility or authority to make response and recovery decisions and take actions across stovepipes. Coordination depends upon personalities. • The State Department is potentially very important to DIO, but is not sufficiently engaged. • A great portion of government doesn't understand DIO issues or appreciate the potential impact of information technology vulnerabilities on their operations.
12c. Request the Commission provide certain national-level capabilities for the Department.	OBE, since PDD 63 was signed. However, the NIPC, for which the DoD provides personnel resources, provides the law enforcement capabilities.	• There is no clear responsibility for rationalizing law enforcement and national defense equities when certain types of cyber attack are detected. • There is currently a bias toward using law enforcement authorities and procedures when a cyber incident is detected. Although this will be satisfactory in the vast majority of cases, no formal means exists to review cases to determine if national security procedures might be more appropriate.
12d. Suggest IW-D roles for government and the private sector.	OBE, since PDD 63 was signed. PDD 63 established roles and responsibilities.	
13. Provide the resources. Develop a plan and associated budget beginning in FY97 to obtain needed IW-D capability (ASD(C3I) lead)	The DIAP is currently attempting to obtain IW-D funding requirements from DoD organizations. With the improved visibility into DoD component budgets, areas requiring additional funding are being identified. The DIAP has established appropriate mechanisms through the PPBS process to identify and justify shortfalls – the issue is how to prioritize and obtain additional funding in a tight budget environment.	The Department has not sufficiently funded protection of its networks and DIO programs. Of particular concern in the Sensitive, But Unclassified (SBU) information, which is critical to JV2020.

Page 1194 of 3957

ANNEX G

Defense Science Board Task Force
on
Defensive Information Operations

Thought Pieces

TAB G-1 Oversight and Management of the GIG Executive Director

TAB G-2 The Problem Continuum from Data to Understanding

TAB G-3 The Insider Threat & The Low and Slow Attack

TAB G-4 Red Teaming and the Cyber Operations Readiness Triad (CORT)

TAB G-1

ISSUE PAPER

OVERSIGHT AND MANAGEMENT OF THE GIG EXECUTIVE DIRECTOR

Issue: Why the CIO Executive Board and the MCEB are not the right management vehicles to provide oversight and governance for the GIG Executive Director as recommended by the DIO DSB.

Background: The DIO DSB has recommended that at DoD "Information Superiority" Board of Directors (BoD) be established to provide oversight and governance for the GIG Executive Director, an office which would provide systems engineering resources for the Global Information Grid. The membership of this BoD would consist of: Chair, DEPSECDEF, USD(AT&L), Vice Chairman of the Joint Chiefs of Staff, ASD(C3I), and the DDCI.

Discussion:

- **DoD CIO Executive Board:** The current charter of the DoD CIO Executive Board is contained in the DEPSECDEF Memo Subj: DoD Chief Information Officer Executive Board, 31 March 2000. This charter states that the Council is the principal forum to advise the DoD CIO on the full range of matters pertaining to the Clinger-Cohen Act (CCA) of 1996 and the Global Information Grid. Additionally, the Board also coordinates implementation of activities under the CCA, and exchanges pertinent information and discusses issues regarding the GIG, including DoD information management (IM) and information technology (IT). The primary mission of the Board is to "advance the DoD's goals in the areas of IM, information interoperability and information security between and among Defense Components." The Board also coordinates with the IC CIO Executive Council on matters of mutual interest pertaining to the GIG. Its management oversight includes recommending, reviewing an advising the DoD CIO on overall DoD IM policy, processes, procedures and standards, as well as to oversee all aspects of the GIG to support the DoD's and IC's mission and business applications. This includes the collaborative development of IT architectures and related compliance reviews; management of the information infrastructure resources as a portfolio of investments; collaborative development of planning guidance for the operation and use of the GIG; and identification of opportunities for cross-functional and/or cross-Component cooperation in IM and in using IT. The Board's Architecture Management responsibilities include ensuring the collaborative development of architectures as specified in the CCA, and ensuring that processes are in place to enforce their standardized use, management and control, as well as aligning IT portfolios with the GIG. Although the Board has budgetary review authority for IT investments, and can make recommendations, it has no direct budgetary authority. It also has no authority, either review or management oversight into the warrior components of the GIG. The membership of the DoD CIO Executive Board includes:

Page 1196 of 3957

- Chair: DoD CIO (ASD(C3I))
- Members: CIOs of the Military Departments
  CIO, Joint Staff
  USD(AT&L)
  USD (P) (Policy)
  USD (C) (Comptroller)
  USD(P&R) (Personnel and Readiness)
  ASD (C3I) (usually the Deputy CIO)
  Director PA&E (Program Analysis and Evaluation)
  J6, Joint Staff
  OPNAV N6
  Director, Communications and Information, USAF, AF/SC
  IC CIO
  CIO, JFCOM (Joint Forces Command)
- Security Advisor: DIRNSA
- Technical Advisor: Director, DISA
- Legal Advisor: DoD General Counsel

- **MCEB:** The charter of the MCEB is contained within DODDIR 5100.35 dtd 10 Mar 1998. The MCEB is supposed to consider those military communications-electronic matters, including those associated with National Security Systems(NSS) referred to it by the SECDEF, CJCS, the DoD CIO, Secretaries of the Military Departments, and Heads of DoD Components. The mission of the MCEB is to obtain coordination among the DoD components, between the Department of Defense and other Governmental Departments and Agencies and between the DoD and representatives of foreign nations on matters under the MCEB jurisdiction. The MCEB provides guidance and direction to the DoD components and advice and assistance as requested. The membership, as listed below, is primarily the communications activities in the listed components, who have little, if any, authority over IT issues in other portions of their component. The MCEB has no budgetary review or execution authority over any component, nor is there any mechanism within the MCEB structure for enforcement of non-compliance with decisions. The relationship between the MCEB and CIO Executive Board is still being discussed, but in effect, the MCEB is a subordinate activity under the direction of the CIO Executive Board and recommendations referred to that Board for final decision. Membership of the MCEB includes:

  - Chair: Joint Staff, J6
  - Members: Vice, J6
    DISC4, U.S. Army
    OPNAV, N6
    HQ USAF, SC
    HQMC, C4
    USCG, Assistant Commandant for Systems

Director, DISA
Director, NSA
Director, DIA

- **General**: Neither the DOD CIO Executive Board nor the MCEB have the membership or authority over budgets and execution activities envisioned as necessary to ensure the GIG is built and managed as intended. Without that level of authority over all elements of the GIG, the architecture is subject to interpretation by each component based on their needs, rather than the needs of the entire organization. There is also little incentive to address cross-cutting issues in a coherent fashion when the funding for these programs is provided via Title 10 channels without some mechanism to force cooperation. Because of the Title 10 and DoD versus Intelligence Community issues, the only level of management senior enough to cross this bridge is at the DEPSECDEF level. Additionally, neither of these two boards has a direct oversight responsibility over any specific office or function which carries out its direction such as the relationship described between the GIG Executive Director's office (a function which does not currently exist) and the DoD "Information Superiority" Board of Directors.

Recommendation: That a body as described for the DoD "Information Superiority" Board of Directors be established to provide oversight for the implementation of the GIG. With the establishment of such a body, the relationship with existing organizations (i.e. CIO Executive Board and MCEB) must be defined and roles, missions and responsibilities clarified.

Page 1198 of 3957

TAB G-2

THE PROBLEM CONTINUUM – FROM DATA TO UNDERSTANDING

One problem of great concern in today's information age, is the overwhelming volume of data and information readily available over the Internet and through the wide range of sensors that support DoD activities. The push to provide more information to the commander in the field has many commanders concerned that they will be so overwhelmed with data and information that it may actually impede the decision making process.

The key to remedying this problem is recognizing and enabling the transition from data, to information, to knowledge, and ultimately to understanding. The concept of "Decision Superiority" put forth in Joint Vision 2020 requires a greater level of understanding in order to make timely and accurate decisions. DoD must identify those technologies and tools that will ensure the rapid transition from data to understanding, investing today, to build a capability that will enable Joint Vision 2020. Simply pumping more data to the front lines is not the answer. Joint Vision 2020 necessitates a more balanced approach including:

- Decreased dependence on data.
- Increased ability to identify key information.
- Larger degree of knowledge based on key information.
- Clear understanding of the information picture in order to gain and maintain Decision Superiority.

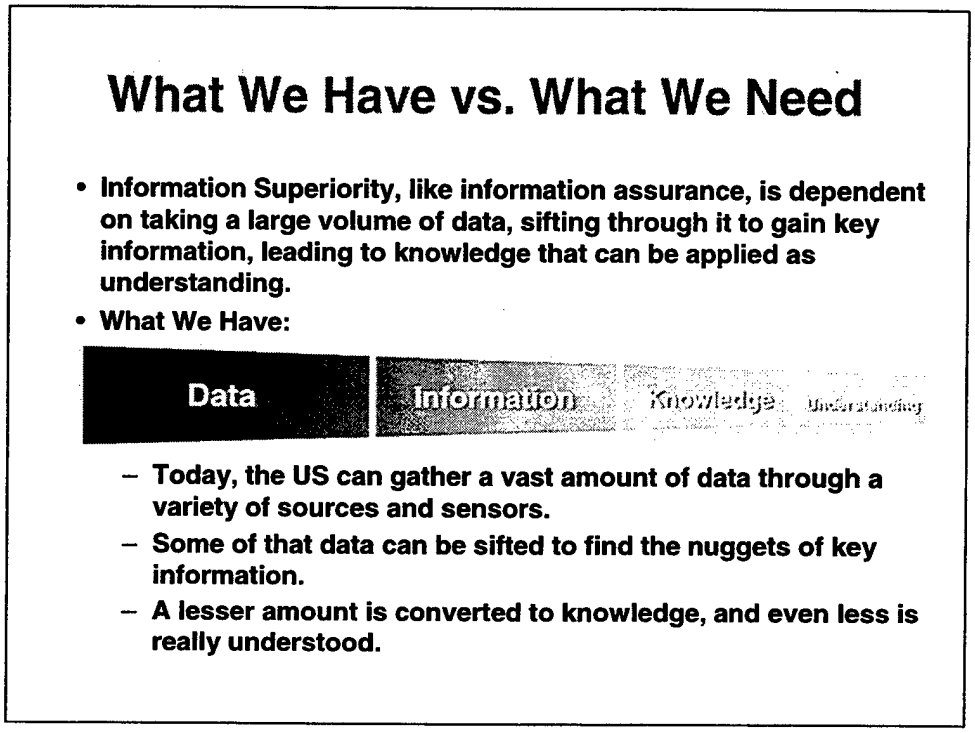
The variety of available and soon-to-be available tools and technologies that support this effort is staggering. Visualization, analysis, and security tools are the centerpiece of the technologies that will enable this transition from data to understanding. Specific categories worthy of investigation include:

- Visualization Tools:
  - Data mining
  - Data warehousing
  - Pattern recognition
  - Profile search agents
- Analysis Tools:
  - Modeling & Simulation
  - Automated data analysis

Page 1199 of 3957

- Security Tools:
  - Intrusion detection
  - Key control
  - Data filtering

The enclosed slides, developed in support of the 1999 Defense Science Board Summer Study, provide further clarification of these critical areas, and the critical transition from data to understanding.



Page 1200 of 3957

What We Have vs. What We Need

What We Need: A More Balanced Approach...

Data	Information	Knowledge	Understanding

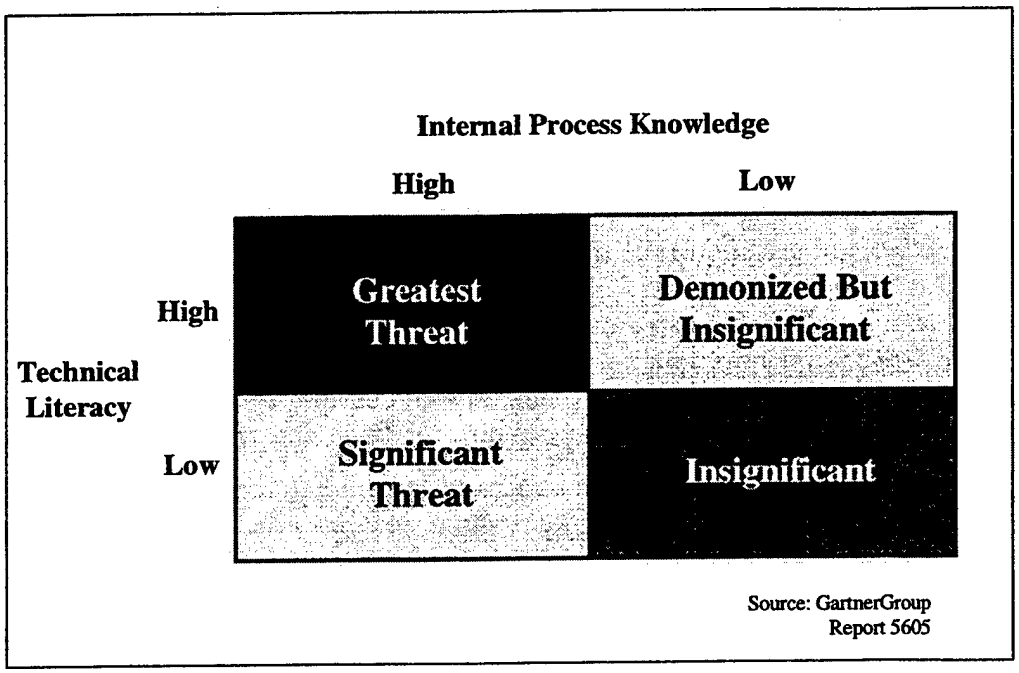
- Decreased dependence on data.
- Increased ability to identify key information.
- Larger degree of knowledge based on key information
- Clear understanding of the information picture in order to gain and maintain Information Superiority.

TAB G-3

THE INSIDER THREAT & THE LOW AND SLOW ATTACK

The threat to U.S. information systems is becoming more and more prevalent as state sponsored terrorists, nation states, and organized crime groups enter the world of cyber warfare. Perhaps the most dangerous threat, however, is the insider and the low and slow attack.

The GartnerGroup published a report in October, 1999, entitled "Information Security Hits the Front Page: How Safe is Safe Enough?" One of the central themes of that report was the danger and likelihood of the insider threat. The following graphic, extracted from the report, demonstrates their conclusions:



The key is as follows:

1) A person with low technical literacy and low internal knowledge is an insignificant threat (bottom right box).
2) A person with high technical literacy and low internal knowledge can be a bother (demonized) but is insignificant (top right box).
3) However, a person with low technical literacy and high internal knowledge (the "dumb" insider) is a significant threat (bottom left box).

Page 1202 of 3957

4) Finally, a person with high technical literacy and high internal knowledge (the "smart" insider) is the greatest threat (top left box).

DoD released the "Insider Threat Mitigation Report" in April, 2000, citing this threat as "real, and very significant." The report cites four basic sources of insider security problems:

- Maliciousness
- Disdain of security practices
- Carelessness
- Ignorance

The report further states that the majority of insiders "are hardworking and dedicated to their professions" and "understand the importance of their work to the nation." The greatest concern, however, is the significant damage a single "malicious" insider could cause. The report continues by stating, "The insider has the capability to disrupt interconnected DOD information systems, to deny the use of information systems and data to other insiders, and to remove, alter or destroy information. Consequently, the insider who betrays the authorities, trust and privileges granted to them may be aided in their malicious activity by the very information systems upon which the department depends."

The report also addresses the Defense Department's heavy reliance on commercial off-the-shelf information systems, adding to the complexities in detecting and dealing with insider threats. The report contends that DoD "has little or no knowledge of who developed the systems and, therefore, no measure of the trustworthiness, reliabilities or loyalties of those individuals". The report acknowledges that individual developers of COTS products "would have an extraordinarily difficult task to target a particular customer because COTS products tend to be produced in large quantities and shipped to customers as an activity that is independent of the individual developer. However, the potential for accepting an error-filled COTS system is real, and demonstrates that "cyber-outsiders can quickly attain many characteristics of an insider".

When this type of infrastructure is attacked from the inside, the results can be catastrophic. The knowledgeable insider has the know-how and the access to delete, modify, or transfer critical data, and may be capable of affecting hardware capabilities through inside attack as well. Add the potential for the low and slow attack, and most network security systems are not capable of detecting unauthorized activity. The low and slow attack is an instance where the attacker uses low visibility access and may not expect or require results for an extended period of time. Data transfers or modifications may be time delayed until the time of the attacker's choosing, or trap doors and trojan horses may be installed for subsequent execution.

The problem is further complicated by the frequent focus toward a perimeter defense mentality to keep out unwanted outsiders, based on the well-published concerns about outside hacker attacks and cyber-terrorism. The real issue is the fact that all of those technological safeguards designed to keep hostile computer attacks out won't help with the disgruntled insider.

Government (GAO) statistics indicate that the average cost of an outside hacking incident was $57,000, while the average cost for a serious insider hacking incident was $2.7 million. This discrepancy merits serious attention if DoD is to have any hope of securing its networks.

Page 1203 of 3957

TAB G-4

"THE CYBER OPERATIONS READINESS TRIAD (CORT)"
VULNERABILITY ASSESSMENTS (VA)
VULNERABILITY EVALUATIONS (VE)
RED TEAMING (RT)

BACKGROUND:

Recently, ASD(C3I) has asked where the Discover Vulnerabilities (DV) process and IO Red Teaming fits into the larger picture of DoD "force readiness protection" and Defensive Information Operations (DIO). ASD(C3I) has also asked the question; "Does DoD actually have a standing DIO Red Team? The answer to that question is yes. NSA is DoD's Red Team, and is the team of choice to do adversarial Red Teaming within DoD. The larger issue of a total look at cyber force readiness as well as Red Teaming is a timely one as the DV process begins to take shape in DoD. Questions like, where does DV belongs in DoD; who is the lead organization; who leads overall technical training of the force; how do we measure readiness; what are the standards/metrics for Readiness; and the question of Defense contractors assisting in meeting the extensive tasking are of importance.

PURPOSE:

This white paper will describe:

- The existing discover vulnerability (DV) process within NSA, recommendations for potential modification to the process, and a possible win-win solution to current operations with regard to the use of the civilian contracting community.
- The IO Red Team process, it's role in force readiness protection and Defensive Information Operations (DIO) and what Red Teaming could evolve to based on NSA's experiences from Eligible Receiver (ER) and the 40+ exercises conducted since then.

DISCUSSION:

NSA and the Services.

The NSA Red Team, as part of NSA's Information Systems Security Organization's (ISSO) mission, is to improve the Operational Readiness (OR) & Defensive Information Operations (DIO) posture of DoD and it's components. The NSA Red Team is an interdisciplinary and sophisticated "opposing force" (OPFOR) that utilizes active and passive, as well as technical and non-technical capabilities to expose and exploit customer IO vulnerabilities in order to improve

Page 1204 of 3957

operational readiness. Based on Red Team findings, timely feedback is provided directly to the customer consisting of their vulnerabilities as well as specific recommendations and countermeasures to thwart potential real-world exploitation of their computer and network systems.

Organizations "stressed" by NSA's Red Team operations gain a sense of their general cyber readiness by measuring effectiveness in protection, detection, response, and reconstitution during Red Team exercises. Upon customer request and negotiated between the customer and the NSA Red Team (also incorporated into the "Rules of Engagement" (ROE)), the NSA Red Team may use cooperative partners & alliances to work as a true OPFOR covering more than one pillar of IO. In the past, the NSA Red Team has partnered with other internal NSA organizations, as well as CIA, DIA, JTF/CND, NIPC, DHS, AFIWC, LIWA, FIWC, SOCOM, and the Military Services.

It is an over statement to say that the readiness posture of individual DoD organizations varies widely across the Department. Some of the component organizations within the CINCs, Services, or Agencies maintain highly effective DIO programs, while others place less emphasis on securing of their networks. Reasons vary for this dilemma, but are telling. For the Services, the total number of people who are highly skilled at discovering and exploiting vulnerabilities remains small, and their time and efforts must be managed wisely. Further, the quantities of such persons are uneven across the Services. For this reason, the Services play up to their strengths, offering a range of assessment services that maximizes their skill usage. The bottom line for the Services is that they cannot yet muster the critical mass of personnel skilled in the area of DV. The CINC's are not in much better shape, as they draw on the Military Services for their technical manpower. Currently, NSA is the only DoD entity that has the ability to focus full-time on computer **and** network vulnerability discovery at all levels of the process. It is NSA's view that it should be designated as DoD's EA for Discovering Vulnerabilities (DV). We have the talent and know-how to organize DoD in the DV process. However, it is also our view that the DV process requires refocus and a relook on where DoD needs to concentrate limited.

THE PROCESS:

We see the DV methodology as a cyclic process composed of 3-levels of service surrounded by OPSEC. The process is called "THE CYBER OPERATIONS READINESS TRIAD (CORT), and it's main goal is to improve the cyber security of DoD. The initial level, called a *Vulnerability Assessment or Infosec Assessment*, provides a high-level review of a customer's automated information system (AIS) security policies, plans, and procedures to determine if a minimal level of protection is in place. This is what is known as a Level 1 assessment. No legal authority is required to conduct this assessment. These people are responsible to support DoD and DoD/NII-associated partners. Due to increased customer request for this service, and working with the National Institute of Standards (NIST) and the DIAP, we have initiated the Information Security System Capabilities Maturity Model (ISS-CMM) process. This process invites the Defense contracting community to become "authorized", via a validated training program, to conduct Level 1 assessments to the same level as NSA. The only difference in the end result is the customer and Contractor negotiate a price for the assessment conducted. For this level of assessment, the contracting community is technically suited to conduct level 1 assessments and is a workable solution to PDD-63 customer concern over DoD evaluators in

their systems. The second level of assessment (Level II) is called a *Security or Vulnerability Evaluation.* This process looks past the basics and provides an in-depth technical analysis of a customer's information system(s). The objective is to identify *any and all* vulnerabilities (not just those associated with a specific threat agent) and assist the customer organization in addressing them. This type of DV evaluation requires NSA general counsel (AGC(I)) and DDI approval to touch a DoD customers networks or computer systems. In order for final approval, the customer must meet certain criteria and standards when requesting NSA to actually "touch" the network. This is an extremely technical operation and requires a certain skill-set to complete the task. Heretofore, NSA has been the only DoD element to conduct this in depth testing on a system or network. It is our experience that the Military Service elements conduct varying degrees of Level 1 and Vulnerability Evaluations and each conducts these services to a component with their own set of standards. *IO Red Teaming* is the third (Level III) and final level of service. It is *normally* reserved for larger DoD elements and other customers who are looking to test their networks and cyber security in an exercise environment, either as a no-notice Red Team-only evolution or as part of a larger exercise; e.g., the Marine exercise URBAN WARRIOR. SECDEF approval is required to conduct these operations and due to the complexity and technical nature of Red Teaming operations, NSA remain the only operative element to conduct this type of Red Teaming. Further dialogue is required to come to closure on where the Military Services and the Defense Contracting community play in the Vulnerability Evaluation (Level II) process and Red Teaming and what standards/metrics are required.

Once Red Teaming is performed on a system and/or network(s), the customer would optimally reevaluate where they are in their respective security environment and then via the Vulnerability Assessment Vulnerability Evaluation, or Red Teaming process, relook at what is required to secure their networks. This continuous process is a strong and proven force in "raising the bar for readiness" on computer and network security. It is this paradigm under which the NSA DV process operates, and that we believe should be required within all DoD Components.

DEFINITION:

A Red Team, as defined in the draft of DoD Directive 3600.3 "DoD Information Operations Red Teaming" is:

> *"An independent, threat-based, and simulated opposition force that uses passive, active, technical, and non-technical capabilities on a formal, time-bounded basis to expose and exploit information system vulnerabilities of friendly forces."*

The directive further states that:

> *"The goal of Red Teaming is to improve the readiness and defensive IO posture of DoD Components."*

In general, a large portion of the Defense community concurs with the DV process, however, there remains many entities throughout the Department, other government agencies, and the private sector who do not subscribe to, define as, or conform to conducting vulnerability discovery in this manner. It is our sense that the DV process be standardized across the board.

Page 1206 of 3957

Should NSA be given the EA responsibility for DV in general, it is our view that we would further refine and adjust the process for use in DoD.

THE PRIVATE SECTOR:

The DV process covers three levels of service. We believe the private sector can play a pivotal role in filling the Departments needs in the DV process where we (NSA, DoD Services, Agencies, etc) are over tasked and lacking, in some areas, skilled personnel. It is our sense that the VA and VE process, where appropriate, can be assisted by the Defense contracting community if trained and certified appropriately. Although a relatively new endeavor, the ISS-CMM for the VA process is proving a workable alternative. Equally, we believe if structured properly, and a system set up to assure the results are equal to the existing VE process, that private sector could assist in that part of the DV process, as well. However, NSA has not yet initiated an effort to begin the training and certification process for vulnerability evaluation (level II) work. If tasked, the strategy is to slowly build-up competencies for Level I assessments within Industry, and then grow additional expertise from there. Our vision is to ultimately *share* with the private sector requirements for Level II evaluations. (I deleted the last sentence)

With regard to Red Teaming, we believe there should be measured involvement by the Defense Contracting community. Contractors are involved in Red Teaming now, however, only as working under NSA authorities. There may come a time, because of the growing concern over cyberattack that we reevaluate contractor play across the board as it applies to Red Teaming. The Red Team is an opposing force. We "attack" U.S. systems. We succeed at breaking into U.S. systems. We have a very elaborate structure in place to handle our mission and/or if our mission goes awry. We have a trusted agent network, deconfliction process, classified tools and techniques, access to real world threat and resource information, sophisticated laboratory testing procedures, cover program, legal authorities and most importantly, a dedicated cadre and critical mass of career personnel with TS/SCI clearances. It also should be stated that we are creating lasting relationships & liaisons with other military departments, Agencies, and others that would simply be extremely difficult for private industry to emulate. Lastly, the "trust and ethical" issues would be most acute. We do not believe that system owners of the most sensitive DoD networks (SIPRNET, JWICS, etc) would feel comfortable with private industry performing the DoD's most sensitive vulnerability evaluations without a DoD cover or operational authority. Since this service is performed at the local as well as the "remoted" level, we envision huge conflicts with private industry performing such services, since they do not have the legal authority to use "jump-points" throughout DoD networks and Agencies.

Exercise planning for Red teaming in the outyears:

Fiscal Year		FY-00	FY-01	FY-02	FY-03	FY-04	FY-05	FY-06	FY07
Major Exercises(CINC-level)		4	8	10	12	14	14	14	14
Minor Exercises		4	6	8	10	10	10	10	10

CONCLUSION:

IO capabilities of DoD's adversaries are growing and becoming more sophisticated. These adversaries include hackers and other unstructured groups intent on supporting political objectives, and structured groups such as terrorists, rogue nations, or nation states. In addition, the strategies of our adversaries are becoming increasingly clever, drawing from across the spectrum of IO techniques. With the growing number of hacking groups and the ease with which a terrorist group or nation state can obtain the tools necessary to conduct an IO campaign, the threat is harder to identify and stop without proper training and readiness. It is essential that the United States have the capability and experience necessary to counter such threats. Issues such as Solar Sunrise, which almost stopped a US troop deployment, the I Love You Virus, as well as the well publicized intrusion called Moonlight Maze, highlight just some of the growing threats. Red Teams and the DV process can "hone" the DoD's DIO capability and provide the experience required to enhance the security awareness and readiness posture; necessary elements to dominate in conflicts where IO represents a strategic advantage.

Page 1208 of 3957

ANNEX H

Defense Science Board Task Force
on
Defensive Information Operations

Reference Data

TAB H-1 **CERT and IO POC Listings**

TAB H-2 **Terms of Reference**

CERT AND IO POC LISTINGS

Name	Function/Constituency	E-Mail/WWW URL
AFIWC - Air Force Information Warfare Center	USAF IW coordination and support to the Numbered Air Forces (in addition to the IO-Flights assigned directly)	http://www.afiwc.aia.af.mil/ http://www.afcert.csap.af.mil/
ANSIR – Awareness of National Security Issues and Response (FBI)	Subset of NIPC providing advisories for corporate security professionals (subscribable messaging)	http://www.leo.gov/ gharter@leo.gov http://www.fbi.gov/ansir.htm
ASD(C3I) – Assistant Secretary of Defense for Command, Control, Computers, and Intelligence	Principal advisor to the President for C3I	http://www.c3i.osd.mil/
CIA – Central Intelligence Agency	Office of Transnational Issues (OTI) Clandestine Information Technical Office (CITO)	http://www.odci.gov/cia/
CIAO -- Critical Infrastructure Assistance Office	Formed from President's Commission on Critical Infrastructure Protection. Site provides text and summary of PDD 62/63, and related policy papers	http://www.ciao.gov/
CND-JTF – Computer Network Defense Joint Task Force	Task force on DoD Computer Network Defense	jtfwo@assist.disa.smil.mil
DARPA – Defense Advanced Research Project Agency	DoD specialized advanced research projects	http://www.darpa.mil/

Page 1210 of 3957
Page 1210 of 3957

Page 1211 of 3957

DIA – Defense Intelligence Agency	IPB for IW / STO coordination & Defensive IO Transnational Warfare Issues (TW) Branch & Information Warfare Support Office (TWI)	http://www.odci.gov/ic/usic/dia.htm
DISA – Defense Information Systems Agency	DoD agency responsible for information technology; central manager for the DII; Answers to ASD(C3I) Center for Information Systems Security (CISS) Automated System Security Incident Support Team (ASSIST)	http://www.disa.mil/ http://www.disa.mil/ciss/index.html http://www.assist.mil/
FIWC – Fleet Information Warfare Center	Operational IW/C2W support to the fleet (Norfolk and San Diego)	http://www.fiwc.navy.mil/
IOTC – Information Operations Technology Center	DoD/DCI center at Ft Meade focused on technology trends (not geographic) for IO Advanced Tech Group (ATG) Analysis & Assess Grp (AAG) Community Coordination Group (CCG)	
ITAC -- Infosec Technical Assistance Center	Navy Infosec assistance service	itac@infosec.navy.mil
JC2WC – Joint Command and Control Warfare Center	Joint support to IO/C2W Located at Kelly AFB, San Antonio	

Page 1211 of 3957

JCS J2	Intelligence; Deputy Dir for Targets (J2T)	http://www.dtic.mil/jcs/
JCS J3	Operations; J39: Deputy Director for IO	http://www.dtic.mil/jcs/
JCS J6	C4; Information Assurance Div	http://www.dtic.mil/jcs/
JCS J8	Force Structure; Joint Warfighting Capabilities Assessment (JWCA)	http://www.dtic.mil/jcs/
JPO – Joint Program Office	Internal US vulnerability assessments	
JSC – Joint Spectrum Center	Management of the electromagnetic spectrum	http://www.jsc.mil/
JWAC – Joint Warfare Analysis Center	External vulnerability assessments; infrastructure & IO focus	http://www.jwac.ic.gov/
LIWA – Land Information Warfare Activity	Army IO coordination and field support	Site under revision
MITRE Corp	FFRDC providing IO-related analysis, and C2 systems analysis	http://www.mitre.org/ corpc@mitre.org
NGIC – National Ground Intelligence Center	Provides Army intelligence support to IO: Ground Crisis Action Team; IW Ground Control Team; Army CI Center	
NIPC – National Infrastructure Protection Center	Critical infrastructure protection (FBI&Other agencies)	nipc@fbi.gov http://www.nipc.gov/
NRO -- National Recon. Office	Space recon systems; Global information superiority	http://www.nro.odci.gov/

Page 1212 of 3957

Page 1212 of 3957

NIST -- National Institute of Standards & Technology	Technical measures and standards coordinated with industry	http://www.nist.gov/
NIWA – Naval Information Warfare Activity	Naval lab support to IW; fielding IW systems; assessing vulnerabilities; IW mod/sim	
NSA – National Security Agency	Infosec; Encryption; Information System Security Organization (ISSO)	http://www.nas.gov/ www.nsa.gov:8080
OSD-NA - Office of the Secretary of Defense for Net Assessment	Assessments on a variety of US vs Other capabilities, including IO/IW	http://www.defenselink.mil/pubs/almanac/osd.html
PM-IW - Program Manager for Information Warfare (Army)	Army acquisition program manager for IW	No web site available
RAND Corp	FFRDC providing C2 systems analysis and integration; focusing on production, distribution, and safeguarding of intelligence information	http://www.rand.org/
USD(C) US Department of Commerce	Trade issues related to IO	http://www.doc.gov/
USD(J) - US Department of Justice	Legal issues related to IO and FBI involvement	http://www.usdoj.gov/
USD-P - Under Secretary of Defense for Policy	Policy advise for IO and ROE	http://www.defenselink.mil/pubs/almanac/osd.html
USD(S) - US Department of State	Foreign policy including IO related issues	http://www.state.gov/

Page 1213 of 3957

Page 1213 of 3957

Page 1214 of 3957

USCENTCOM US Central Command	J33 – IO Cell	http://www.centcom.mil/
USSOCOM - US Special Operations Command	Special Operations – Information Operations Office (SOIO)	http://www.socom.mil/
USSOUTHCOM - US Southern Command	J33 – IO Cell	http://www.ussouthcom.com/southcom

LABS

ARL - Army Research Lab	Electronic Warfare, Directed Energy, and Electronic Countermeasures research; Information Science and Technology Branch (IS&T)	http://www.arl.mil/ gowens@arl.mil
Carnegie Mellon University	Founder of CERT for Internet; Provides advisories and tools	http://www.cert.org/ http://www.cmu.edu/
CSRC - Computer Security Resource Clearinghouse	Collects and disseminates compusec information and assistance; encryption support and incident handling	http://www.csrc.ncsl.nist.gov/
Lawrence Livermore National Lab	Department of Energy focus in support for: Computer Incident Advisory Capability (CIAC); Computer Security Technical Center (CSTC); Department of Energy – Information Security (DOE-IS)	http://www.llnl.gov/ http://www.ciac.llnl.gov/ http://www.ciac.llnl.gov/cstc http://www.doe-is.llnl.gov/

Page 1214 of 3957

Lincoln National Lab	FFRDC specializing in advanced electronics, network survivability, air traffic control, and radar/space systems – USAF affiliation	http://www.ll.mit.edu/ office@sst.ll.mit.edu
NRL - Naval Research Lab	R&D for IW/EW/Sensing technology; Information Technology Division (Code 5300)	http://www.nrl.navy.mil/
Rome Lab	USAF affiliated R&D for information systems: Info & Intelligence Exploitation; Information Grid; Information Technology Division	http://www.if.afrl.af.mil/
Sandia National Lab	R&D focus for computers, information science, pulsed power, SCADA assessments	http://www.sandia.gov/
SPAWAR / IOCOF	Develop, procure, field and support interoperable Navy IW systems (PD16); IOCOF – Information Operations Center of the Future: Provides integrated IO strategies, concepts, and services; assesses technologies; experimentation; and wargaming	http://www.spawar.navy.mil/ http://www.infosec.navy.mil/code72.html IOCOF web site under revision

Page 1215 of 3957

Page 1215 of 3957

Page 1216 of 3957

Selected Computer Emergency Response Teams Worldwide

Response Team	Constituency	E-Mail/WWW URL
Advanced Network Services, INC (ANS)	ANS Customers	Anscert@and.net http://www.ans.net
Air Force CERT (AFCERT)	Air Force	Afcert@afcert.csap.af.mil
Apple Computer	Apple Computer	Isefton@apple.com
Australian CERT (AUSCERT)	Australia	Auscert@auscert.org.au Http://www.auscert.org.au
Bellcore	Bellcore	Sb3@cc.belcore.com
Boeing CERT (BCERT)	Boeing	Compsec@maple.a1.boeing.com
BSI/GISA	German Government	Fwf@bsi.de http://www.cert.dfn.de/eng
CCTA	UK Government and Agencies	Cbaxter.esb.ccta@gnet.gov.uk
CERT Coordination Center	UNIX, Internet Research	Cert@cert.org http://www.cert.org
CERT-IT	Italian Internet Sites	Cert-it@dsi.unimi.it
CERT-NL	SURFnet Sites	Cert-nl@surfnet.nl http://www.nic.surfnet.n1/surfnet.security.cert-nl.html
Cisco Systems	Cisco Systems	Karyn@cisco.com

Page 1216 of 3957

Response Team	Constituency	E-Mail/WWW URL
DEC SSRT	Digital Equipment Corp and Customers	Rich.boren@cxo.mts.dec.com
Defense Research Agency Malvern	Defense Research Agency	Shore@ajax.dra.hmg.gb
DFN CERT	Germany	Dfncert@cert.dfn.de
DISA	MILNET	Scc@cc.ims.dsa.mil
DoD ASSIST	DoD Interest Systems	Assist@assist.mil
DOE CIAC	Department of Energy	Ciac@llnl.gov http://ciac.llnl.gov
DOW USA	DOW	Whstewart@dow.com
EDS	EDS and Customers	Jcutle01@novell.trts01.eds.com
FedCIRC	Federal Gov/Civil Agencies; Incident reports & handling	http://www.fedcirc.gov/ fedcirc@fedcirc.gov
FIRST	Forum of Incident Response and Security Teams	First-sec@first.org http://www.csrc.ncsl.nist.gov/first/
General Electric	GE Businesses	Sandstrom@gies.ges.com
Goddard Space Flight Center	Goddard SPC	Hmiddleeton@gsfcmai.nasa.gov
Goldman, Sachs and Company	Goldman, Sachs offices Worldwide	Safdas@gsco.com
Hewlett Packard	All HP-UX Customers	Security-alert@hp.com
Israeli Academic Network	Israeli University users	Cert-1@vm.tau.ac.il
Janet Cert	All JANET networks	Cert@cert.ja.net

Page 1217 of 3957
Page 1217 of 3957

Page 1218 of 3957

Response Team	Constituency	E-Mail/WWW URL
JP Morgan	JP Morgan employees and consultants	
MCI	Corporate Systems Security	6722867@mcimail.com
Micro-BIT Virus Center	Anyone	Ry15@uni-karlsrube.de
Motorola CERT	Motorola	Mcert@mot.com
NASA (Ames Research Center)	Ames Research Center	Hwater@nas.nasa.gov
NASIRC – NASA Automated Incident Response Cap.	NASA and International Aerospace Community	Nasire@nasirc.nasa.gov http://nasirc.nasa.govNASIRC_HOME.html
NavCIRT	U.S. Navy	navcirt@fiwc.navy.mil http://infosec.nosc.mil/navcirt.html
NIST/SCRC	National Institute of Standards And Tech.	Jwack@nist.gov http://cs-www.ncsl.nist.gov
NORDUnet	NORDUnet	Ber@sunet.se
Northwestern University	Northwestern Faculty/Staff/Students	r-safian@nwu.edu http://grumpy.asns.nwu.deu/nu-cert
Penn State University	Penn State Faculty/Staff /Students	Krk5@psu.edu
Purdue CERT	Purdue University	Pcert@cs.purdue.edu http://www.cs.purdue.edu/pcert/pcert.html
Renater	Minister of Research and Education	Morel@urec.fr

Page 1218 of 3957

Response Team	Constituency	E-Mail/WWW URL
SBACERT	Small Business Nationwide (US)	Hfb@oirm.sba.gov
Silicon Graphics, Inc	Silicon Graphics User Community	Security-alert@sgi.com
Stanford University NST	Stanford University Faculty/Staff/Students	Security@stanford.edu http://www.stanford.edu/security/
SUN Microsystems	SUN Customers	Mark.graff@sun.com
SWITCH	Swiss Universities and Government	Cert-staff@switch.ch http:/www.switch.ch/switch/cert
TRW Inc.	TRW Network and System Administrators	Zorn@gumby.sp.trw.com
U.S. Sprint	SprintNet(X.25) and Sprint Link (TCP/IP)	Steve.mathews@sprint.sprint.com
UCERT	UNISYS Users	Garb@po3.bb.unisys.com
Veterans Health Administration IRT	Veteran's Health Administration	Frank.marino@forum.va.gov http://www.va.gov
Westinghouse Electric Corp.	Westinghouse Corp	Nicholson.m%wec@dialcom.tymnet.com

Page 1219 of 3957
Page 1219 of 3957

TAB H-2

TERMS OF REFERENCE

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION AND
TECHNOLOGY

FEB 29 2000

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board Task Force on Defensive Information Operations

You are requested to form a Defense Science Board (DSB) Task Force to review and evaluate DoD's ability to provide information assurance to carry out Joint Vision 2010 in the face of information warfare attack.

Tasks to be accomplished:

Using the "1996 DSB report on Information Warfare – Defense" as the departure point, address the following:

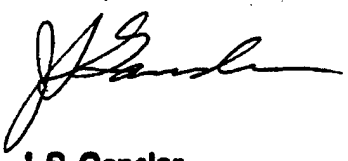
- What is the status of action on the recommendations?
- Where there are shortfalls, what are the barriers to action and what should be done?
- What important aspects did the 1996 Task Force miss that should have been addressed?
- Assess the recommendations of other important reports that have addressed information assurance issues.

The Defensive Information Operations Task Force will determine:

- Adequacy of the process toward the information assurance goals needed to carry out Joint Vision 2010.
- Adequacy of the Department's readiness to project and sustain power in the face of information warfare attacks.
- The appropriate role(s) and capability of DoD to provide information assurance in support of Homeland Defense and in support of Critical Infrastructure Protection.
- Recommendations for research and development which are uniquely in DoD's interest, and thus not likely to be accomplished by the private sector in the time required to meet DoD's Defensive Information Operations objectives.
- Areas in which DoD should seek strong partnering relationships outside DoD, such as with the Critical Infrastructure Assurance Office (CIAO).
- The Task Force should provide an interim report by June 30, 2000 and the final report around October 2000.

The study will be co-sponsored by the Under Secretary of Defense (Acquisition, Technology and Logistics) and Assistant Secretary of Defense for C3I. Mr. Larry Wright will serve as the Task Force Chairman; Col Gregory Frick will serve as the Executive Secretary; and Maj Tony Yang, USAF, will serve as the Defense Science Board Secretariat Representative.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5104.5, "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, United States Code, nor will it cause any member to be placed in the position of acting as a procurement official.



J. S. Gansler

OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
27 APRIL 2023 DHS-IA-IF-2023-07757

FOREIGN INFLUENCE

(U//FOUO) China: Municipal Government Publishing Anti-US, Pro-China Social Media Content With Limited Reach

(U//FOUO) ***Scope Note:*** *DHS has attributed a cluster of inauthentic Twitter accounts to a municipal government entity in the People's Republic of China. At least some of the accounts are part of a larger unattributed network of social media accounts that promotes Beijing's interests, called DRAGONBRIDGE. Our attribution of these accounts to the municipal government could yield continuing insight into People's Republic of China social media messaging operations; this analysis provides a framework for identifying and attributing other PRC clusters, which may grant greater insight into the command and control structures of PRC social media messaging operations.*

(U//FOUO) **A People's Republic of China (PRC) municipal government-controlled media outlet is very likely directing a cluster of English-language, coordinated inauthentic Twitter accounts that posted content denigrating the United States *(see graphics).*** The cluster of accounts, which we have dubbed SPICYPANDA, has been active from at least January 2021 and has published sophisticated content, but it failed to grow a follower base thus far. DHS attributed SPICYPANDA to the municipal media entity Chongqing International Communications Center (CICC) based on its leadership's creation of SPICYPANDA's anti-US messaging campaign, its overt ties to a website promoted by the accounts, and its Western social media messaging accolades and capabilities.

- *(U//FOUO)* From August 2021 through February 2022, SPICYPANDA carried out a messaging campaign created by the CICC Editor-in-Chief of Overseas Social Media, judging from a professional biography and a review of the identified accounts. This messaging campaign offered pro-PRC and anti-US commentary on current events by portraying the United States as a global antagonist, especially relating to the US Intelligence Community's investigation of the origins of COVID-19, the US withdrawal from Afghanistan, the Summit for Democracy, and the 2022 Beijing Winter Olympics *(see graphic 2)*.
- *(U//FOUO)* SPICYPANDA also aggressively amplified a Twitter account overtly operated by CICC for the Chongqing municipal government, judging from a DHS

Page 1223 of 3957

review of the accounts. This account, and an associated website called iChongqing, presents news about Chongqing and resources for individuals looking to visit, study, or invest in the city. The website is overseen by the Chongqing Municipal Party Committee's Propaganda Department, according to a Chinese-language newspaper article about the website's launch.

- *(U//FOUO)* In addition to its relationship with the Chongqing local government, CICC was tasked in 2018 by the Chinese Communist Party (CCP) with influencing overseas audiences on behalf of the city, and it received an award in 2020 for the quality of its overseas communications, judging from Chinese state media reporting and numerous Chinese language job postings. In February 2021, CICC further committed to using Western social media accounts by seeking to hire staff to operate them, according to a Chinese language news article and job postings.

(U//FOUO) **Overview of DRAGONBRIDGE and its Narratives**

(U//FOUO) Some of the identified inauthentic Twitter accounts are part of both the SPICYPANDA cluster and a larger network known as DRAGONBRIDGE. DRAGONBRIDGE has been tracked for the past three years by private sector researchers, but it has not been previously attributed—in whole or in part—to a specific person or group.

(U//FOUO) DRAGONBRIDGE (also known as SPAMOUFLAGE DRAGON) is a large network of social media accounts first observed on Facebook, Twitter, and YouTube in 2019 criticizing pro-democracy protests in Hong Kong. Since then, accounts in the network have been observed posting in seven languages on 20 social media platforms and on over 40 other websites. The network is comprised of many clusters of co-managed accounts that seemingly operate independently of each other, judging from two private sector analytic reports on the network and a DHS review of identified and suspected accounts. DRAGONBRIDGE has employed at least 100,000 accounts in its history on a single social media platform, according to the identified platform, and we assume it has employed similar numbers of accounts on other major platforms. Despite the size of the network, it rarely engages with authentic social media users; however, it has had some limited success in reaching individuals recently.

(U) Since 2019, DRAGONBRIDGE has posted content regarding Hong Kong, COVID-19, the US withdrawal from Afghanistan, Taiwan, the 2022 Beijing Olympics, rare earth mineral mining companies, the 2022 US midterm election, and many other topics. Content promoted by the network is consistently aligned with Beijing's interests.

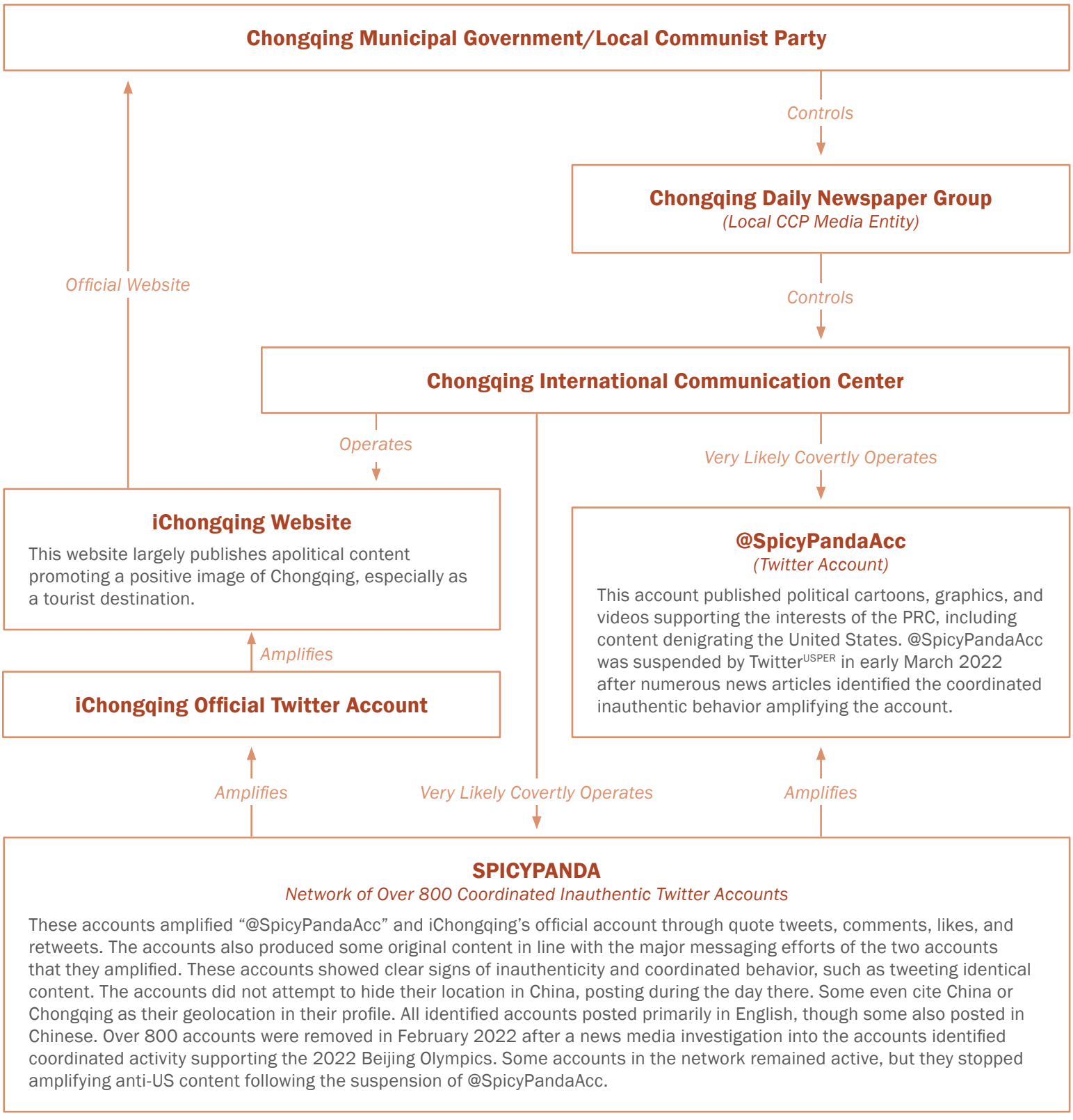
(U//FOUO) **The reach of SPICYPANDA's content likely was limited by its narrow focus on PRC-related issues, obvious indications of inauthenticity, and ongoing enforcement mechanisms. However, DHS's attribution of the accounts could yield greater insight into PRC adjustments and improvements in future social media campaigns.** SPICYPANDA illustrates the PRC's ability to publish commentary on current events through sophisticated content, including videos, memes, and topical political cartoons, which may reach more Americans if the PRC overcomes the obstacles that constrained SPICYPANDA's reach.

- *(U//FOUO)* Content proliferated by SPICYPANDA primarily focused on themes of political importance to the PRC, which may interest few US social media users. Individual accounts lacked convincing personas, and content intended to attract views was infrequent and insufficient to entice people to actively follow the accounts, judging from a review of identified accounts.
- *(U//FOUO)* Clear indications of the accounts' inauthenticity may have also reduced the reach of SPICYPANDA, as we assume authentic users generally seek to avoid inauthentic accounts and indications of inauthenticity enabled the removal of the accounts. Twitter[USPER] sporadically removed accounts in the network and removed over 800 accounts for rules violations in February 2022 following two Western newspapers' identification of the accounts as inauthentic; at least three dozen remain. While the DRAGONBRIDGE network has rebounded from numerous takedowns in the past, removals prevent accounts from building large follower bases.
- *(U//FOUO)* Despite using relatively unsophisticated accounts, SPICYPANDA published timely and highly sophisticated content, including dozens of original political cartoons, graphics, memes, and videos, judging from a review of identified accounts. These posts often responded to trending news topics within days and leveraged popular, and sometimes divisive, figures to press their narratives. SPICYPANDA responded more dynamically to emerging events than other pro-PRC inauthentic networks, judging from open-source reporting and a DHS review of the accounts.

OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
27 APRIL 2023

(U//FOUO) Known and Assessed Relationships Between Chongqing Municipal Government and SPICYPANDA Social Media Account Cluster

OVERALL GRAPHIC 1 CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY



OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN FOCUS

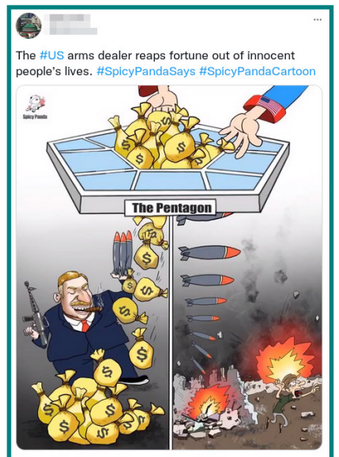
27 APRIL 2023

(U//FOUO) Timeline of Select SPICYPANDA Narratives From August 2021 Through February 2022

(*U//FOUO*) SPICYPANDA engaged in three distinct messaging campaigns on Twitter between January 2021 and the present, judging from a review of the identified accounts. From July 2021 through a partial takedown at the end of February 2022, the accounts published commentary on current events that aligned with Beijing's interests, with a particular focus on denigrating the United States (depicted below). From August 2021 through a partial takedown in February 2022, the accounts promoted content extolling the PRC's achievements in technology, infrastructure, and environmentalism. Finally, from at least January 2021 through the present, including after the takedown of most accounts, SPICYPANDA published content praising the city of Chongqing.

OVERALL GRAPHIC 2 CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

EXAMPLE TWEETS



PRECIPITATING EVENTS

27 Aug: US Government COVID Origin Investigation Concludes

30 Aug: US Withdrawal From Afghanistan

9–10 Dec: US-Hosted Summit For Democracy

4–20 Feb: Beijing Olympics

AUGUST 2021	SEPTEMBER 2021	OCTOBER 2021	NOVEMBER 2021	DECEMBER 2021	JANUARY 2022	FEBRUARY 2022

MAJOR NARRATIVES

SPICYPANDA suggested COVID-19 originated in a biolab in the United States and that the US Intelligence Community's investigation into its origin was a ploy to denigrate China.

SPICYPANDA portrayed the United States as a global antagonist that profited from the conflict at the expense of the Afghan people. Criticism of the US military continued through November.

SPICYPANDA argued that the US system of democracy is unjust and inferior to China's system of government. The accounts also extolled the Hong Kong elections.

SPICYPANDA almost exclusively promoted the 2022 Beijing Olympics during the event. The accounts also criticized the US diplomatic boycott.

PARTIAL TAKEDOWN
Over 800 accounts removed for violating Twitter's rules.

Source, Reference, and Dissemination Information	
Privacy, Civil Rights, Civil Liberties, Intelligence Oversight Notice	*(U//FOUO)* US persons linking, citing, quoting, or voicing the same arguments raised by these foreign influence activities likely are engaging in First Amendment-protected activity, unless they are acting at the direction or control of a foreign threat actor. Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect foreign influence or malign activity absent information specifically attributing the content to malign foreign actors. This information should be considered in the context of all applicable legal and policy authorities to use open-source information while protecting privacy, civil rights, and civil liberties.
Definitions	*(U//FOUO)* **Co-Managed Accounts:** Accounts that are operated by the same person or entity. *(U//FOUO)* **Coordinated Inauthentic Behavior:** An evolving and varied term used by social media platforms to describe a form of online manipulation that relies on multiple fake accounts—either assumed or fabricated—acting together to achieve a strategic goal. This activity can include creating false or divisive narratives, building false audiences, and amplifying existing narratives or conspiracy theories. It can also include the use of artificial intelligence tools, including bots, to create authentic-looking fake users and increase content dissemination and interaction. These methods vary by platform. *(U//FOUO)* **Coordinated Inauthentic Account:** An account that is co-managed with others and engaged in coordinated inauthentic behavior (see above). *(U//FOUO)* **Foreign Influence**: Any covert, fraudulent, deceptive, or unlawful activity of foreign governments—or persons acting on their behalf—undertaken with the purpose or effect of influencing, undermining confidence in, or adversely affecting US democratic processes or institutions or otherwise affecting sociopolitical sentiment or public discourse to achieve malign objectives. • *(U//FOUO)* **Covert Influence:** Activities in which a foreign government hides its involvement, including the use of agents of influence, covert media relationships, cyber influence activities, front organizations, organized crime groups, or clandestine funds for political action. • *(U//FOUO)* **Overt Influence:** Activities that a foreign government conducts openly or has clear ties to, including the use of strategic communications, public diplomacy, financial support, and some forms of propaganda. *(U//FOUO)* **Network:** In this product, "network" always refers to the DRAGONBRIDGE network of accounts. See text box, "Overview of DRAGONBRIDGE and its Narratives" for more details on DRAGONBRIDGE/SPAMOUFLAGE DRAGON. *(U//FOUO)* **Cluster:** In this product, "cluster" always refers collectively to the co-managed accounts operated by CICC. These accounts make up a subset of the accounts that make up the DRAGONBRIDGE network.
Reporting Suspicious Activity	*(U)* **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi. *(U)* **To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form.** The US-CERT Incident Reporting System provides a secure, web-enabled

	means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent. *(U)* To report a similar incident to the Intelligence Community, please contact your DHS I&A Regional Intelligence officer at your state or major urban area fusion center, or e-mail DHS.INTEL.ORI.HQ@hq.dhs.gov. DHS I&A Regional Intelligence officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Dissemination	*(U)* Authorized audiences, such as private sector partners, federal officials, governors, lieutenant governors, secretaries of state, homeland security advisors, and fusion center directors and their staff.
Warning Notices & Handling Caveats	*(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

2019
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Combatting Targeted Disinformation Campaigns

A whole-of-society issue

October 2019

ACKNOWLEDGMENTS

We would first like to thank the Office of the Director of National Intelligence and the Department of Homeland Security for their thoughtful support throughout the duration of the program.

We are also very thankful for the unique insights we received from contacts and interviewees who contributed their time and information to this report by educating our group on the many aspects of how disinformation campaigns are conducted, the technologies involved, and the legal, regulatory, and policy landscape that affects how we confront this issue. The suggestions on further areas for exploration identified through our conversations have also helped considerably in the shaping of this paper, and where we would like our future research endeavors to go.

The people stepping up to help provide information for this project included private industry experts from technology and social media companies, university and think tank scholars and researchers, and state and federal agencies. We would like to acknowledge all the Team Members and Champion listed below for their contributions to this project and this report. This report would not have been possible without the diverse public and private sector makeup of this team and their legal, technical, academic, and policy expertise.

Team Members

Peter M.	FBI	Champion
Sam Alexander	Fannie Mae	Private Sector
Adam Cambridge	The MITRE Corporation	Private Sector
S. Renee Farner	National Oilwell Varco	Private Sector
Robert Kang	Booz Allen Hamilton	Private Sector
Stephanie Kiefer	NC4	Private Sector
Kawika Takayama	Proofpoint, Inc.	Private Sector
Christopher Vallandingham	University of Florida Levin College of Law	Private Sector
Laci F.	FBI	Government
Michael G.	FBI	Government
Katie M.	Northern California Regional Intelligence Center	Government

EXECUTIVE SUMMARY

In today's information environment, the way consumers view facts, define truth, and categorize various types of information does not adhere to traditional rules. The shift from print sources of information to online sources and the rise of social media have had a profound impact on how consumers access, process, and share information. These changes have made it easier for threat actors to spread disinformation and exploit the modern information environment, posing a significant threat to democratic societies. Accordingly, disinformation campaigns should be viewed as a whole-of-society problem requiring action by government stakeholders, commercial entities, media organizations, and other segments of civil society.

Outline

Executive Summary
Disinformation Overview
Information Environment
The Motives of Threat Actors
Disinformation Kill Chain
Combatting the Issue
Response Framework
Conclusion

Before the 2016 U.S. presidential election, disinformation was not at the forefront of American discourse. U.S. government efforts in the disinformation arena had focused primarily on combatting transnational terrorist organizations. Social media companies were just becoming aware how their platforms empowered threat actors on a large scale. Mainstream media organizations were not yet plagued by accusations of spreading "fake news" and fears of concerted foreign efforts to undermine American society had not seeped into the consciousness of the general public.

Since the presidential election, disinformation campaigns have been the subject of numerous investigations, research projects, policy forums, congressional hearings and news reports. The end result has been a better understanding of the methods and motives of threat actors engaging in disinformation campaigns and the impact of these campaigns, which in turn has led to improved efforts to combat these campaigns and minimize the harm they cause.

Until the end of 2018, much of the work on disinformation campaigns was post-mortem—after the campaign had nearly run its course. At that point, the desired effect of the threat actor had been achieved and the damage done. Since late 2018, civil society groups, scholars, and investigative journalists have made great strides in identifying ongoing disinformation campaigns and sharing findings with social media platforms, who then remove inauthentic accounts. However, these campaigns are often identified after the disinformation has already entered and been amplified inside the information environment, too late to fully negate the harm.

The extent of private and public sector cooperation over the next five years to address targeted disinformation campaigns will determine the direction of the issue. We view this issue as a whole-of-society problem requiring a whole-of-society response. The purpose of this paper is to provide a framework for stakeholders to understand the lifecycle of disinformation campaigns, then to recommend a preliminary set of actions that may assist with the identification and neutralization of a disinformation campaign before disinformation is amplified within the information environment, thus mitigating its impact.

The framework recommends actions for a variety of stakeholders to combat targeted disinformation campaigns by neutralizing threat actors, bolstering social media technology to make it less susceptible to exploitation, and building public resilience in the face of disinformation.

We recommend:

- Support for government legislation promoting transparency and authenticity of online political content. We support passage of the Honest Ads Act, which would hold digital political advertising to the same disclosure requirements as those required for political advertisements on television, radio and print media.
- Funding and support of research efforts that bridge the commercial and academic sectors. Academic research efforts, armed with the appropriate real-world data from commercial platforms, could more effectively explore the trends and methodologies of targeted disinformation campaigns. This research could also help to better identify segments of the population most susceptible to disinformation campaigns and guide resources for media literacy efforts. This research should also include the development of technical tools to analyze disinformation across platforms and identify inauthentic content such as deep fakes.
- Establishment of an information sharing and analysis organization to bring together government entities, research institutions and private-sector platforms. The organization could facilitate information exchange through a trusted third-party. The organization could serve as an information center that would pool expertise and track disinformation trends and methods.
- Encouragement of media organizations to promote the need for healthy skepticism by their users when consuming online content. This includes providing media literacy resources to users and enhancing the transparency of content distributors.
- Expansion of media literacy programs to build societal resilience in the face of disinformation campaigns. Media literacy could be framed as a patriotic choice in defense of democracy. Public education through advocacy groups like AARP, which can tailor the message of media literacy for their members, could be an effective means of encouraging the adoption of healthy skepticism towards online information.

Scope

This paper was produced by the Combatting Targeted Disinformation Campaigns team, operating under the auspices of the Department of Homeland Security's Analyst Exchange Program. The paper was developed based on open source research and interviews with identified subject matter experts. All judgments and assessments are based soley on unclassified sources and are the product of joint public and U.S. government efforts and do not necessarily represent the judgments and assessments of the team members' employers.

DISINFORMATION OVERVIEW

Disinformation is not synonymous with false information or "fake news." False information that is shared with others without the intent to mislead can be defined as misinformation. People share misinformation because they believe the information is true when, in fact, it is not.

On the other hand, the purpose of disinformation is to mislead. Disinformation is information created and distributed with the express purpose of causing harm.[1] Disinformation is not necessarily false information. Even true information can be presented in misleading ways and thus form the grist of a targeted disinformation campaign.

A targeted disinformation campaign, in the context of this paper, is more insidious than simply telling lies on the internet. One untrue meme or contrived story may be a single thread in a broader operation seeking to influence a target population through methods that violate democratic values, societal norms and, in some jurisdictions, the law.

A disinformation campaign occurs when a person, group of people, or entity (a "threat actor") coordinate to distribute false or misleading information while concealing the true objectives of the campaign. The objectives of disinformation campaigns can be broad (e.g., sowing discord in a population) or targeted (e.g., propagating a counternarrative to domestic protests) and may employ all information types (disinformation, misinformation, malinformation, propaganda, and true information). The target of a disinformation campaign is the person or group the threat actor aims to influence in order to achieve the campaign's objective.

Information Types

Propaganda has a political connotation and is often connected to information produced by governments (the lines between advertising, publicity, and propaganda are often unclear).

Disinformation is manufactured information that is deliberately created or disseminated with the intent to cause harm.

Misinformation is false information shared without the intent to mislead.

Malinformation is genuine information, typically private or revealing, that may be distributed in a campaign to cause harm to a person s reputation in furtherance of the campaign s objective.

Inauthentic Information is *not* transparent in its origins and affiliation. The source of the information tries to mask its origin and identity.

Authentic Information is transparent in its origins and affiliation. The source of the information is unhidden.

***Sources*:**

Claire Wardle, Information Disorder: The Essential Glossary, First Draft, Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School, July 2018, https://firstdraftnews.org/wp content/uploads/2018/07/infoDisorder_glossary.pdf?x 19860

Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East." FireEye Intelligence, August 21, 2018, https://www.fireeye.com/blog/threat research/2018/08/suspected iranian influence operation.html

Targeted disinformation campaigns are not a new phenomenon and sophisticated ones follow a predictable progression. After establishing the objective, a threat actor follows distinct steps, discussed later in more detail: recon, build, seed, copy, amplify, and control to bring about an outcome. But first we will explore the history and impacts of these campaigns, the information environment that facilitates modern campaigns, and the motives of disinformation threat actors.

[1] Claire Wardle, "Information Disorder: The Essential Glossary," First Draft. Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School, July 2018, https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x19860.

A Brief History of Influence Operations

To understand the role of disinformation in contemporary society, it is helpful to look at examples of how national governments, non-governmental organizations, and informal groups of individuals in modern history have used influence operations to sway public opinion both domestically and internationally. In international relations, the very essence of "soft power" is the ability to influence other nations through persuasion and other non-coercive means.

Within democratic societies, public support for policy and legislative initiatives is often critical for the success of these initiatives.[2] Eroding public support for U.S. involvement in the Vietnam War, not battlefield defeats, led to the eventual U.S. withdrawal from that conflict.[3] For decades, the U.S. Department of Agriculture promoted healthy eating habits through publication and distribution of nutrition guidelines.[4] In similar fashion, U.S. Surgeon General reports linking smoking and other tobacco use with cancer and other diseases, along with mandatory warning labels and limitations on advertisements for tobacco products, has helped lead to a precipitous decline in the U.S. smoking rate since the 1940s.

Nongovernmental organizations attempt to steer public opinion on a host of issues. Methods these organizations might use include editorials in newspapers, celebrity endorsements, chain e-mails, hosting public forums, publishing reports, organizing conferences, recording podcasts, and direct mail campaigns.

On the international front, within the U.S. Department of State, a core mission of the Bureau of Global Public Affairs is promotion of international support for the "values and policies of the United States."[5] Likewise, a core mission of the Peace Corps is "to help promote a better understanding of Americans on the part of the peoples served."[6]

Other countries, whether democratic or autocratic, also attempt to influence domestic and international audiences. Israeli Prime Minister Benjamin Netanyahu endeavored to undermine international support for the Iran nuclear deal.[7] China has attempted to polish its international reputation by spending vast sums of money worldwide to promote Chinese culture and allay the concerns of other countries uneasy about Chinese economic and military ambitions.[8] France has cultural centers in 137 countries to raise awareness of French culture.[9] And Russia has attempted to portray itself as a viable alternative to the West.[10]

Shaping public opinion through licit means is a legitimate function of government. However, there are many instances when governments have used illicit means to accomplish their objectives. During the First World War, false news stories about atrocities committed by the German Army served to demonize the

---

[2] Cheryl Boudreau and Scott A. Mackenzie, "Wanting What Is Fair: How Party Cues and Information about Income Inequality Affect Public Support for Taxes," *The Journal of Politics* 80, no. 2 (2018): 367–81, https://doi.org/10.1086/694784.
[3] W.L. Lunch and P. W. Sperlich, "American Public Opinion and the War in Vietnam," *Political Research Quarterly* 32, no. 1 (January 1979): 21–44, https://doi.org/10.1177/106591297903200104; William M. Darley, "War Policy, Public Support, and the Media," *The US Army War College Quarterly: Parameters*, 2005, 121–34, https://ssi.armywarcollege.edu/pubs/parameters/articles/05summer/darley.pdf.
[4] U.S. Department of Agriculture. "A Brief History of USDA Food Guides." Choose MyPlate, updated November 30, 2018, https://www.choosemyplate.gov/brief-history-usda-food-guides.
[5] U.S. Department of State, "Our Mission," Bureau of Global Public Affairs, accessed September 17, 2019, https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/bureau-of-global-public-affairs/.
[6] Peace Corps, "About Our Mission," accessed September 17, 2019, https://www.peacecorps.gov/about/.
[7] Katie Zezima. "Netanyahu Warns That Nuclear Deal 'Paves Iran's Path' to a Bomb." *Washington Post*, March 3, 2015, https://www.washingtonpost.com/news/post-politics/wp/2015/03/03/in-much-anticipated-speech-netanyahu-to-address-congress-tuesday/.
[8] "China Is Spending Billions to Make the World Love It," *The Economist*, March 23, 2017, https://www.economist.com/china/2017/03/23/china-is-spending-billions-to-make-the-world-love-it.
[9] Ministère de l'Europe et des Affaires étrangères, "France's Overseas Cultural Network," accessed September 17, 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/cultural-diplomacy/france-s-overseas-cultural-network/.
[10] Andrew Radin and Clint Reach, "Russian Views of the International Order," RAND Corporation, May 18, 2017, https://www.rand.org/pubs/research_reports/RR1826.html.

enemy in the eyes of the British public.[11] In the years leading up to the Second World War, a key objective of the Nazi propaganda machine was "to absorb the individual into a mass of like-minded people, and the purpose of the 'suggestion' was not to deceive but to articulate that which the crowd already believed."[12] Soviet disinformation campaigns, so-called "active measures," were central to the Soviet Union's efforts to increase its influence throughout the world and undermine the influence of its rivals.[13] Soviet efforts to control the press of foreign countries, forge documents, and manipulate other countries' societal infrastructure, including the academic, economic, and political spheres, were hallmarks of its organized disinformation efforts.[14] During the Cold War, the Soviet KGB and East German Stasi peddled the notion that the U.S. Department of Defense genetically engineered the human immunodeficiency virus (HIV).[15]

Impact of Disinformation Campaigns

The mere fact that domestic and foreign actors are engaging in disinformation campaigns against domestic audiences, especially during election cycles, is cause for concern irrespective of the success of these campaigns. Though it is often challenging to determine the full impact of disinformation campaigns, it is possible to identify, in some cases, short-term and long-term impacts. In the short term, targeted disinformation campaigns may:

- cause and exploit emotional reactions to sensational topics, causing disinformation to spread more rapidly than legitimate news.[16]
- aggravate existing societal fissures, inflaming ideological, political, gender-based, ethnic, and religious differences.[17] This heightened state of agitation may fuel acts of harassment and violence.[18]
- increase health risks. Disinformation campaigns aimed at health issues and the provision of health care may lead to sudden changes in dietary habits, the adoption of treatments which have not been scientifically verified, and engender distrust in the advice given by medical professionals.[19,20]

[11] Roy Greenslade, "First World War: How State and Press Kept Truth Off the Front Page," *The Guardian*, July 27, 2014, https://www.theguardian.com/media/2014/jul/27/first-world-war-state-press-reporting.
[12] Nicholas O'Shaughnessy, "The Nazis' Propaganda Trick: Invite the Public to Help Create an Alternate Reality," Slate, March 14, 2017, https://slate.com/news-and-politics/2017/03/how-nazi-propaganda-encouraged-the-masses-to-co-produce-a-false-reality.html.
[13] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference (Strategic Perspectives, No. 11)," *Strategic Perspectives*, June 2012, https://doi.org/10.21236/ada577586.
[14] U.S. Department of State, "Soviet 'Active Measures' Forgery, Disinformation, Political Operations (Special Reports No. 88)", October 1981, accessed September 17, 2019, https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf.
[15] Douglas Selvage and Christopher Nehring, "Operation 'Denver': KGB and Stasi Disinformation Regarding AIDS," Wilson Center, July 22, 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids.
[16] Katie Langin, "Fake News Spreads Faster than True News on Twitter—Thanks to People, Not Bots," *Science*, March 8, 2018, https://doi.org/10.1126/science.aat5350.
[17] Lisa Reppell and Erica Shein, "Disinformation Campaigns and Hate Speech: Exploring the Relationship and Programming Interventions," International Foundation for Electoral Systems, April 2019, https://www.ifes.org/sites/default/files/2019_ifes_disinformation_campaigns_and_hate_speech_briefing_paper.pdf.
[18] Paul Mozur, "A Genocide Incited on Facebook, With Posts From Myanmar's Military," *New York Times*, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.
[19] Marc Trotochaud and Matthew Watson, "Misinformation and Disinformation: An Increasingly Apparent Threat to Global Health Security," The Bifurcated Needle, Center for Health Security, John Hopkins University, November 29, 2018, http://www.bifurcatedneedle.com/new-blog/2018/11/29/misinformation-and-disinformation-an-increasingly-apparent-threat-to-global-health-security.
[20] Emma Woollacott, "The Viral Spread Of Ebola Rumors," *Forbes*, October 9, 2014, https://www.forbes.com/sites/emmawoollacott/2014/10/09/the-viral-spread-of-ebola-rumors/#191c27f219d8.

- harm the reputations of individuals, governments, companies, and other organizations, even if the disinformation is later proven false. [21]
- cause panic that reverberates through financial markets and leads individuals to make unsound financial decisions. [22]

The long-term effects of disinformation campaigns are potentially serious to democratic societies. While there is no sure-fire method to predict the outcomes of disinformation campaigns, based on the analysis of available literature and discussions with experts in the public and private sectors, there are a number of possible outcomes. In the long term, disinformation campaigns may:

- manipulate and further radicalize domestic audiences through impersonating and amplifying their existing messaging.[23]
- blur the lines between authentic and inauthentic content.[24] By mimicking legitimate sources of information, actors engaging in disinformation campaigns make it more difficult for individuals to distinguish truth from fiction.
- increase distrust of all online information sources.[25] Disinformation campaigns make individuals less apt to view online news sources as credible and fact-based, potentially harming democratic outcomes since exposure to a variety of reliable information sources helps to fuel rational, informed decision-making. Absent reliable sources of information, individuals are more likely to succumb to decision-making based on emotional appeal and personal whim.[26]
- undermine trust in democracy and confidence in the ability of government institutions to solve societal problems.[27]

INFORMATION ENVIRONMENT

The Social Media Revolution

As the invention of the movable type machine in the 15th century revolutionized the way the public received and shared information, so did the invention and widespread use of social media platforms in the 21st century. Social media platforms have granted individuals the ability to create communities with other individuals who have shared views and ideologies far more easily than was possible before the emergence of these platforms.

---

[21] Amanda Seitz, "NOT REAL NEWS: Anderson Cooper Didn't Fake Flood Broadcast," AP NEWS, September 18, 2018, https://www.apnews.com/f1b624dc8154458d8c193d3d6be341de; "2019 Brand Disinformation Impact Study," New Knowledge, January 2019, https://www.newknowledge.com/articles/2019-brand-disinformation-impact-study/.

[22] Max Fisher, "Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?," *Washington Post*, April 23, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/.

[23] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," Atlantic Council, June 13, 2019, https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/.

[24] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," Atlantic Council, June 13, 2019, https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/.

[25] Katherine Costello, "Russia's Use of Media and Information Operations in Turkey: Implications for the United States," RAND Corporation, August 28, 2018, https://www.rand.org/pubs/perspectives/PE278.html; Paul Butcher, "Disinformation and Democracy: The Home Front in the Information War," European Policy Centre, January 30, 2019, https://www.epc.eu/documents/uploads/pub_8984_disinformation.pdf?doc_id=2102.

[26] Paul Butcher, "Disinformation and Democracy: The Home Front in the Information War," European Policy Centre, January 30, 2019, https://www.epc.eu/documents/uploads/pub_8984_disinformation.pdf?doc_id=2102.

[27] W.L. Bennett and S. Livingston, "The disinformation order: Disruptive communication and the decline of democratic institutions," *European Journal of Communication*, 2018: 33(2), pp. 122-139.

This development has had far-reaching implications. For example, in the Arab world, online social networks fostered communities of individuals who shared grievances against their governments. This virtual collaboration led to plans to rise up against these governments. The ensuing uprisings resulted in a change of government in Tunisia, Libya, Egypt, Yemen, Sudan, Iraq, and political and economic concessions from the governments in Algeria, Oman, Bahrain, Morocco, and Saudi Arabia.[28] In a very real sense, without online social networks, the Arab Spring would not have occurred.

The development of mobile technologies with messaging platforms that are wifi-enabled and cellular-enabled has led to an explosion of interconnectivity. More than five billion people are estimated to own mobile devices and more than 50% of these devices are smartphones.[29] With these new technologies, individuals and groups can rapidly share content, including disinformation. This content includes messages from individuals or groups, hyperlinks to media articles, and other web content such as images and video. However, these messaging platforms may mask the identity of the sender and thus facilitate the spread of disinformation. Information shared via these messaging platforms is generally not vetted for accuracy, which makes these platforms prime candidates for exploitation by threat actors. Furthermore, end-to-end encryption on these messaging platforms can prevent the platform host from being able to moderate the content that flows through the platform.

For example, in 2017, the spread of false information led to acts of violence in India when false information about a purported gang of child kidnappers was disseminated on WhatsApp, a mobile messaging service used by over 200 million people in India.[30] Misinformation-fueled mobs killed seven people in the Indian state of Jharkhand.[31]

How Social Media Platforms Enable Disinformation Campaigns

Since the rise of social media, threat actors, whether individuals, nation-states, or other organized groups, have exploited the information environment on an unprecedented scale. Unlike the publication and distribution of print sources, which require publishing houses, editors, proofreaders, promotional advertisements, and bookstores, online information does not require an intermediary between content creator and consumer. As public confidence in mainstream media outlets has waned, interest in social media platforms and other online forums that offer uncensored communication channels to share ideas and commentary has increased. [32]

Though these platforms typically do not require payment from users in order to establish an account or access content on the platform, they are not cost-free. In exchange for granting users free access to these platforms, platform owners gather user data that enable advertisers to tailor online advertisements to known user preferences. In this arrangement, users are spared from content they have little interest in, platform owners can study user behavior to determine how to maximize the time users spend on the platform, and advertisers can serve up content more likely to engage users.

---

[28] Jean-Pierre Filiu. *The Arab Revolution: Ten Lessons from the Democratic Uprising*, (New York: Oxford University Press, 2011).

[29] "The Mobile Economy 2018," GSM Association, 2018, https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf.

[30] Kurt Wagner, "WhatsApp Is at Risk in India. So Are Free Speech and Encryption," Vox, February 19, 2019, http://www.vox.com/2019/2/19/18224084/india-intermediary-guidelines-laws-free-speech-encryption-whatsapp.

[31] Anant R. Zanane, "WhatsApp Rumours Led To Mob Killing Of 7 In Jharkhand, Say Police," NDTV.com, May 22, 2017, https://www.ndtv.com/india-news/whatsapp-rumours-led-to-mob-killing-of-7-in-jharkhands-singhbhum-district-say-police-1696551.

[32] "Indicators of News Media," Gallup, Inc., 2018, https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/216/original/KnightFoundation_Panel4_Trust_Indicators_FINAL.pdf.

The key to this system is the attention of users. The more alluring the content, the greater the time on the platform, and thus the greater the potential profit.[33] Therefore, social media platforms have an incentive to provide their users with an array of clickbait because doing so increases the revenue generated by selling online advertisements.[34]

By customizing user content, a platform effectively connects users with others who share similar views and interests. These platforms stoke the curiosity of users who want to discover what other users like them are wearing, watching, reading, and thinking.[35] The algorithms that determine what content will be displayed to individual users are designed to feed users more of what they *want* to know, not necessarily what they *should* know. The end result of this process is the creation of "echo chambers" where content inconsistent with a user's preferences fails to appear in his or her newsfeeds and other content-distribution channels.

The Pervasiveness of Russian Disinformation

This is why when we focus on social media effects of Russian disinfo, we completely miss the point. This is a multi dimensional, multi channel strategy, which uses different tools in complementary ways, and through which they have shaped U.S. political discourse...disinformation is often seeded at the bottom of the environment and trickles into more mainstream sites, but eventually it hits media and political influences. We cant measure the effects of disinfo through votes, but we can note where it becomes part of mainstream discourse.

Source: Kate Starbird (University of Washington), Twitter Post, July 9, 2019, 11:10 AM, https://twitter.com/katestarbird/status/1148610356895289346

For many people in the United States, social media platforms have become an important source of news. According to the Pew Research Center, in 2018, less than 38% of any segment of the U.S. population relied often on print newspapers.[36] Only 16% of Americans between the ages of 18 and 29 relied often on television news broadcasts; whereas 36% of this demographic group relied often on social media for news.[37] Overall, 68% of Americans get news on social media from time to time.[38] Forty-three percent (43%) of Americans get news on Facebook.[39]

The customization of content on social media platforms makes these platforms especially susceptible to disinformation campaigns.[40] Users can share information online easily and quickly, often doing so without verifying the accuracy of the shared information.[41] Although 79% of U.S. adults believe that steps should be taken to rein in fake news stories,[42] 23% have shared fake news, knowingly or unknowingly, with friends and other people online.[43] Because search algorithms provide results tied to prior online behavior, search

[33] Tim Hwang, "Digital Disinformation: A Primer," Atlantic Council, September 2017, https://www.atlanticcouncil.org/wp-content/uploads/2017/09/Digital_Disinformation_Primer_web_0925.pdf.

[34] Allcott Hunt and Matthew Gentzkow, "Social media and fake news in the 2016 election," *Journal of Economic Perspectives,* vol. 31, no. 2. 2017, pp. 1–28, https://web.stanford.edu/~gentzkow/research/fakenews.pdf.

[35] Lee Ross (professor of psychology, Stanford University), in discussion with the authors, June 27, 2019.

[36] Elisa Shearer, "Social Media Outpaces Print Newspapers in the U.S. as a News Source," Pew Research Center, December 10, 2018, https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/.

[37] Elisa Shearer, "Social Media Outpaces Print Newspapers in the U.S. as a News Source," Pew Research Center, December 10, 2018, https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/.

[38] "News Use Across Social Media Platforms 2018," Pew Research Center, September 12, 2018, https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/.

[39] A.W. Geiger, "Key Findings about the Online News Landscape in America," Pew Research Center, September 11, 2019, https://www.pewresearch.org/fact-tank/2019/09/11/key-findings-about-the-online-news-landscape-in-america/.

[40] Paul Oliver, "The State of Disinformation on Social Media," NYU Center for Data Science, April 23, 2018, https://medium.com/center-for-data-science/the-state-of-disinformation-on-social-media-397d3c30f56a.

[41] Mike Wood, "How Does Misinformation Spread Online?," *Psychology Today*, December 6, 2018, https://www.psychologytoday.com/us/blog/web-mistrust/201812/how-does-misinformation-spread-online.

[42] Galen Stocking, "Many Americans Say Made-Up News Is A Critical Problem That Needs to Be Fixed," Pew Research Center, 5 June 2019, https://www.journalism.org/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/.

[43] Denise-Marie Ordway, "Fake News and the Spread of Misinformation," Journalist's Resource, September 1, 2017, https://journalistsresource.org/studies/society/internet/fake-news-conspiracy-theories-journalism-research/.

returns will likely conform to users' preexisting biases. This content will seem more credible, at least initially, than content that flies in the face of these biases.[44] The desire of users to distinguish fake news from real news is often minimal when the news is emotionally compelling.[45] In the eyes of the user, the emotional appeal of the information may outweigh an interest in its trustworthiness.

As information is shared from user to user, the cumulative impact of this sharing may seem to render this information more legitimate due to the fact that so many users have shared it.[46] In other words, "if you make it trend, you make it true."[47] Popularity trumps accuracy.

Threat actors take advantage of the design of social media platforms and how users share information to target specific users and groups with disinformation in the hope that these users will spread this disinformation throughout the information environment. The easy transference of online information between users and platforms increases the effectiveness of modern disinformation campaigns.

During the 2016 U.S. presidential election campaign, the Internet Research Agency (IRA), based in Russia, created fake social media accounts by pretending to be U.S. citizens, operated fraudulent social media pages, and formed phony online groups all designed to attract U.S. audiences. On Twitter alone, the IRA created approximately 3,000 fake accounts that posted over 10 million tweets.[48] These accounts had over 6.4 million followers and followed 3.4 million other Twitter accounts.[49]

By capitalizing on divisive U.S. political and social issues and identifying U.S. audiences vulnerable to manipulation on social media, the IRA drew the attention of users with tantalizing content and was able to insert disinformation into the information environment where it spread rapidly and eventually metastasized to other social media platforms.[50] Mainstream news outlets, which monitored social media platforms for trending topics and reported on those topics, expanded the reach of this disinformation, highlighting how the ease of information transfer facilitates the effectiveness of modern disinformation campaigns.[51]

THE MOTIVES OF THREAT ACTORS

The sheer volume of information on the internet makes any attempt to rid the internet of inaccurate information, fake news, doctored audiovisual media, disinformation, or any other undesirable content a herculean, if not impossible, task. Therefore, government and industry leaders must focus their resources on identifying and neutralizing the greatest threats. One way to assess and prioritize threats is to identify suspected disinformation threat actors through understanding the motives for their campaigns.[52]

---

[44] Denise-Marie Ordway, "What Research Says about How Bad Information Spreads Online," Journalist's Resource, July 19, 2018, https://journalistsresource.org/studies/society/news-media/fake-news-bad-information-online-research/.

[45] Joe Andrews, "Fake News Is Real - A.I. Is Going to Make It Much Worse," CNBC, July 12, 2019, https://www.cnbc.com/2019/07/12/fake-news-is-real-ai-is-going-to-make-it-much-worse.html.

[46] Jon Hermann, "Defending America's National Security against Adversary ...," National Academies of Sciences, Engineering, and Medicine, accessed September 17, 2019, https://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_179824.pdf.

[47] Renée DiResta, "Computational Propaganda: If You Make It Trend, You Make It True," *The Yale Review*, October 12, 2018, https://yalereview.yale.edu/computational-propaganda.

[48] Gillian Cleary, "Twitterbots: Anatomy of a Propaganda Campaign," Symantec, June 5, 2019, https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation.

[49] Gillian Cleary, "Twitterbots: Anatomy of a Propaganda Campaign," Symantec, June 5, 2019, https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation.

[50] "Internet Research Agency Indictment," U.S. Department of Justice, February 16, 2018, https://www.justice.gov/file/1035477/download.

[51] Stephen Pritchard, "The Reader's Editor...reporting in haste," *The Guardian*, February 27, 2016, https://www.theguardian.com/media/2016/feb/28/the-readers-editor-on-reporting-in-haste; Casey Newton, "It's Time to End 'Trending' on Twitter," The Verge, August 13, 2019, https://www.theverge.com/interface/2019/8/13/20802974/twitter-trending-epstein-conspiracy-theories.

[52] Kaley Leetaru, "Stopping Disinformation Requires Measuring And Understanding It Not Just Monitoring And Debunking It," *Forbes*, April 27, 2019, https://www.forbes.com/sites/kalevleetaru/2019/04/27/stopping-disinformation-requires-measuring-and-understanding-it-not-just-monitoring-and-debunking-it/#57d3f1df5fd3.

Understanding why a piece of disinformation is directed at a specific audience will provide purchase on how to direct resources to negate the actor and mitigate the campaign.

Once one understands the motives of a threat actor, one may gain clarity on the objectives of specific disinformation campaigns, thus providing insight into how to neutralize the campaign and better predict the events and audiences who could be targeted in the future. The motives for disinformation campaigns are diverse and often mixed. Motivations can be financial (e.g., Macedonian threat actors' scheme to create ad revenue through incendiary content about a U.S. election[53]), political (e.g., push polling to plant false information in the minds of potential voters[54] or interest groups creating false social media content about an opponent to divide a voting bloc[55]), ideological (e.g., disagreement over a corporation's use of a social issue in its advertising, see Nike example below), legal/reputational (e.g., defense lawyers preventing reputational harm for a high-profile client and/or perpetrating harm against a defendant[56]), or a combination thereof.

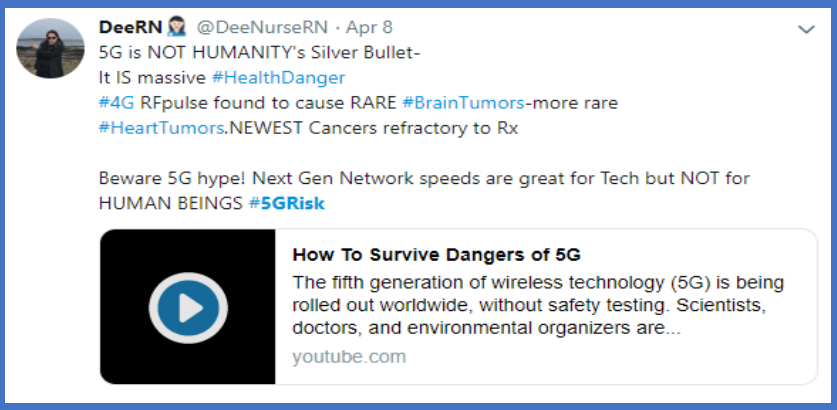
The following two pages offer case studies of disinformation threat actors motivated by different factors — the first, a nation-state motivated to slow the economic and technological progress of its adversaries (Russian Promotion of 5G Dangers); the second, ideologically-motivated actors conducting a low-budget campaign to tarnish a major corporation (Campaign to Damage Nike Brand).

[53] Samanth Subramanian, "Inside the Macedonian Fake-News Complex," *Wired*, February 15, 2017, https://www.wired.com/2017/02/veles-macedonia-fake-news/.
[54] Richard Gooding, "The Trashing of John McCain," *Vanity Fair*, September 24, 2008, https://www.vanityfair.com/news/2004/11/mccain200411; Jennifer Steinhauer, "Confronting Ghosts of 2000 in South Carolina," *New York Times*, October 19, 2007, https://www.nytimes.com/2007/10/19/us/politics/19mccain.html.
[55] Scott Shane and Alan Binder, "Democrats Faked Online Push to Outlaw Alcohol in Alabama Race," *New York Times*, January 7, 2019, https://www.nytimes.com/2019/01/07/us/politics/alabama-senate-facebook-roy-moore.html; Scott Shane and Alan Binder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *New York Times*, December 19, 2018, https://www.nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html?module=inline.
[56] Michael Barbaro, "Keeping Harvey Weinstein's Secrets, Part 1: Lisa Bloom," *New York Times*, podcast audio, September 18, 2019, https://www.nytimes.com/2019/09/18/podcasts/the-daily/harvey-weinstein-lisa-bloom.html.

RUSSIAN PROMOTION OF 5G DANGERS

Starting in 2018, Russia has supplied foreign audiences with disinformation about the supposed health dangers of 5G cellular signals. This disinformation campaign capitalizes on anxieties about radio waves causing cancer and other bodily damage.

Russia has used its RT America network to target Americans with a series of stories and news reports about the health hazards of 5G cellular signals. Inside Russia, RT reports on the scientific consensus that 5G signals promote human health; outside Russia, it reports that 5G cellular signals are more dangerous than existing 3G and 2G signals. By relying on a number of so called experts on the topic, Russia has promoted the notion that scientific controversy surrounds the issue, even though there is consensus in the scientific community that 5G signals are safe. The resulting public concern has possibly slowed the implementation of 5G technology in the West, stymied the business plans of Russia's economic competitors, and thus given Russian companies more time to establish their own 5G networks.



Sources:

William Broad, Your 5G Phone Won't Hurt You But Russia Wants You to Think Otherwise, *New York Times*, May 12, 2019, https://www.nytimes.com › science › 5g phone safety health russia/.

Aaron Pressman, Health Concerns May Slow Rollout of Super Fast 5G Mobile Networks, Analyst Warns," *Fortune*, May 22, 2019, https://fortune.com/2019/05/22/health concerns 5g cellphones cancer/.

Chris Zappone, Russian propaganda stoking 5G health fears in Australia, *Sydney Morning Herald*, September 16, 2019, https://www.smh.com.au/world/oceania/russian propaganda stoking 5g health fears in australia 20190916 p52rmc.html.

DeeRN, Twitter Post, April 8, 2019, 10:36 PM, https://twitter.com/DeeNurseRN/status/1115443371298967552.

CAMPAIGN TO DAMAGE NIKE BRAND

Right wing actors, unhappy about Nike's featuring of former NFL quarterback Colin Kaepernick in a 2018 advertising campaign, sought to discredit and undermine Nike's brand reputation. Kaepernick was controversial for his refusal to stand during pregame renditions of the national anthem in protest of what he saw as police brutality and systemic racism in America. After the Nike commercial aired, the disinformation threat actors created, posted, and spread fake Nike coupons featuring Kaepernick's picture and offering 75% discounts on Nike products for "people of color."

The threat actors weaponized an existing controversy to do economic harm to a corporation with whom they disagreed. They deliberately manufactured false information (the coupon) in a low budget operation to advance a narrative that Nike is overtly political, biased, and even un American. Therefore, consumers should avoid Nike products. Although the campaign, per se, may not have done lasting damage to Nike, it shows the susceptibility of public corporations to low budget actors who can create and advance false information about an existing controversy.

Sources:

A.J. Perez, Bogus Nike Coupon featuring Colin Kaepernick offers discount to people of color, *USA Today*, September 13, 2018, https://www.usatoday.com/story/sports/nfl/2018/09/13/fake nike colin kaepernick coupon offers discount people color/1294875002/.

Misinformation vs. Disinformation: What's the difference? New Knowledge, March 7, 2019, https://www.newknowledge.com/articles/misinformation vs disinformation whats the difference/.

Attribution

Ascertaining the intent of a threat actor can be difficult if the identity of the threat actor is not known.[57] Attributing a targeted disinformation campaign to a specific threat actor is often a painstaking process.[58] Developments in technology and tactics that help mask the identity of threat actors outpace developments in technology and tactics that unmask these threat actors, especially as threat actors become more adept at exploiting authentic users.[59] The process of assessing the threat actor can be facilitated by making three preliminary determinations: (1) Is the threat actor based inside or outside the United States?; (2) Is the threat actor a nation-state, backed by a nation-state, or independent of a nation-state?; and (3) Is the purveyor of disinformation a witting or unwitting agent?

Domestic or Foreign-Based: The physical location where the disinformation originated may offer some clues as to the motives of the threat actor. A targeted disinformation campaign that originates in Mississippi whose purpose is to enflame racial tensions in the United States will have different implications than an identical campaign that originates in Tehran. Fixing the location where the disinformation originated will also help to determine which responses to the disinformation are available and which entities are best suited to respond.

State or Non-State Affiliation: State-sponsored threat actors generally have more resources available to conduct disinformation campaigns than threat actors not backed by nation-states and therefore the resources to sustain and protect these campaigns over an extended period of time. Different tools are available to respond to the actions of nation-states, as opposed to the actions of non-state actors. The former is a matter of international relations and national security; the latter may be best addressed through the criminal justice system.

Witting or Unwitting Agents: Threat actors are witting purveyors of disinformation—people or entities directly supporting a disinformation campaign and aware of the campaign's malign motives. Threat actors should be distinguished from unwitting agents, people or entities supporting a disinformation campaign while unaware of the malign motives underlying the campaign. A "useful idiot" is a type of unwitting agent who is perceived to be sympathetic to the actor's cause, but does not comprehend the objectives of the campaign. Unwitting agents often spread disinformation not knowing that he or she is participating in a disinformation campaign. Responses to the different threat actors will vary depending on their level of intentional involvement in the targeted disinformation campaign.

The Role of Bots in Disinformation Campaigns

Threat actors can amplify disinformation through the use of bot networks, social media followers, or pre-established accounts. Bots are computer algorithms designed to execute specific online tasks autonomously and repetitively.[60] They simulate the behavior of human beings in social networks, interacting with other

[57] Alice Marwick and Rebecca Lewis, "Media Manipulation and Disinformation Online," Data & Society, May 15, 2017, https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.
[58] David E. Sanger, Jim Rutenberg, and Eric Lipton. "Tracing Guccifer 2.0's Many Tentacles in the 2016 Election." *New York Times*, July 15, 2018, https://www.nytimes.com/2018/07/15/us/politics/guccifer-russia-mueller.html.
[59] Elizabeth Bodine-Baron, Todd C Helmus, Todd C., Andrew Radin, and Elina Treyger, "Countering Russian Social Media Influence," RAND Corporation, 2018, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf.
[60] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019, https://www.cits.ucsb.edu/fake-news/spread.

users and sharing information and messages.[61] Millions of bots spread information on social media platforms such as Facebook, Twitter, and Instagram. According to a 2017 estimate, there were 23 million bots on Twitter (around 8.5% of all Twitter accounts), 140 million bots on Facebook (up to 5.5% of all Facebook accounts) and approximately 27 million bots on Instagram (8.2% of all Instagram accounts).[62] These three platforms alone contained 190 million bots—more than half the number of people who live in the entire United States.[63] These zombie-like accounts often sit dormant, waiting for external activation to begin their preassigned tasks on the platform. Bot accounts are advertised and sold legally on a number of websites. See the table below for an example of publicly available plans to purchase bots.

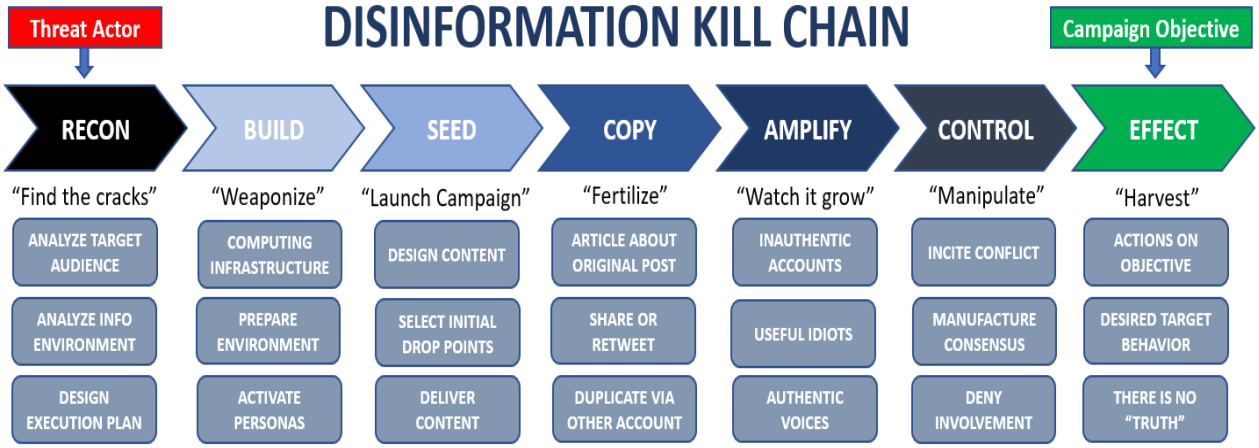
1000 Followers	2000 Followers	5000 Followers	10000 Followers
$12.94	$25.84	$58.26	$110.05
World-wide followers	World-wide followers	World-wide followers	World-wide followers
Less than 24 hours delivery	Less than 24 hours delivery	Less than 24 hours delivery	Less than 24 hours delivery
Bot Followers	**Bot Followers**	**Bot Followers**	**Bot Followers**
Secure Paypal payments	Secure Paypal payments	Secure Paypal payments	Secure Paypal payments
100% Money back guarantee	100% Money back guarantee	100% Money back guarantee	100% Money back guarantee
BUY NOW	BUY NOW	BUY NOW	BUY NOW

Source: "Fake Twitter Followers (Bots)," CompraSocialMedia.com, accessed September 19, 2019, https://www.compra-seguidores.com/en/buy-fake-followers/.

DISINFORMATION KILL CHAIN

The "connectedness" of modern society and the free availability of content distribution platforms has greatly increased the scope, scale, and speed of disinformation campaigns. Disinformation campaigns are not a new phenomenon. While the scale of attack, scope of impact, and speed of execution of modern disinformation campaigns have brought new attention to the issue, the fundamental elements of such campaigns pre-date the internet. The cyber kill chain model[64] serves as an inspiration for the following framework, which outlines the basic structure of these campaigns.

[61] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019, https://www.cits.ucsb.edu/fake-news/spread.
[62] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019. https://www.cits.ucsb.edu/fake-news/spread.
[63] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019. https://www.cits.ucsb.edu/fake-news/spread.
[64] *The Cyber Kill Chain*®, Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.



Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so can reduce the effectiveness of the campaign and erode protections aimed at obfuscating the identity and objectives of the actor.

Source: The MITRE Corporation

Campaign objective: A threat actor starts with an objective, such as changing a population's opinion on a topic (Brexit, war in Syria, Hong Kong protesters), steering voters toward a preferred candidate, or offering a counternarrative to the status quo.

1. Reconnaissance: Analyze target audience and how information flows through the target's environment, identify societal fissures to exploit, and design campaign execution plan.
2. Build: Build campaign infrastructure (computing resources, operational staff, initial accounts, personas, bots, and websites). Sophisticated threat actors may prepare the environment through tailored diplomatic, propaganda, and/or official messaging.
3. Seed: Create fake and/or misleading content, then launch campaign by delivering content to initial seeding locations such as online forums or social media platforms. Delivering content to multiple locations using different accounts can create the illusion that there are multiple sources for a story.
4. Copy: Write articles, blogs, and/or new social media posts referencing the original story. Witting agents can assist by using their media platforms for seemingly authentic distribution. The copy phase is a form of "information laundering," laying the groundwork for amplification by adding legitimacy to poorly sourced stories.
5. Amplify: Amplify content by pushing the story into the communication channels of the target audience. The use of bots and inauthentic accounts help provide momentum, then the content may be distributed by other witting agents (quasi-legitimate journalists) and unwitting agents (useful idiots). Successful amplification will result in the content being distributed by authentic voices, such as the mainstream media, which provides a trending effect and subsequent amplification by other unwitting agents and the target audience (i.e., now the unwitting audience is spreading misinformation because they do not know it is false and want to be helpful by informing their peers).
6. Control: Control the effect and manipulate the target's reaction by infiltrating conversations about the content. Incite conflict and/or strengthen the illusion of consensus by trolling comment sections of online posts. If a threat actor is accused of propagating disinformation, he or she may deny it vehemently, offer a counternarrative, and/or accuse an opposing party of planting the story.
7. Effect: Target actualizes the desired effect, such as voting for a preferred candidate, expressing behavior against a preferred group, or losing faith in the very idea of truth.

A threat actor may skip steps in this process, but doing so can reduce the effectiveness of the campaign and make it more difficult to mask the identity and objectives of the threat actor. Well-resourced threat actors may support and enable their campaigns through use of the entire influence toolkit, including economic and diplomatic activities, public relations, and espionage.

Case Studies

Below are two examples of disinformation campaigns executed by state-sponsored threat actors, which illustrate the phases of the disinformation kill chain.

In the first example, a fake story about the purported political assassination of Seth Rich, an employee of the Democratic National Committee (DNC), made its way from a Russian propaganda and conspiracy website, through Fox News, and into mainstream American discourse. It is important to note that Seth Rich's murder has remained unsolved, but no evidence has emerged which suggests that his death was a political assassination. The Rich family sued Fox News for "intentional infliction of emotional distress."[65] Fox News later retracted the article, saying "the article was not initially subjected to the high degree of editorial scrutiny we require for all our reporting."[66] Despite the retraction, high-profile Fox News personalities continued to discuss the conspiracy. After it trended, it was "true." Examples of content from the Seth Rich conspiracy are followed by an outline of the campaign (note the involvement of Russia's UK Embassy):

[65] Avie Schneider, "Appeals Court Reinstates Lawsuit Against Fox News Over Seth Rich Story," NPR, September 13, 2019, https://www.npr.org/2019/09/13/760681773/appeals-court-reinstates-lawsuit-against-fox-news-over-seth-rich-story.

[66] "Statement on coverage of Seth Rich murder investigation," Fox News, May 23, 2017, https://www.foxnews.com/politics/statement-on-coverage-of-seth-rich-murder-investigation.

Russian Embassy, UK ✓
@RussianEmbassy

Follow

#WikiLeaks informer Seth Rich murdered in US but 🇬🇧 MSM was so busy accusing Russian hackers to take notice.

4:13 AM - 19 May 2017

6,819 Retweets **7,703** Likes

Sean Hannity ✓
@seanhannity

Follow

Congress, investigate Seth Rich Murder! @JulianAssange made comments u need to listen to! If Seth was wiki source, no Trump/Russia collusion

> **Kim Dotcom** ✓ @KimDotcom
> Excellent and comprehensive reporting of FACTS. #SethRich
> twitter.com/cassandrarules...

2:42 PM - 21 May 2017

13,317 Retweets **21,045** Likes

WikiLeaks ✓
@wikileaks

Follow

ANNOUNCE: WikiLeaks has decided to issue a US$20k reward for information leading to conviction for the murder of DNC staffer Seth Rich.

5:58 AM - 9 Aug 2016

11,170 Retweets **11,372** Likes

CASE STUDY Seth Rich Murder (2016)		THREAT ACTOR Russian Foreign Intelligence Service (SVR)	
AFFILIATION	**TARGET AUDIENCE**	**OBJECTIVE**	**MOTIVE**
State-sponsored	US population	Counternarrative: Deflect special counsel investigation; if Seth Rich leaked the emails, then Russia wasn't involved with the DNC hack	Political
NARRATIVE	Seth Rich was a staffer for the Democratic National Committee; he leaked DNC emails to Wikileaks and planned to report wrongdoing by the Hillary Clinton campaign to the FBI; Clinton-affiliated assassins murdered him.		
PHASE	**PRIMARY PLATFORM**	**PHASE DESCRIPTION**	**AGENTS**
Seed	SVR bulletin; whatdoesitmean.com	SVR circulates ficticious intel report about the murder; citing "Russian intelligence," an article is published to an obscure website suggesting Rich was murdered by Clinton assassins; website is known source for Russian propaganda	threat actor
Copy	Reddit; alt-right sites; Twitter; RT; Sputnik	Rich conspiracy story posted on Reddit and Twitter	threat actor; witting agents; unwitting agents
Amplify	Twitter; Facebook; YouTube; Infowars; America First Media; Fox News	IRA bots repost story en masse; witting and unwitting agents retweet; alt-right websites aggressively push the story; Fox News picks it up and amplifies to mainstream US audiences	threat actor (bots); witting agents; unwitting agents
Control	Twitter comments; Fox News; YouTube; alt-right sites; RT; Sputnik	Bots & trolls infiltrate organic online conversations discussing the story to sow divisions; Julian Assange suggests Seth Rich was source for Wikileaks; Fox News continues to push the story; after Yahoo News report about SVR as source of conspiracy, a new disinformation effort begins to counter that narrative	threat actor (bots & trolls); witting agents; unwitting agents

Sources:

Michael Isikoff, "Exclusive: The true origins of the Seth Rich conspiracy theory. A Yahoo News Investigation," Yahoo News, July 9, 2019, https://news.yahoo.com/exclusive-the-true-origins-of-the-seth-rich-conspiracy-a-yahoo-news-investigation-100000831.html.

Charlie Mole, "Seth Rich: How a young man's murder attracted conspiracy theories," BBC News, April 21, 2018, https://www.bbc.com/news/blogs-trending-43727858.

The second example is the disinformation campaign launched against protestors in Hong Kong in 2019. Facebook and Twitter revealed that they had removed or suspended over 200,000 fraudulent accounts that were circulating information to discredit individuals and groups that had been protesting against the extradition bill pending in the Legislative Council of Hong Kong.[67] This campaign, sponsored by the Chinese government, sought to discredit the protestors and the larger pro-democracy movement in Hong Kong. The fraudulent accounts, some of which claimed to be users with American identities, pushed narratives praising the police and depicting the protestors in Hong Kong as cockroaches and terrorists.[68] The following are two disinformation items used in the campaign against the Hong Kong protests.

[67] Kari Paul, "Twitter and Facebook Crack down on Accounts Linked to Chinese Campaign against Hong Kong," *The Guardian*, August 19, 2019, https://www.theguardian.com/technology/2019/aug/19/twitter-china-hong-kong-accounts.
[68] Marie C. Baca and Tony Romm, "Twitter and Facebook Take First Actions against China for Using Fake Accounts to Sow Discord in Hong Kong," *Washington Post*, August 19, 2019, https://www.washingtonpost.com/technology/2019/08/19/twitter-suspends-accounts-it-accuses-china-coordinating-against-hong-kong-protesters/.

Source: Kate Conger, "Facebook and Twitter Say China Is Spreading Disinformation in Hong Kong," *New York Times*, August 19, 2019, https://www.nytimes.com/2019/08/19/technology/hong-kong-protests-china-disinformation-facebook-twitter.html.

CASE STUDY Hong Kong 2019 Protests		THREAT ACTOR Chinese Government	
AFFILIATION State-sponsored	**TARGET AUDIENCE** Worldwide Audience	**OBJECTIVE** Discredit the Pro-Democracy Movement	**MOTIVE** Political
NARRATIVE	Individuals protesting the previously proposed extradition bill in Hong Kong bill are not credible and destructive to China.		
PHASE	**PRIMARY PLATFORM**	**PHASE DESCRIPTION**	**AGENTS**
Seed	Facebook, Twitter	Set up fake profiles as Americans from Nevada, Ohio, and Texas with mainstream conservative views.	Chinese government; witting agents
Copy	Facebook, Twitter	Create approximately 20,000 additional accounts to propogate similar information across platforms	witting agents; unwitting agents
Amplify	Twitter, Facebook, including paid advertisements from Chinese state-run media (China Daily, Xinhua News, and CGTN)	Bots and other user accounts repost story en masse; witting and unwitting agents retweet	witting agents; unwitting agents
Control	Facebook, Twitter	In response to the campaign, Twitter and Facebook shut down thousands of accounts. Twitter closed nearly 1,000 active accounts that were part of the operation and roughly 200,000 it said amplified and supported the campaign. Facebook closed five accounts, seven pages and three groups on its platform. Facebook said that the pages it removed had about 15,500 accounts following one or more pages, while 2,200 accounts joined at least one of the groups.	Chinese government (bots & trolls); witting agents; unwitting agents

Sources: Marie C. Baca and Tony Romm, "Twitter and Facebook Take First Actions against China for Using Fake Accounts to Sow Discord in Hong Kong," *Washington Post*, August 19, 2019, https://www.washingtonpost.com/technology/2019/08/19/twitter-suspends-accounts-it-accuses-china-coordinating-against-hong-kong-protesters/.

Craig Timberg, Drew Harwell and Tony Romm, "In accusing China of disinformation, Twitter and Facebook take on a role they've long rejected," *Washington Post*, August 20, 201,. https://www.washingtonpost.com/technology/2019/08/20/after-twitter-facebook-blame-china-hong-kong-disinformation-government-defends-its-right-online-speech/?noredirect=o.

Louise Matsakis, "China Attacks Hong Kong Protesters with Fake Social Posts," *Wired*, August 19 2019, https://www.wired.com/story/china-twitter-facebook-hong-kong-protests-disinformation/.

COMBATTING THE ISSUE

The rapid pace of innovations on social media platforms, the shifting tastes of users who skip from one platform to another, and the immense array of content on social media, and comparable forums make it extremely challenging for government entities and platform owners to monitor and regulate inauthentic behavior. Since no government or platform owner has unlimited resources to devote to combatting disinformation campaigns, the amount of effort and resources required to keep pace with ongoing campaigns detracts from the capacity to develop strategies and technology that might prevent future disinformation campaigns or mitigate the damage these campaigns might cause. Before turning to a response framework to combat disinformation campaigns, we will review current efforts by some of the major stakeholders.

Social Media Platforms

While some major social media platforms have taken steps to limit disinformation on their platforms, these steps, in general, have been reactive in nature. The use of third-party fact checkers and the development of techniques to detect inauthentic accounts are examples of such steps.[69] During elections, Facebook has established "war rooms" to identify and respond to disinformation found on the platform.[70] Google has committed to sharing information concerning disinformation campaigns with law enforcement and other platforms when encountered.[71] However, these platforms are currently fighting a losing battle. As soon as one disinformation campaign is dismantled or inauthentic account deleted, another rears its ugly head, forcing the platforms to engage in a perpetual game of "whack-a-mole".

Social media platforms are also implementing more proactive measures to combat disinformation campaigns. Facebook and Instagram now permit organizations, which buy political ads or issue-oriented ads on these platforms, to run these ads only under the identities that the platform has first verified.[72]

Following the takedown of the Hong Kong protest disinformation campaign described above, Twitter updated its advertising policies whereby it "will not accept advertising from state-controlled news media entities. Any affected accounts will be free to continue to use Twitter to engage in public conversation, just not our advertising products."[73] Since social media platforms have a financial incentive to permit content that attracts user attention, whether factual or false, they are unlikely without external pressure to fundamentally adjust their business models.[74]

Government

In many respects, government entities have a far more powerful and extensive arsenal with which to combat targeted disinformation campaigns than social media companies. Governments can impose economic sanctions and civil fines, arrest and prosecute, limit international travel, seize websites, and withdraw tax-exempt status. Governments can also attempt to pressure social media companies to modify their practices by exposing these practices to public scrutiny.[75] However, constitutional and other legal guarantees of free speech constrain government efforts to regulate the content of online information.

The U.S. government's approach to combatting disinformation campaigns includes the establishment of special units whose focus is to counter foreign influence and share threat information with the private sector. Additionally, there is growing support for amending Section 230 of the Communications Decency Act, which could potentially make social media platforms civilly liable for content that users post on these platforms.

---

[69] "Working to Stop Misinformation and False News," Facebook, April 7, 2017, http://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news.
[70] Davey Alba, "Facebook Tightens Rules on Verifying Political Advertisers," *New York Times*, August 28, 2019, https://www.nytimes.com/2019/08/28/technology/facebook-election-advertising-disinformation.html.
[71] Salvador Rodriguez, "The FBI Visits Facebook to Talk about 2020 Election Security, with Google, Microsoft and Twitter Joining," CNBC, September 5, 201, https://www.cnbc.com/2019/09/04/facebook-twitter-google-are-meeting-with-us-officials-to-discuss-2020-election-security.html.
[72] Nancy Scola, "Facebook Revamps Election Ad Rules amid Disinformation Fears," POLITICO, August 28, 2019, https://www.politico.com/story/2019/08/28/facebook-election-ad-rules-disinformation-1476638.
[73] "Information Operations Directed at Hong Kong," Twitter, August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html; "Updating Our Advertising Policies on State Media," Twitter, August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/advertising_policies_on_state_media.html.
[74] Michael Posner, "How Social Media Companies Need To Address Disinformation Globally," *Forbes*, June 16, 2019, https://www.forbes.com/sites/michaelposner/2019/06/16/how-social-media-companies-need-to-address-disinformation-globally/#2d2e178e3f9f.
[75] Douglas Soule, "US Falls Behind EU in Responding to Disinformation Campaign," The Globe Post, August 3, 2019, https://theglobepost.com/2019/08/03/us-eu-disinformation-response/.

Citizenry

The brunt of the effort to combat disinformation campaigns ultimately falls on the users of social media platforms and other online forums. Without users willing to endorse and share disinformation, disinformation campaigns would be deprived of the fuel that powers them – "We have met the enemy and he is us."[76] Some researchers have likened the problem of making users less vulnerable to disinformation to inoculating a population against disease, suggesting that disinformation can infect a population similar to a virus.[77] Media literacy campaigns can be an effective means of inoculating users against the disease of disinformation. The U.S.-based National Association for Media Literacy Education defines media literacy as "the ability to access, analyze, evaluate, create, and act using all forms of communication…Media literacy empowers people to be critical thinkers, effective communicators, and active citizens."[78]

There are indications that the American public sense the need to become more media literate. Studies indicate that news consumers had difficulty distinguishing between real news and disinformation during the 2016 U.S. presidential election.[79] These consumers thought accuracy, impartiality, and transparency were the most important factors in trusting news sources, and they want news organizations to do a more thorough job of vetting information on their websites and to provide more ready access to fact-checking resources.[80]

RESPONSE FRAMEWORK

Mitigating the threat posed by sophisticated disinformation threat actors requires a whole-of-society response. Our recommendations revolve around three themes: hit the actor, hit the technology, and build public resilience. Fundamental to these themes is a culture of shared responsibility and a framework to share threat information across stakeholders in a way that protects the privacy of social media users.

Hit the Actor

<u>Government Stakeholders:</u>

- Move aggressively to collect information regarding the order of battle, objectives, tactics, techniques, and procedures of disinformation threat actors;
- Hold those actors accountable through a comprehensive approach involving diplomatic pressure, adversary engagement, criminal indictments, and daylighting their malign activities;
- Develop a prioritized list of events disinformation threat actors are likely to target (elections, political events, military exercises, census, etc.) and convene "war rooms" to bring together appropriate public and private sector stakeholders to combat disinformation in real time.

[76] Thomas Fingar (Shorenstein APARC Fellow in the Freeman Spogli Institute for International Studies, Stanford University), quoting the Pogo comic strip from 1971 in discussion with the authors, June 28, 2019.
[77] Jon Roozenbeek and Sander van der Linden, "The Fake News Game: Actively Inoculating Against the Risk of Misinformation," accessed September 17, 2019, https://www.cam.ac.uk/sites/www.cam.ac.uk/files/fakenews_latest_jrr_aaas.pdf.
[78] "Media Literacy Defined," National Association for Media Literacy Education, accessed September 17, 2019, https://namle.net/publications/media-literacy-definitions/.
[79] Darrell M. West, "How to Combat Fake News and Disinformation," Brookings, December 18, 2017, https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.
[80] "Indicators of News Media Trust," Knight Foundation, September 11, 2018, https://www.knightfoundation.org/reports/indicators-of-news-media-trust.

Social Media Platforms:

- Improve disinformation discovery tools and promptly take down the threat actor's infrastructure upon discovery;
- Share relevant signatures of disinformation campaigns with other platforms;
- De-emphasize content promulgated by overt authoritarian state-sponsored organizations. Further prohibit political advertisement by such organizations.

Academia and Civil Society Researchers: Continue investigating active disinformation campaigns across the information environment and analyze past campaigns to better understand the threat actors, their motives, and their techniques.

Hit the Technology

Government Stakeholders: Continue funding research for the development of technical tools to identify disinformation campaign signatures across platforms, including coordinated inauthentic behavior (e.g., creation of false personas, creation of fraudulent groups and websites, deployment of bots and trolls, and other suspicious account activity) and associated inauthentic content (e.g., fake or manipulated video, audio, images, text, and documents).

Industry and Academia: Design, build, and sell technical tools to identify and analyze disinformation campaigns across platforms.

Social Media Platforms: Employ technical tools to rapidly identify and analyze disinformation campaigns.

Build Resilience

Educational Institutions: Educational programs, from primary through graduate level, should integrate media literacy into their curricula. Increased media literacy across society would build resilience in the face of disinformation attacks, hardening the nation's defenses against both foreign and domestic disinformation actors. Media literacy and mature information consumption could be framed as a patriotic choice in defense of democracy.

Advocacy Groups: Advocacy and special interest groups (AARP, NAACP, Veterans of Foreign Wars, etc.) should promulgate media literacy information through their information distribution channels in a format tailored to their membership (e.g., The War on Pineapple).[81]

Government Stakeholders:

- *Transparency* – Legislation should emphasize the importance of content transparency and authenticity. Follow through on Honest Ads Act proposed in the U.S. Senate, which currently has bipartisan support. The act would amend the 1971 definition of "electioneering communication" to include internet-based political advertising, making internet-based ads subject to the same disclosure requirements as television, radio, and print media.
- *Literacy* – Fund research investigating the impact of disinformation campaigns across demographics and effective methods for providing media literacy education to those demographics.

[81] Department of Homeland Security, "The War on Pineapple: Understanding Foreign Interference in 5 Step," Cybersecurity and Infrastructure Security Agency, June 2019, https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf.

Academia and Civil Society Researchers:

- *Transparency* – Continue investigating the methods and technical means to provide transparency to the source of online content, such as a "nutrition label" for content providers (i.e. the Trust Project).[82]
- *Literacy* – Conduct media literacy research to identify trends in susceptibility to disinformation across demographics, the negative impact of disinformation campaigns, and approaches to providing media literacy education to susceptible populations.

Social Media Platforms:

- *Transparency* – Provide transparency regarding the geographic location of organizational page owners, history of name changes for the page, and apply "nutrition label" type information for organizational content providers.
- *Literacy* – Make readily available for users information about the platform's policies on disinformation and provide educational material about the judicious consumption of information online.

News Media Organizations:

- *Transparency* – Provide transparency regarding the source, author, and/or producer of news content, including their expertise, funding, conflicts of interest, and agenda. This information should be embedded with content and easily discoverable by consumers. News media organizations should strive to meet journalism standards of trustworthiness, such as citing sources, correcting mistakes, and avoiding conflicts of interest and political bias. Apply a news content "nutrition label" or Trust Mark[83] so consumers are aware of any explicit bias.

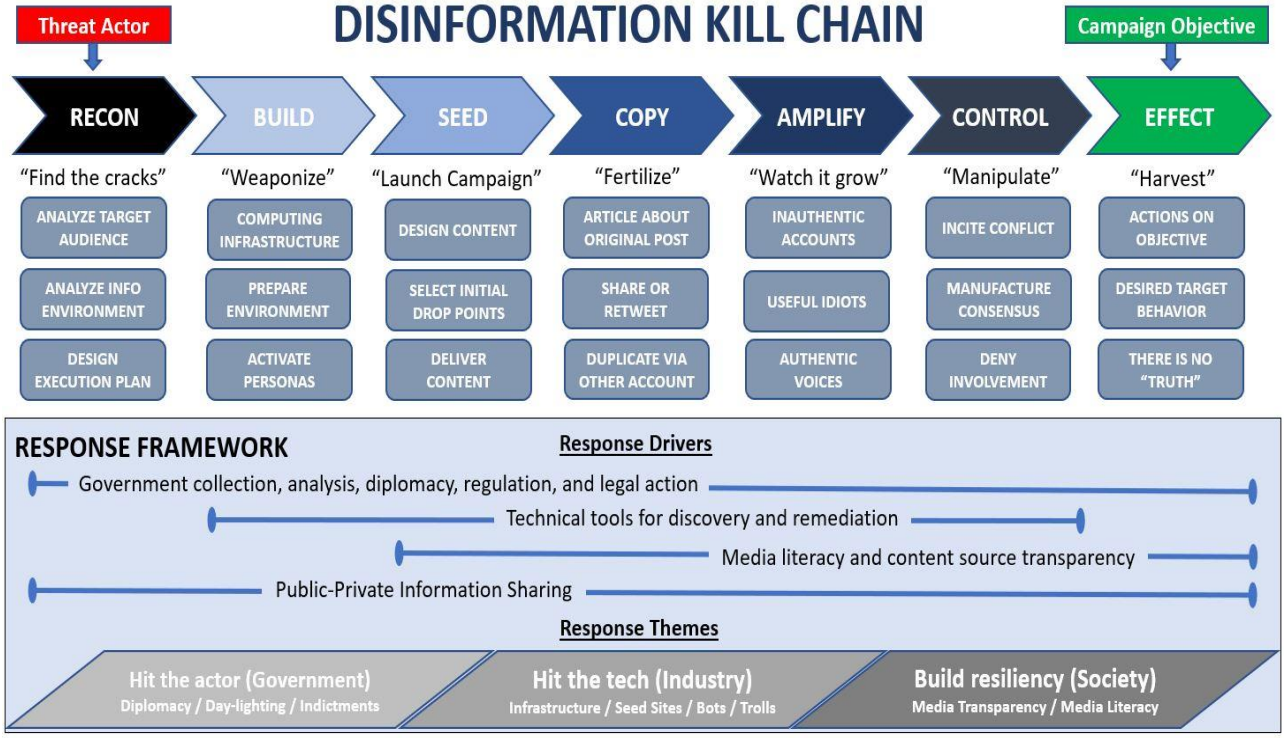
Information Sharing

An information sharing and analysis organization should be established with members from social media companies, research institutions, and news media organizations with the following objectives:

1. Establish a repository of social media data accessible to vetted researchers. Data stored and shared in a way that ensures user privacy (a trusted third party may act as gatekeeper);
2. Provide a framework for cross-platform analysis of disinformation campaigns to better understand threat actors, their tactics, and the impact of their activities;
3. Promote the advancement of methodologies, technical tools, and strategies for detecting disinformation, neutralizing threat actors, and reducing the negative impact of disinformation;
4. Facilitate information exchange between the federal government (appoint government lead responsible for disinformation issues) and social media companies;
5. Provide a process for sharing real-time threat information in a way that ensures user privacy.

[82] "What Is the Trust Project and What Does It Do?," The Trust Project, accessed September 17, 2019, https://thetrustproject.org/faq/#what_does_it_do.

[83] "What Is the 'Trust Mark'?," The Trust Project, accessed September 17, 2019, https://thetrustproject.org/faq/#trust_mark.



Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so can reduce the effectiveness of the campaign and erode protections aimed at obfuscating the identity and objectives of the actor.

Source: The MITRE Corporation

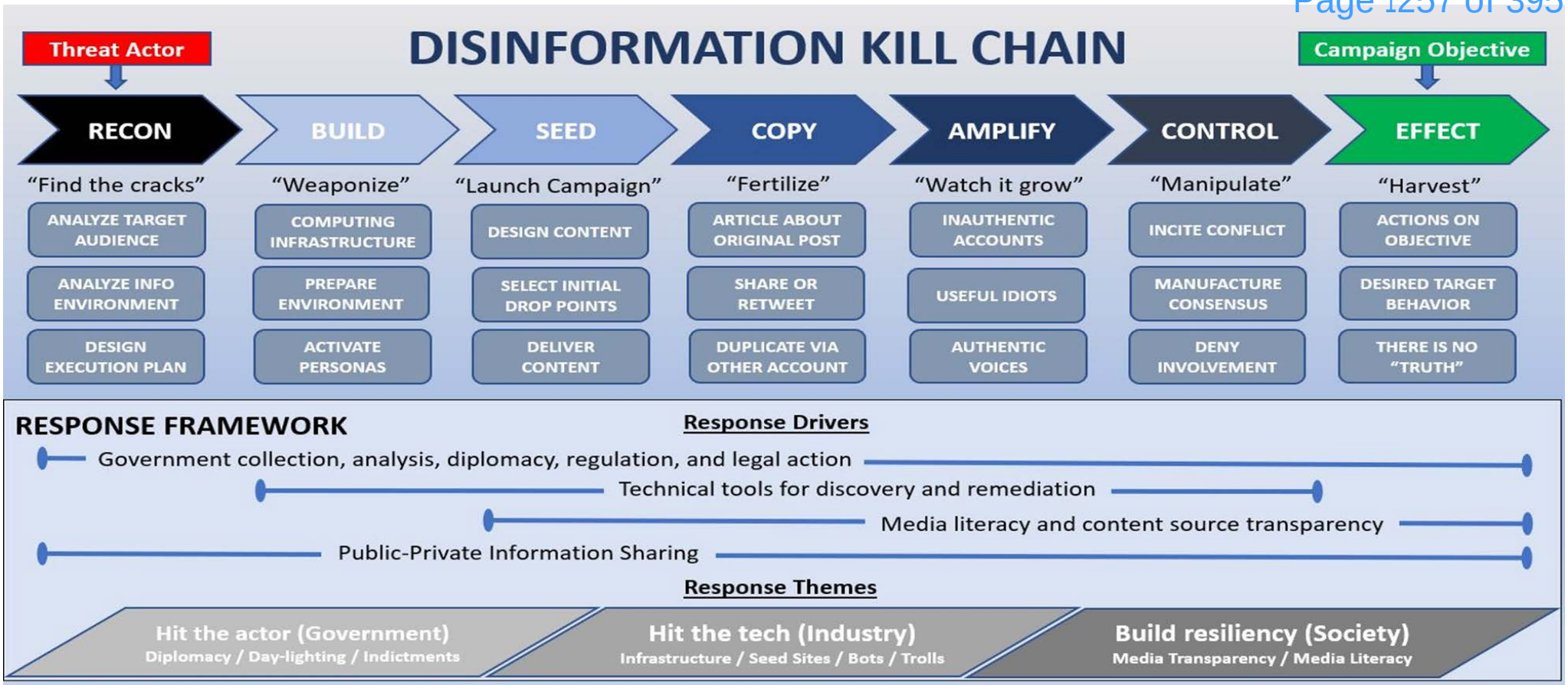
CONCLUSION

Since the events of the 2016 U.S. presidential election, the phenomenon of disinformation campaigns has received a great deal of attention, not just in the news media, but from government, academic, and commercial platforms determined to identify and understand it. While research efforts are plentiful, there is still much to learn about these campaigns and how best to defend against them. While it is not appropriate to dictate what media content Americans consume, we can, as researchers, suggest that opportunities for collaboration across interested sectors should continue to expand and to encourage public education to build resilience.

In a media environment where mere popularity, attention, and trending imbue truth and legitimacy, the internet can become a turbo-charged rumor mill with no editorial board. Disinformation can generate a lot of activity in a very short period of time, but whether this disinformation amounts to little more than noise in the system or represents a genuine threat is often not readily apparent. This paper emphasizes the importance of understanding targeted disinformation campaigns in the interest of hardening public defense against them. This includes understanding the threat actors who propagate these campaigns, how users are prone to them in a complex information environment and gaining the ability to identify these campaigns through their tell-tale signs.

Combatting disinformation campaigns by curtailing the free exchange of ideas could lead to a pyrrhic victory. Limits on free speech would further the objectives of threat actors seeking to weaken our democratic values. We must instead focus on building resilience, hitting the actor, and undermining their technical advantage. As these efforts mature, stakeholders can identify and counter campaigns "left of amplify," thus neutralizing the threat to democratic society and maintaining the integrity of our information environment.

Appendix: Disinformation Kill Chain



Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so can reduce the effectiveness of the campaign and erode protections aimed at obfuscating the identity and objectives of the actor.

Source: The MITRE Corporation

Information Types

Propaganda has a political connotation and is often connected to information produced by governments (the lines between advertising, publicity, and propaganda are often unclear).

Disinformation is manufactured information that is deliberately created or disseminated with the intent to cause harm.

Misinformation is false information shared without the intent to mislead.

Malinformation is genuine information, typically private or revealing, that may be distributed in a campaign to cause harm to a person's reputation to further the campaign s objective.

Inauthentic Information is *not* transparent in its origins and affiliation. The source of the information tries to mask its origin and identity.

Authentic Information is transparent in its origins and affiliation. The source of the information is unhidden.

Sources:

Claire Wardle, "Information Disorder: The Essential Glossary," *First Draft*, July 2018, https://firstdraftnews.org/wp content/uploads/2018/07/infoDisorder glossary.pdf?x19860
FireEye Intelligence, "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East," 21 August 2018, https://www.fireeye.com/blog/threat research/2018/08/suspected iranian influence operation.html

OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN VIEW

23 SEPTEMBER 2022

(U//FOUO) Online Foreign Influence Snapshot: August 2022

(U//FOUO) We judge that narratives driven by Chinese, Iranian, and Russian state media, and proxy websites linked to these governments, often involve fact-based articles as well as editorials; these publications may include misinformation, disinformation, or factual but misrepresented information. This monthly "Snapshot" compiles English-language narratives, which we assess are intended for US and Western audiences, and highlights both consistent trends and emergent messaging, which we assess to reveal foreign actors' changing influence priorities. We judge that, typically, China uses state and proxy media—including US-based outlets—to try to shape diaspora conduct and US public and leadership views; Iran state media manipulates emerging stories and emphasizes Tehran's strength while denigrating US society and policy; and Russia uses both state and proxy media to amplify narratives seeking to weaken Washington's global position relative to Moscow's. This snapshot identifies the most persistent or emergent narratives being spread by these actors for English-speaking—probably US—audiences, as well as narratives of interest to Homeland Security stakeholders.

OVERALL GRAPHIC CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

KEY TAKEAWAYS

CHINA

(U//FOUO) Chinese state media continued July's heavy shift to Taiwan issues—away from significant focus on Ukraine or COVID-19—while also claiming that several US domestic controversies show a failing democracy. Outlets denounced visits to Taiwan by US politicians as political grandstanding, and as attempts to undermine the One-China policy.

IRAN

(U//FOUO) Iranian state media focused on long-standing narratives. Outlets praised Tehran's purported efforts to revitalize the Joint Comprehensive Plan of Action (JCPOA), while criticizing Washington's negotiating stance, and pushed stories of US social discord, including inflation and the search of the former president's property.

RUSSIA

(U//FOUO) Russian state media and proxy websites continued their heavy focus on Ukraine by blaming global economic, energy, and food insecurity on the Western response. They also alleged that Ukrainian military actions endangered the Zaporozhye nuclear power plant. Moscow further highlighted its support for Beijing after the Taiwan visits of US Congressional delegations.

AUGUST CONSISTENT AND EMERGENT NARRATIVES

(U) US CONGRESSIONAL VISITS TO TAIWAN

(U) Chinese state media denounced the 2–3 August visit to Taiwan by the US Speaker of the House as a desperate act to boost Democrats' popularity and interfere with China's sovereignty; they also decried two later Congressional delegations as political showboating ahead of US midterm elections.[1–6]

(U) ONE-CHINA POLICY

(U) Chinese state media amplified narratives alleging US provocations in the Taiwan Strait, claiming that Washington is undermining the One-China principle, and denouncing US actions as hegemonic and designed to destabilize Indo-Pacific stability.[7,8,9]

(U) US DOMESTIC ISSUES

(U) Chinese state media amplified news stories involving contentious US domestic issues such as alleged abuses of immigrants, neglect of veterans, gun control, and crime rates. They characterized these issues as showing that US democracy and leaders are ineffective and that Washington is hypocritical in critiquing human rights abuses abroad.[10,11,12,13]

(U) JCPOA

(U) Iranian state media criticized the US position in JCPOA negotiations, asserting that Tehran has made reasonable demands and offered constructive solutions, while Washington was less committed to negotiating.[18,19,20]

(U) INFLATION

(U) Iranian state media amplified stories on contentious US domestic issues, particularly the US inflation rate, resulting sacrifices by US citizens, increasing political turmoil due to the economy, and growing disapproval ratings for the current US president.[21,22,23]

(U) MAR-A-LAGO SEARCH

(U) Iranian state media amplified reporting about the search of the former president's Mar-a-Lago Club[USPER], criticisms of the DOJ and FBI, and discord between Republicans and Democrats. Outlets also pushed stories about supporters of the former president who allegedly sent death threats to the US Attorney General and held armed protests by FBI buildings.[14,15,16,17]

(U) WAR IN UKRAINE

(U) Russian state media and proxies alleged Ukrainian military atrocities, and blamed Western support to Ukraine for price and energy inflation, and food insecurity.[24,25,26,27]

(U) ZAPROZHYE NUCLEAR POWER PLANT

(U) Russian state media and proxies amplified allegations that the Ukrainian military shelled the Russia-held nuclear plant in Zaporozhye, Ukraine, blaming Kyiv for any potential nuclear disaster.[28,29,30]

(U) US CONGRESSIONAL VISITS TO TAIWAN

(U) Russian state media and proxies focused on the visits to Taiwan by the US Speaker of the House and later congressional delegations, while promoting Russia's alliance with China as a sign of falling US global influence.[31,32]

Source, Reference, and Dissemination Information	
Prepared By	(U) Cyber Mission Center
For Questions, Contact	(U) DHS-SPS-RFI@hq.dhs.gov
Privacy, Civil Rights, Civil Liberties, Intelligence Oversight Notice	(U//FOUO) US persons linking, citing, quoting, or voicing the same arguments raised by these foreign influence activities likely are engaging in First Amendment-protected activity, unless they are acting at the direction or control of a foreign threat actor. Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect foreign influence or malign activity absent information specifically attributing the content to malign foreign actors. This information should be considered in the context of all applicable legal and policy authorities to use open source information while protecting privacy, civil rights, and civil liberties.
Definitions	(U//FOUO) **Foreign Influence:** Any covert, fraudulent, deceptive, or unlawful activity of foreign governments—or persons acting on their behalf—undertaken with the purpose or effect of influencing, undermining confidence in, or adversely affecting US democratic processes or institutions or otherwise affecting socio-political sentiment or public discourse to achieve malign objectives. • (U//FOUO) **Covert Influence:** Activities in which a foreign government hides its involvement, including the use of agents of influence, covert media relationships, cyber influence activities, front organizations, organized crime groups, or clandestine funds for political action. • (U//FOUO) **Overt Influence:** Activities that a foreign government conducts openly or has clear ties to, including the use of strategic communications, public diplomacy, financial support, and some forms of propaganda. (U//FOUO) **Disinformation:** A foreign government's deliberate use of false or misleading information intentionally directed at another government's decisionmakers and decision-making processes to mislead the target, force it to waste resources, or influence a decision in favor of a foreign government's interests. (U//FOUO) **Malinformation:** An adversary's deliberate use of otherwise verifiable information with malicious intent, such as by amplifying the information selectively or out of context, or to the detriment of specific persons. (U//FOUO) **Misinformation:** An adversary's use of false or misleading information. An adversary's intent can change misinformation to disinformation.
Malign Foreign Influence Collection and Analysis Methodology	(U//FOUO) The Office of Intelligence and Analysis (I&A) collects and receives reporting on messaging from foreign governments or any entity assessed to be operating on behalf of a foreign power, including reporting on covert, fraudulent, deceptive, and unlawful activities undertaken with the purpose or effect of influencing, undermining confidence in, or adversely affecting our democratic processes or institutions or otherwise affecting socio-political sentiment or public discourse to achieve malign objectives. (U//FOUO) This reporting includes state-controlled media outlets—some that are officially registered under the Foreign Agents Registration Act—as well as covert proxy websites and social media accounts we assess are operated by foreign governments or entities operating on behalf of a foreign power. (U//FOUO) I&A routinely reviews the totality of this malign foreign influence content and, in the case of this report, identified a number of prominent COVID-19, domestic,

	and socio-political themes regularly presented by these actors since the beginning of 2020.
Dissemination	*(U//FOUO)* Federal, state, local, and private sector stakeholders.
Warning Notices & Handling Caveats	*(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. *(U)* **Warning:** This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. Should you require the minimized US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@hq.dhs.gov. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.

Discovering Deception in Online Cybersecurity Discourse:

Using Social Media to Enable Effective Insider Risk Management

Mr. Luke Osterritter

losterritter@sei.cmu.edu

Page 1261 of 3957

The views expressed are those of the author and do not reflect the official policy or position of the Office of the Director of National Intelligence, the Department of Defense, or the US Government.

Document Markings

Copyright 2022 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM22-0551

[Distribution Statement A] Approved for public release and unlimited distribution.

Who We Are

Carnegie Mellon University
Software Engineering Institute

Carnegie Mellon University

- Pioneering discoveries that enrich the lives of people on a global scale
- Turning disruptive ideas into success through leading-edge research

Software Engineering Institute

- Bringing innovation to the U.S. government
- Researching software engineering, cybersecurity, and artificial intelligence

CERT Division

- Giving birth to modern cybersecurity
- Strengthening the resilience of systems and networks

[Distribution Statement A] Approved for public release and unlimited distribution.
Page 1263 of 3957

Why is disinformation an insider risk problem?

- **BLUF** – adversaries can exploit and recruit insiders by way of mis-, dis-, and malinformation

One possible example:

- Theory of psychological **reactance** - "an unpleasant motivational arousal that emerges when people experience a threat to or loss of their free behaviors. It serves as a motivator to restore one's freedom." (Steindl et al. 2015)
- Individuals experiencing reactance as a result of actions or perceived actions of an organization may engage in organizational deviance.
- Such individuals may now be susceptible to **influence** from **adversarial entities** seeking to harm the organizations that the individual is a member of.

- Possible triggers
  - Office requirement
  - Vaccination reqs.
  - Extremists ideologies

Page 1264 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

From Insider Threat to Insider Risk

[Distribution Statement A] Approved for public release and unlimited distribution.

What is an “Insider Threat”?

- Malicious Insider
  - a current or former employee, contractor, or business partner who meets the following criteria:
    - has or had authorized access to an organization’s network, system, or data
    - has intentionally exceeded or intentionally used that access in a manner that negatively affected the **confidentiality, integrity,** or **availability** of the organization’s information or information systems
- Can also be inadvertent (non-malicious)

Page 1266 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

From Insider Threat to Insider Risk

- **Insider Threat**: Insider threat for an organization is the potential for an insider to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

- **Insider Risk:** Insider risk is the potential for loss associated with the realization of an insider threat.

As a discipline, we are moving away from a purely threat hunting mindset to one of risk management.

Page 1267 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Insider Risk and External Threat

- Insider risk is unique in organizational security in that the potential threat agents play **fundamental roles** in accomplishing the organization's mission.

- Insider goodwill is **essential** to both keeping intentional insider risk to a minimum and ensuring organizational success generally.

- External adversaries can potentially use mis- dis- and malinformation with coordinated **information maneuver campaigns** to target trusted insider.

Page 1268 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Mis- Dis- and Malinformation

[Distribution Statement A] Approved for public release and unlimited distribution.

Page 1269 of 3957

What does “disinformation” mean?

Page 1270 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Untangling the Terms

DISINFORMATION

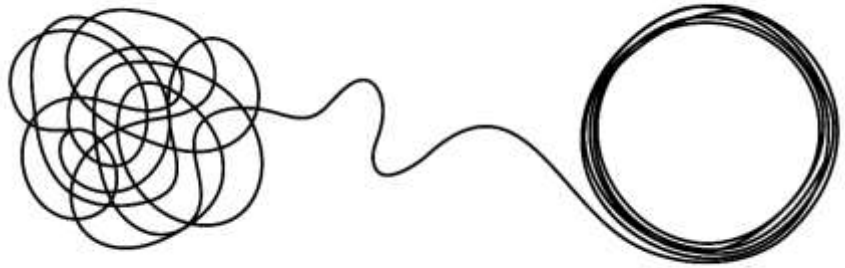
Information that is false and spread specifically by those who DO know it's not true.

MISINFORMATION

Information that is false but spread by those who DON'T know it's not true.

MALINFORMATION

Information that is based on fact but is spread – out of context – by people intending to mislead or cause harm.



Source: IDeaS Center, CMU

[Distribution Statement A] Approved for public release and unlimited distribution.

Page 1271 of 3957

Why are disinformation, misinformation, and malinformation spread?

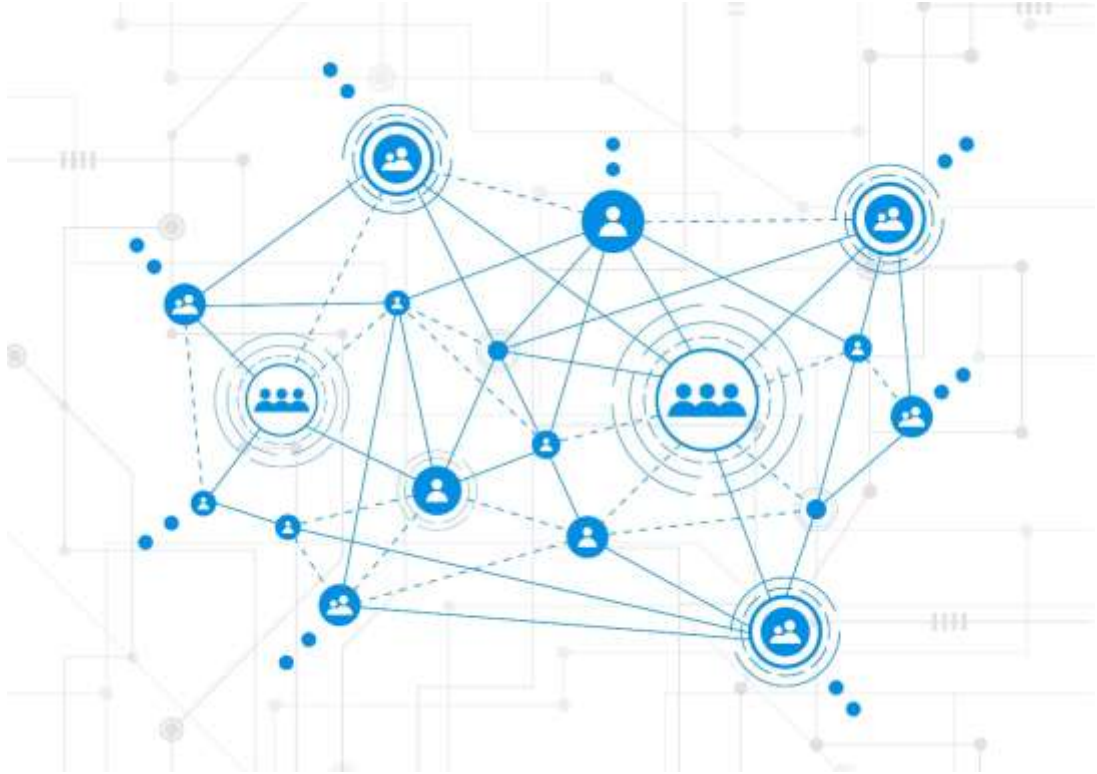
- Money
- Boredom
- Politics
- Disrupt society
- Reduce the voice of marginalized groups
- Building community

Source:
IDeaS Center, CMU

[Distribution Statement A] Approved for public release and unlimited distribution.
Page 1272 of 3957

How does disinformation, misinformation, and malinformation spread?

- Bots
- Trolls
- Bogus news outlets
  - “Pink slime”
- Your family
- Your friends
- Me
- You!



Source:
IDeaS Center, CMU

[Distribution Statement A] Approved for public release and unlimited distribution.
Page 1273 of 3957

Cybersecurity and Social Cybersecurity

- A scientific discipline to help us recognize and understand what's happening to us online and be able to see it coming

- Figuring out how to build policy and tech that protects society from social cyber threats

- **CYBERSECURITY**
  - Hacking machines
  - Harming confidentiality
  - Compromising data integrity and availability

- **SOCIAL CYBERSECURITY**
  - Hacking people
  - Capturing hearts and minds

Source: IDeaS Center, CMU

[Distribution Statement A] Approved for public release and unlimited distribution.
Page 1274 of 3957

Conversations around Insider Threat in Public Forums

[Distribution Statement A] Approved for public release and unlimited distribution.

Page 1275 of 3957

Conversations around Insider Threat

- Why look at public conversation? Unlikely to find any insider threats…
- …but, there may be actors trying to shape the conversation to their own ends – corporations, nation-states, etc.
- Understanding the conversation will lead to informed research
  - Wisdom of the crowd
  - Data for computational modeling
- **Research question**: Can network analytical techniques be used to discover the nature of public conversations around insider threat and related organizational threats?
  - Gain **situational awareness** around public discourse

Source:
IDeaS Center, CMU

[Distribution Statement A] Approved for public release and unlimited distribution.
Page 1276 of 3957

Collection Methods

- Use Python package twarc to retrieve tweets from Twitter Search API V1 based on hashtag query
- Tweets collected between March 27th and April 15th 2020 (there are gaps)
- Import Twitter JSON data into ORA-PRO
  - ORA-PRO handles creating derived networks and basic stats.
- Reporting and network visualizations

Source:
IDeaS Center, CMU

Page 1277 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Hashtag Collection

Category	Hashtags			
General	#insiderthreat	#insiderattack	#cyberespionage	#dataloss
Corporate	#industrialespionage	#tradesecrets	#embezzlement	#embezzling
Nation-state	#militarysecrets	#spy	#spying	#spies

Source:
IDeaS Center, CMU

[Distribution Statement A] Approved for public release and unlimited distribution.
Page 1278 of 3957

Data Description

Network	Twitter JSON All Hashtags
First tweet date	2013-01-15 07:06:07-05
Last tweet date	2020-04-15 08:45:03-04
Number of tweets	13640
Number of tweets with geotag	9
Number of tweets with URL	4939
Number of retweets	5826
Number of tweeters	6260
Number of verified tweeters	145
Number of news agency tweeters	17
Number of mentions	4233
Number of distinct hashtags	6795
Number of distinct hashtags used more than once	3212
Number of distinct words	0
Number of distinct words used more than once	0
Number of distinct locations	9

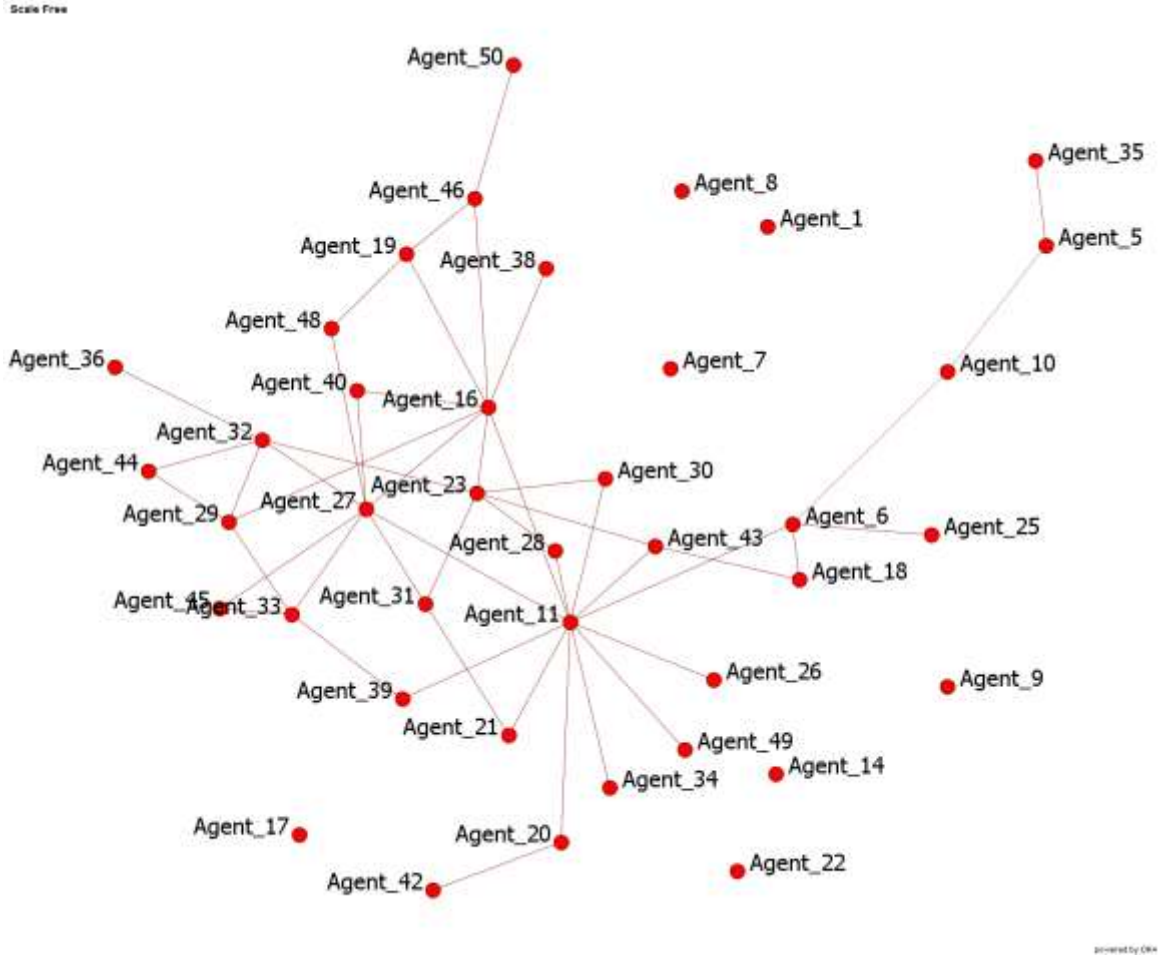
Source:
IDeaS Center, CMU

Page 1279 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Understanding Networks

- Node – red circles
- Links (Edges) – lines between nodes
- Unidirectional or bidirectional (asymmetric)

- Can be multi-modal (different types of nodes)
- Or multi-plex (different types of links)

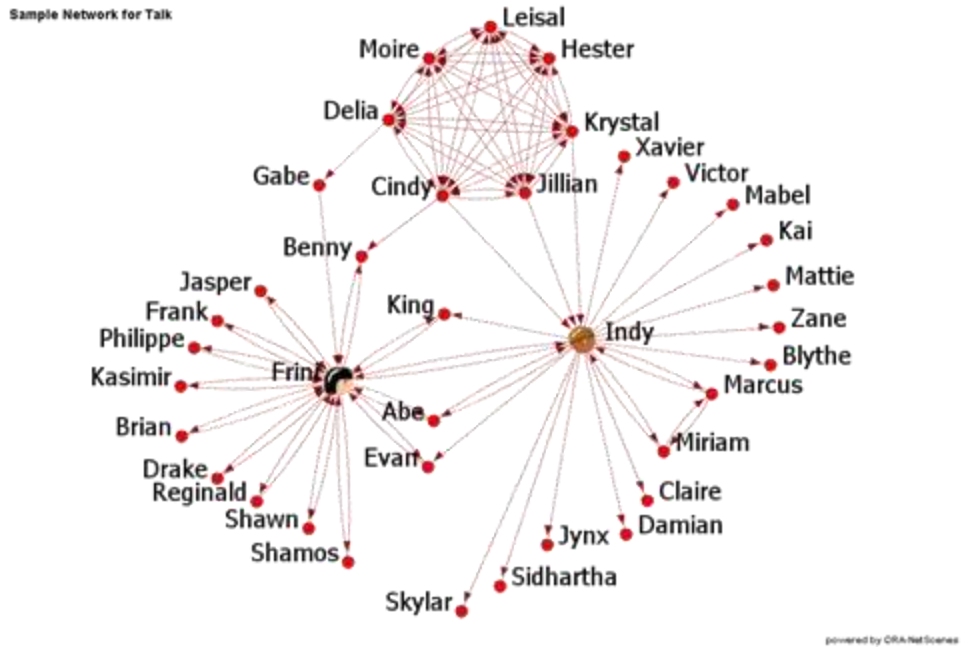


Source: IDeaS Center, CMU

[Distribution Statement A] Approved for public release and unlimited distribution.
Page 1280 of 3957

Key Network Terms – Finding Actors of Interest

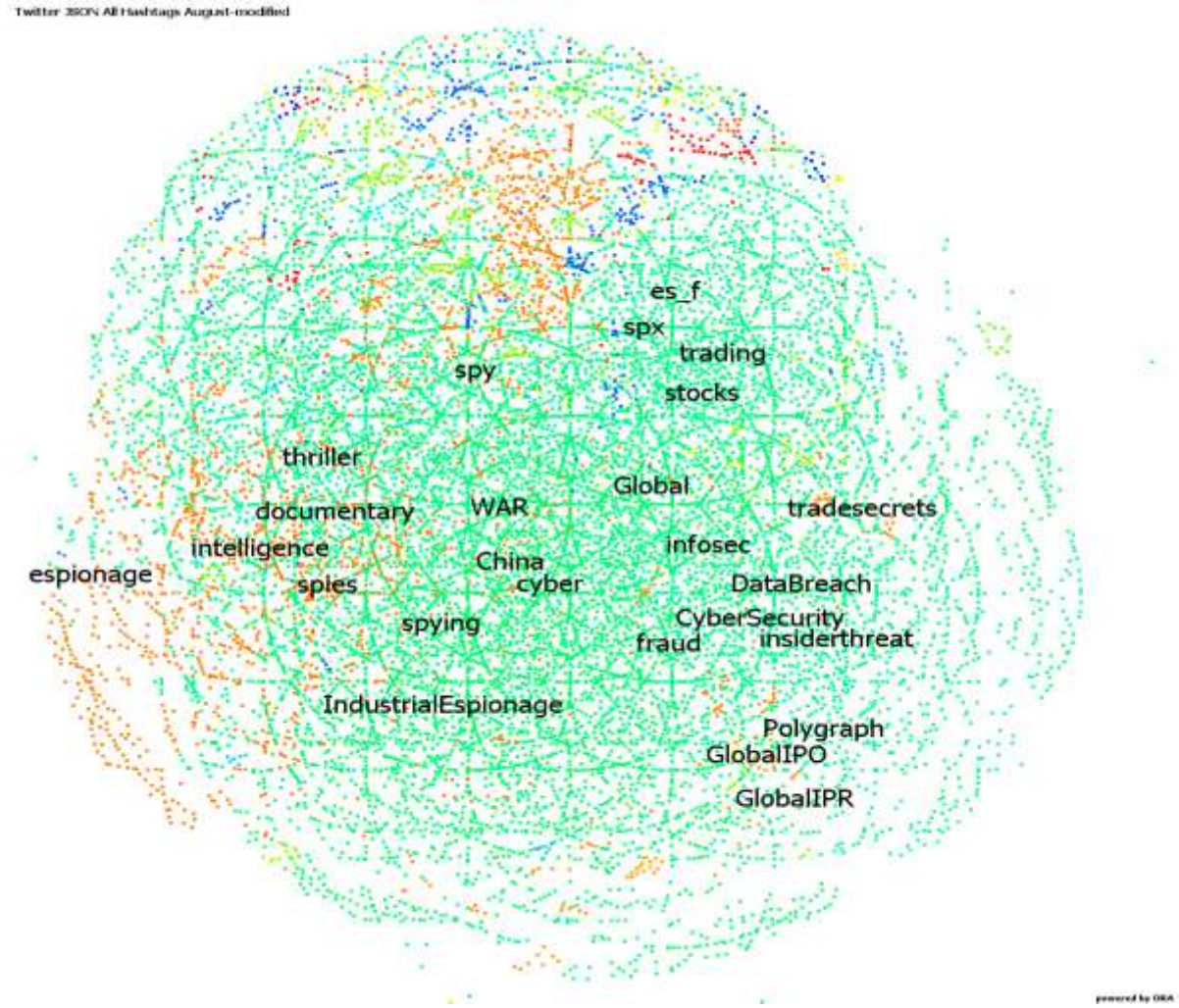
- Super-spreader
  - A communicator who has **exceptional ability to spread** information
- Super-friends
  - A communicator who is exceptionally involved in dialogue with others (**reciprocal communication**)
- Echo Chamber
  - A group of users and topics that are **strongly interconnected** at both the social and the knowledge level



Source: IDeaS Center, CMU

[Distribution Statement A] Approved for public release and unlimited distribution.
Page 1281 of 3957

Top Hashtag Visualization

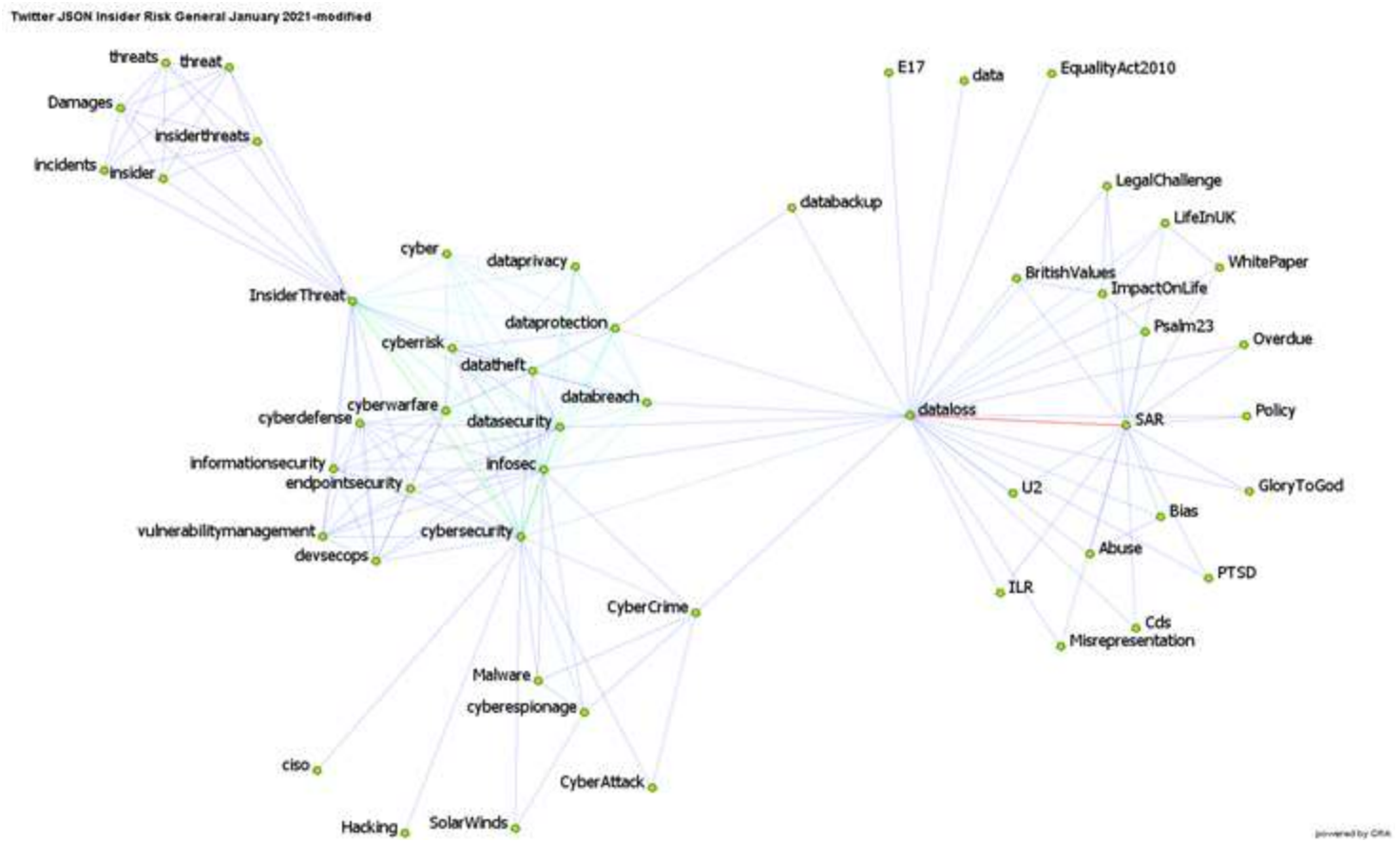


Source: IDeaS Center, CMU

[Distribution Statement A] Approved for public release and unlimited distribution.

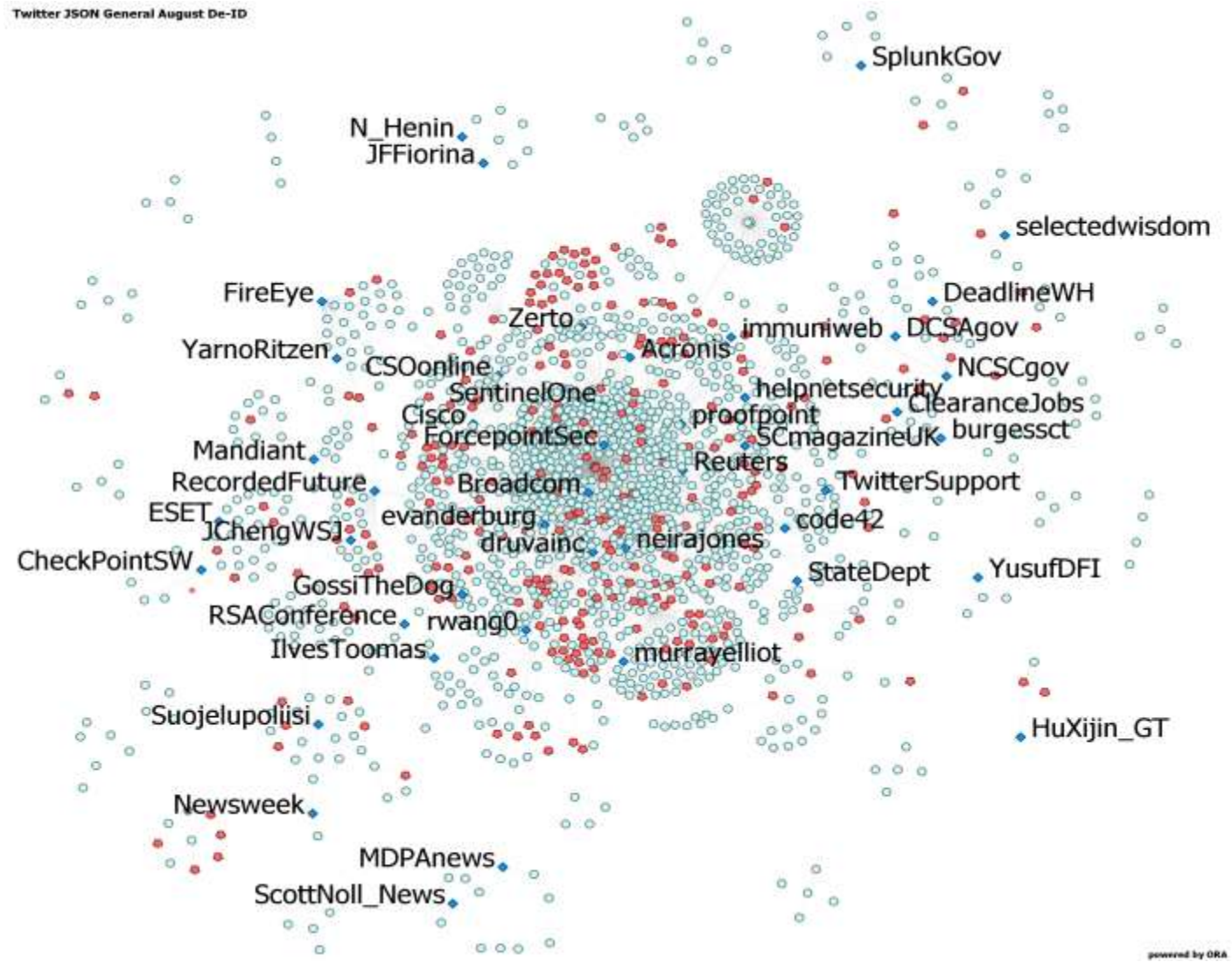
Page 1282 of 3957

Hashtag Co-occurrence Network (General grouping)



Source:
IDeaS Center, CMU

Page 1283 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

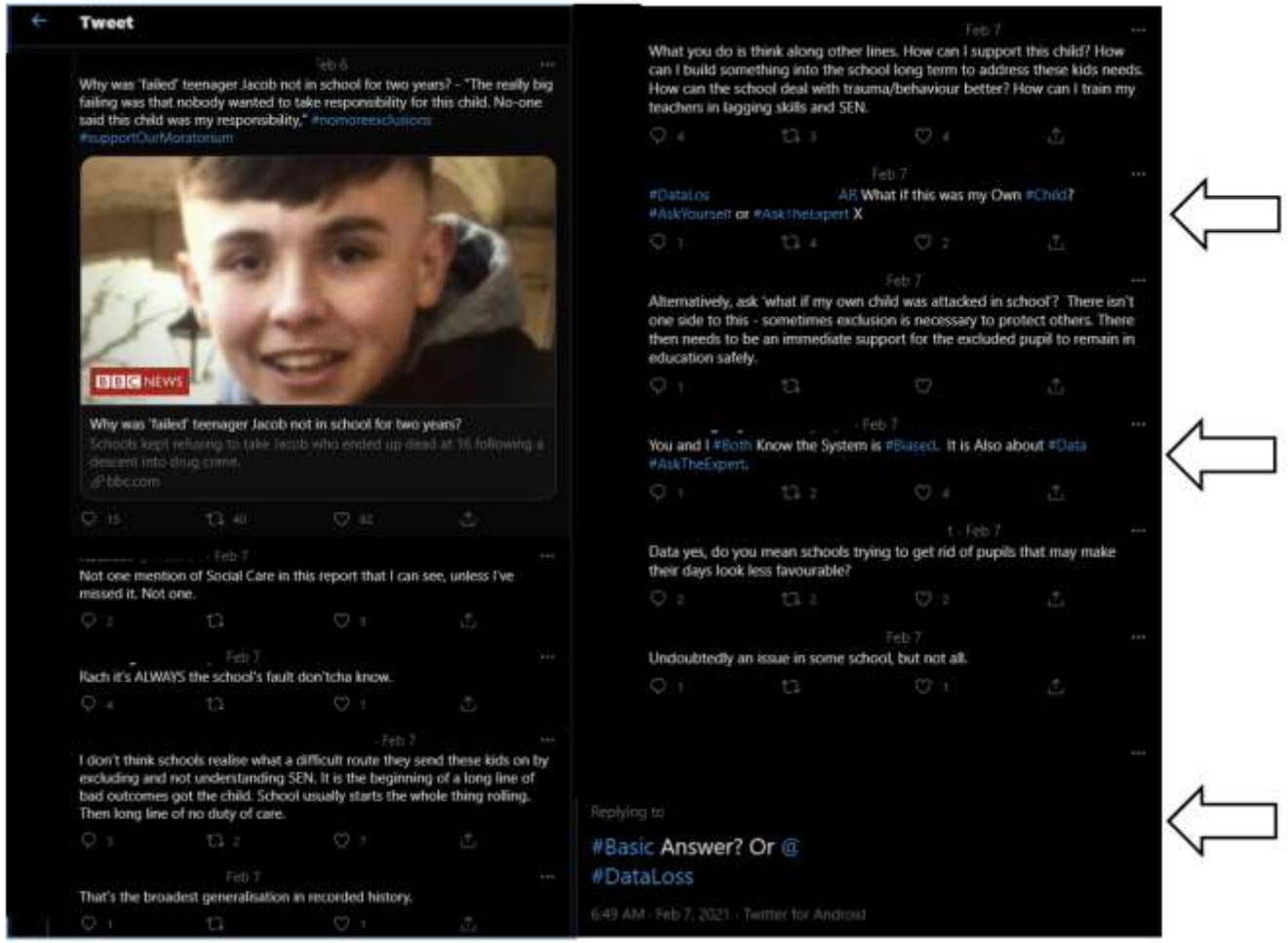


Standard Users
Verified Users
Bots

Source:
IDeaS Center, CMU

Page 1284 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Conversations with Bots



Source:
IDeaS Center, CMU

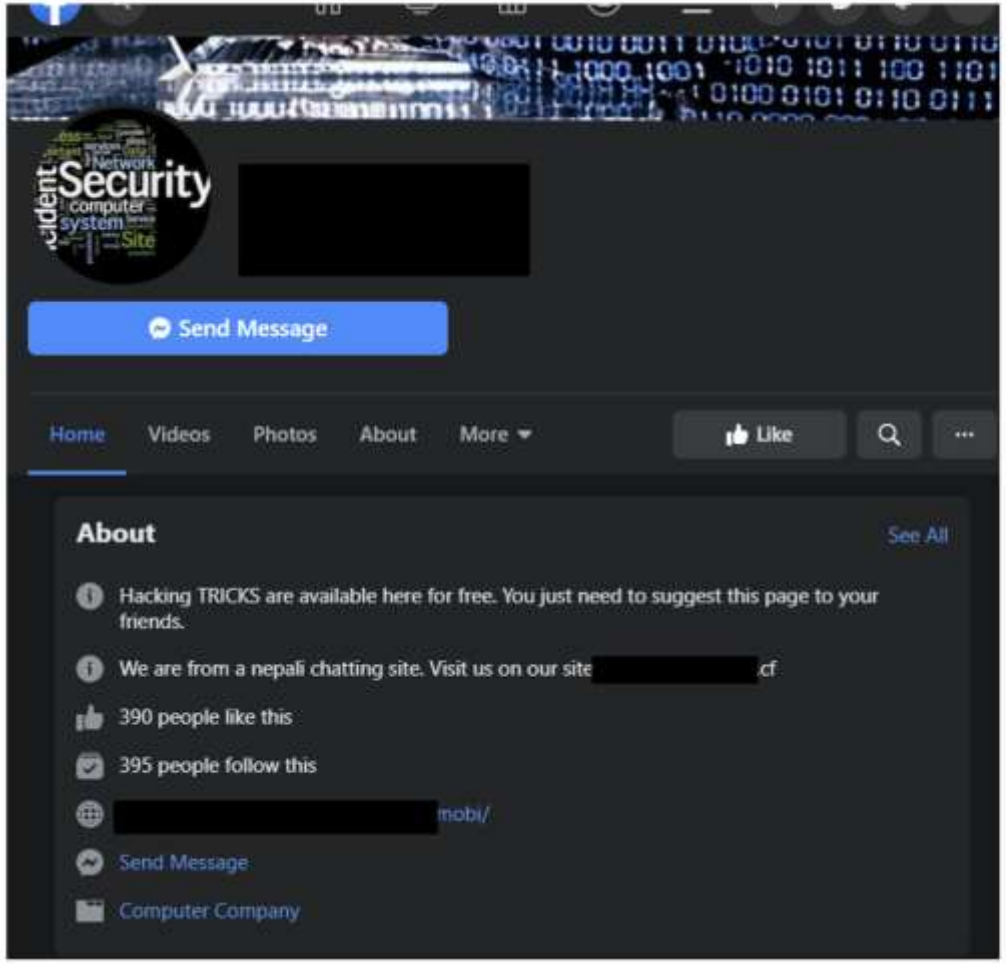
[Distribution Statement A] Approved for public release and unlimited distribution.
Page 1285 of 3957

Bogus Security Accounts – Legitimate followers

Source:
IDeaS Center, CMU

Page 1286 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Presence on Other Platforms



Source: IDeaS Center, CMU

Page 1287 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Findings and Takeaways

- Autonomous agents (bots) or semi autonomous agents (cyborgs) are present in public forum discussion

- Studying the public conversation around a topic enables us to gain cyber situational awareness – Studying Insider Risk on Twitter is just one example

  Characterizing Public Conversations -> Social Cybersecurity

- Understanding the public conversation can help us understand how to maintain and bolster organizational resilience

Source: IDeaS Center, CMU

Page 1288 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

What can we do?

Inoculation against MDM -> Increase Organizational resilience

- The importance of positive deterrence
  - From Big Brother to Good Employer
  - Analogous to “hardening the workforce”
- MDM Awareness
  - Think before you share
  - Fact checking
  - Media Literacy

Page 1289 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Future work

- Can we identify when insiders become susceptible?
  - Draw on social sciences:
    - Reactance
    - Normative conflict
    - Social identity theory
    - Social influence theory
- Can we identify ways to recruit insider via information campaigns?
- Computational Modeling
    - Inform models with network data
    - Can we simulate base rates of insider influence
        - … and then, simulate policy interventions?
    - **Inside** - **outside**

Page 1290 of 3957
[Distribution Statement A] Approved for public release and unlimited distribution.

Mr. **Luke Osterritter**
Cybersecurity Researcher
CERT Division, Software Engineering Institute, Carnegie Mellon
CASOS/IDeaS, Institute for Software Research, Carnegie Mellon

losterritter@sei.cmu.edu
https://www.sei.cmu.edu/our-work/insider-threat/
https://www.cmu.edu/ideas-social-cybersecurity/

[Distribution Statement A] Approved for public release and unlimited distribution.

C-InT SBS 2022 summit

Thank You

the ThreatLab
Integrating Research Into Practice

[Distribution Statement A] Approved for public release and unlimited distribution.

Page 1292 of 3957

Department of Defense

INSTRUCTION

NUMBER O-5240.21
May 14, 2009
Incorporating Change 1, November 19, 2010

USD(I)

SUBJECT: Counterintelligence (CI) Inquiries

References: See Enclosure 1

1. PURPOSE. This Instruction implements the policy in DoD Directive (DoDD) O-5240.02 (Reference (a)) to assign responsibilities and establish procedures for conducting CI inquiries within the Department of Defense pursuant to the authority in DoDD 5143.01 (Reference (b)).

2. APPLICABILITY. This Instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands (CCMDs), the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

b. Does not apply to general security functions such as inquiries, procedures, or personnel security investigations as defined in DoD Instruction (DoDI) 5200.01 (Reference (c)), DoD 5200.1-R (Reference (d)), and DoD 5200.2-R (Reference (e)) or to information assurance (IA) monitoring as defined in DoDD 8500.01E (Reference (f)) and DoDI 8500.2 (Reference (g)).

3. DEFINITIONS. Unless otherwise noted, the CI terms used in this Instruction are defined in Reference (a).

a. CI inquiry. For the purposes of this Instruction, "CI inquiry" has the same meaning as "CI preliminary inquiry," defined in Reference (a).

b. reasonable belief. Defined in DoD 5240.1-R (Reference (h)).

This document contains information
exempt from mandatory disclosure under
the FOIA. Exemption 2 applies.

Page 1293 of 3957

4. POLICY. It is DoD policy (Reference (a)) that the CCMDs and the Defense Agencies with organic CI capabilities may conduct CI inquiries.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. INFORMATION REQUIREMENTS. The information requirement contained in this Instruction is exempt from licensing in accordance with paragraphs C4.4.1., C4.4.7., and C4.4.8. of DoD 8910.1-M (Reference (i)).

8. RELEASABILITY. RESTRICTED. This Instruction is approved for restricted release. ~~Authorized users may obtain copies on the SECRET Internet Protocol Network from the DoD Issuances Web Site at http://www.dtic.smil.mil/whs/directives~~ *It is available to users with Common Access Card authorization on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives*.

9. EFFECTIVE DATE. This Instruction is effective immediately.

James R. Clapper, Jr.
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. Procedures

TABLE OF CONTENTS

REFERENCES.....4

RESPONSIBILITIES 5

UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)).....5
DEPUTY UNDER SECRETARY OF DEFENSE FOR HUMAN INTELLIGENCE, COUNTERINTELLIGENCE, AND SECURITY (DUSD(HCI&S)) 5
DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE CENTER (DCHC) 5
CCMD COMMANDERS (CCDRs) AND HEADS OF THE DEFENSE AGENCIES WITH ORGANIC CI ASSETS 5
SECRETARIES OF THE MILITARY DEPARTMENTS.....6

PROCEDURES.....7

INITIATING CI INQUIRIES.....7
CONDUCTING INQUIRIES 7
FOLLOW-UP ACTIVITIES 8

ENCLOSURE 1

REFERENCES

(a) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007
(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(c) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008
(d) DoD 5200.1-R, "Information Security Program," January 14, 1997
(e) DoD 5200.2-R, "Personnel Security Program," January 16, 1987
(f) DoD Directive 8500.01E, "Information Assurance," October 24, 2002
(g) DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003
(h) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1, 1982
(i) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
(j) Deputy Secretary of Defense Directive-Type Memorandum 08-032, "Establishment of the Defense Counterintelligence and Human Intelligence Center (DCHC)," July 22, 2008
(k) DoD Instruction 3305.11, "DoD Counterintelligence (CI) Training," March 19, 2007
(l) DoD Instruction 5240.04, "Counterintelligence (CI) Investigations," February 02, 2009
(m) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness, Briefing, and Reporting Programs," August 7, 2004
(n) Fifth Amendment to the Constitution of the United States, December 15, 1791
(o) Chapter 47 of title 10, United States Code
(p) DoD Instruction S-5240.17, "Counterintelligence Collection (U)," January 12, 2009
(q) DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in accordance with References (a) and (b), shall develop, coordinate, and oversee the implementation of DoD CI inquiry policy.

2. DEPUTY UNDER SECRETARY OF DEFENSE FOR HUMAN INTELLIGENCE, COUNTERINTELLIGENCE, AND SECURITY (DUSD(HCI&S)). The DUSD(HCI&S), under the authority, direction, and control of the USD(I), shall:

a. Develop and recommend CI inquiry policy.

b. Serve as the OSD staff point of contact for CI inquiry-related issues.

3. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE CENTER (DCHC). The Director, DCHC, under the authority, direction, and control of the Director, Defense Intelligence Agency, and in accordance with Deputy Secretary of Defense Directive-Type Memorandum 08-032 (Reference (j)) shall:

a. Oversee the conduct of CI inquiries.

b. Serve as the focal point to analyze information gleaned from CI inquiries to identify and report trends, anomalies, and other matters of CI interest.

c. Provide the CCMDs and Defense Agencies with the guidelines and reporting process for CI inquiries.

d. Facilitate CCMD and Defense Agency requests for review of CI inquiries referred for investigation when Military Department CI organizations or the Federal Bureau of Investigation (FBI) decline to investigate.

e. Develop, conduct, and validate training for personnel conducting CI inquiries in accordance with DoDI 3305.11 (Reference (k)).

4. CCMD COMMANDERS (CCDRs) AND HEADS OF THE DEFENSE AGENCIES WITH ORGANIC CI ASSETS. The CCDRs and the Heads of the Defense Agencies with organic CI assets shall:

a. Conduct CI inquiries in accordance with Enclosure 3.

b. Notify the Director, DCHC, of CI inquiries in accordance with DCHC guidelines and reporting processes.

c. Submit to DCHC requests for review of CI inquiries referred for investigation when Military Department CI organizations or the FBI decline to investigate.

d. Require that all personnel assigned to conduct CI inquiries are appropriately trained to the standards established by the Director, DCHC, prior to participation in any CI inquiry.

5. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments shall:

a. Evaluate CI inquiry referrals and initiate CI investigations in accordance with DoDI 5240.04 (Reference (l)) when warranted.

b. Consider using, as appropriate, the organic CI capabilities of the CCMDs and Defense Agencies to assist with the investigation of referred CI inquiries.

ENCLOSURE 3

PROCEDURES

1. INITIATING CI INQUIRIES

a. The CCMDs and Defense Agencies with organic CI assets shall initiate a CI inquiry upon receipt of information that cannot be resolved through security procedures, such as:

(1) The existence of a clandestine relationship between DoD personnel and agents of a foreign power, or of relationships between DoD personnel and individuals associated with international terrorist organizations.

(2) Failure to report contact with a foreign intelligence service.

(3) Other intelligence and/or international terrorist threats directed against U.S. Government or military facilities, property, information, operations, or personnel that appear to be at the behest of a foreign power or international terrorist organization.

(4) Failure to comply with the reporting requirements of DoDI 5240.6 (Reference (m)).

b. The goal of the CI inquiry is to establish or refute a reasonable belief that a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities.

c. The CCMDs and Defense Agencies shall use DCHC guidelines and reporting processes to document CI inquiries.

d. The CCMDs and Defense Agencies shall not delay the initiation of a CI inquiry for any improper purpose, to include attempts to delay the initiation of a CI inquiry to permit the use of otherwise prohibited techniques through security or other inquiry methods.

2. CONDUCTING CI INQUIRIES

a. CI inquiries shall be conducted in accordance with Reference (h).

b. (FOUO) Within the Department of Defense, only Military Department CI organizations have CI investigative authority and are authorized to use the intrusive techniques identified in Reference (h). The CCMDs and Defense Agencies are not authorized to use procedures 5 through 11 and procedure 13 of Reference (h). Additional prohibited techniques after the initiation of a CI inquiry are:

(1) (FOUO) Examining any information technology system or information within, except information that was gathered during the course of IA monitoring conducted before the CI inquiry began.

(2) (FOUO) Conducting consensual physical searches.

(3) (FOUO) Questioning the subject of a CI inquiry.

(4) (FOUO) Administering oaths, advising of rights pursuant to the Fifth Amendment to the Constitution of the United States (Reference (n)), and taking sworn statements, excluding unsworn official statements, except when an inquiry officer who is subject to chapter 47 of title 10, United States Code, (Reference (o)) is questioning another person who is also subject to Reference (o). In this case the inquiry officer must be familiar with the requirements of Article 31(b) of Reference (o) and, if necessary, consult with the local servicing judge advocate.

(5) (FOUO) Conducting liaison with Federal or military prosecutors unless accompanied by a representative of a CI investigative agency.

(6) (FOUO) Conducting polygraph examinations of subjects of CI inquiries.

(7) (FOUO) Requesting financial information from non-governmental institutions.

(8) (FOUO) Formally recruiting and tasking human sources.

c. CI inquiries need not be opened to:

(1) Review agency files at the request of an intelligence community (IC) member.

(2) Check agency and DoD databases to determine if an individual holds or held a DoD security clearance and has or had access to classified information or material, and provide the results to an IC member.

(3) Report, through an Intelligence Information Report (IIR), information that does not meet the threshold for initiating a CI inquiry but is of intelligence value.

(4) Report information that indicates a violation of Federal, State, or local laws. This information shall be disseminated to Federal, State, or local law enforcement agencies as appropriate and in accordance with Reference (h).

(5) Resolve internal security matters.

3. FOLLOW-UP ACTIVITIES

a. During a CI inquiry, if information establishes a reasonable belief that a clandestine relationship exists between DoD personnel and agents of a foreign power; that DoD personnel

have unreported or unauthorized contact with a foreign intelligence service; or that DoD personnel have relationships with individuals associated with international terrorist organizations, this information shall be reported immediately to DCHC and to the appropriate Military Department CI organization or the FBI.

b. If a CCMD or Defense Agency CI inquiry develops foreign intelligence information or indications of international terrorist threats, this information shall be reported through IIR or directly to the affected organization in accordance with DoDI S-5240.17 (Reference (p)) or DoDD 2000.12 (Reference (q)).

c. Once a matter has been accepted for investigation by the investigative organization, the CCMD or Defense Agency shall terminate its CI inquiry activities, but may continue to document, through the CI inquiry, any assistance provided to the CI investigative organization.

d. CCMD and Defense Agency CI personnel may participate in a CI investigation involving their organization, with the permission and under the direction of the lead investigating Service CI organization or the FBI.

U.S. Department of Justice
Federal Bureau of Investigation

FOREIGN GOVERNMENT Efforts to Influence Policy & the Public

Foreign governments routinely engage in efforts to influence our domestic and foreign policies, legislation, democratic processes, and public opinion. These governments sometimes exert this influence by employing lobbyists, public relations professionals, prominent businesspeople, or former U.S. government officials on their behalf. Such efforts are legal—if they are transparent.

Originally enacted in 1938, the Foreign Agents Registration Act—known as FARA—helps the American people and their elected officials understand who is really behind such influence activity. The statute requires persons working on behalf of foreign governments or other foreign principals (including Americans) to disclose their relationships to foreign principals and information about their activities.

Agents who fail to register are violating federal law, and they can be prosecuted if their failure is deliberate.

How FARA Works

The Foreign Agents Registration Act (FARA) Unit, which is part of the U.S. Department of Justice's National Security Division, administers and enforces FARA. Agents who register must disclose their agreements with foreign principals, report the amounts and sources of funding they have received, and provide a log of all activities they have performed on behalf of foreign principals. Agents must also label informational materials they disseminate to disclose their agency relationship, and file copies of those materials with the Unit.

FARA's definition of foreign principals includes foreign governments, political parties, corporations, individuals, and nongovernmental organizations. It defines agents as those who act at the request of or under the direction, control, or order of a foreign principal.

FARA requires an agent of a foreign principal to register when engaging in political activities or those designed to influence the U.S. government or public regarding domestic or foreign policy; taking part in perception management efforts or acting as a public relations counsel, publicity agent, or information service employee; performing fundraising or disbursement of funds; or lobbying Congress or the Executive Branch.

FARA includes exemptions for certain agents who register with the Secretary of the Senate and the Clerk of the House of Representatives under the Lobbying Disclosure Act and are therefore permitted to lobby the Legislative or Executive Branches. However, this exemption is not available to agents of foreign governments or foreign political parties—or when a foreign government or foreign political party is the principal beneficiary of the lobbying activities. Covert foreign influence campaigns often run afoul of this provision.

Read FARA at 22 U.S.C. § 611 et seq., and learn more at www.fara.gov.

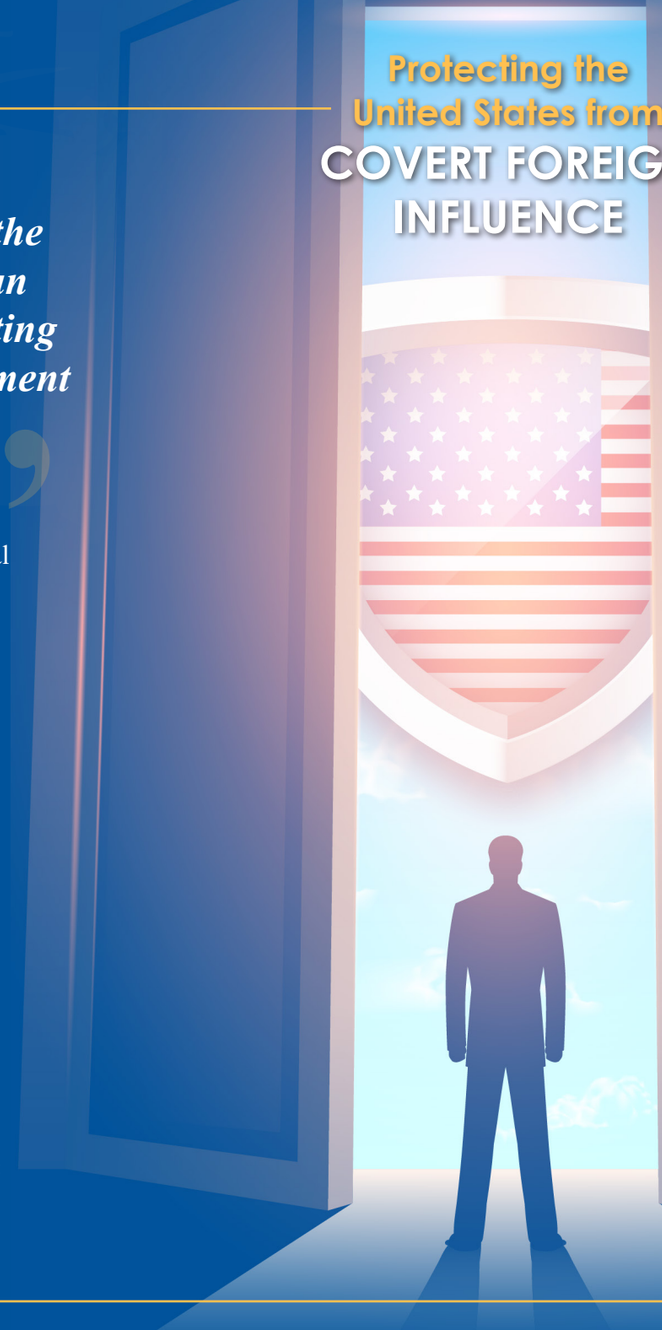
"FARA helps protect the integrity of American democracy by combating covert foreign government influence in our political process."

—Assistant Attorney General
John C. Demers

Contact us:
www.fbi.gov/contact-us
fara.public@usdoj.gov

FARA
Foreign Agents Registration Act

Protecting the United States from COVERT FOREIGN INFLUENCE



IDENTIFYING UNREGISTERED FOREIGN AGENTS

How can you tell if someone might be acting as an agent of a foreign principal and might be required by FARA to register with the Department of Justice? You could encounter a scenario like one of these:

SCENARIO 1

A PROMINENT BUSINESSMAN schedules an appointment to discuss energy policy. While you expect the meeting to focus on how U.S. policy affects his company or industry, instead he discusses an unrelated topic: a foreign country's image in the United States. During the discussion, the businessman seems to repeat statements previously made by the foreign country's leaders or spokespeople.

SCENARIO 2

A FORMER CONGRESSMAN arranges a meeting to discuss tariffs on agricultural products, but the topic seems outside his scope or areas of interest, as he previously represented an urban district and was uninvolved in agricultural or trade policy. When you meet, the former Congressman does not discuss tariffs but instead focuses on a foreign country's high-profile and longstanding request to release a prominent dissident, mirroring talking points used by the foreign country's leaders or spokespeople.

SCENARIO 3

A LOBBYIST requests a meeting to discuss telecommunications infrastructure, but when she arrives, she is accompanied by members of a foreign government or political party. They do most of the talking, discussing only the significance of telecommunications infrastructure to the foreign country—not to any U.S. businesses or companies—and highlighting issues significant to their country's relationship with the United States.

SCENARIO 4

A LOBBYIST arranges a meeting with you, and you confirm he has registered under the Lobbying Disclosure Act. However, when you meet, the lobbyist discusses topics of interest to foreign entities that are not mentioned in his filings.

Any of these scenarios could indicate you have come in contact with an unregistered agent of a foreign principal.

If you suspect you've encountered an unregistered agent of a foreign government, contact your local FBI field office or the Department of Justice's FARA Unit.

FBI

COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN)

SPIN: 15-007 SEP 2015

(U) Chinese Talent Programs

(U) INTRODUCTION

(U) Chinese Talent Programs are a vital part of Chinese industry. Talent programs recruit experts to fill technical jobs that drive innovation and growth in China's economy. National, provincial, and municipal talent recruitment programs provide opportunities for experts to work in industry and academic organizations supporting key areas deemed critical to China's development. The talent programs recruit experts globally from businesses, industry, and universities with multiple incentives to work in China. Associating with these talent programs is legal and breaks no laws; however, individuals who agree to the Chinese terms must understand what is and is not legal under US law when sharing information. A simple download of intellectual property (IP) or proprietary information has the potential to become criminal activity.

(U//FOUO) The large number of foreign students, researchers, scientists, and professionals in the United States, combined with current technological capabilities, allows foreign governments to contact and recruit individuals with the hopes to acquire advanced technology without research costs. While the majority of the population are law abiding individuals, anyone has the capability to acquire information. The theft of information can come from current or former employees, business partners, consultants, contractors, temporary hires, foreign agents, suppliers, or even vendors who have access to proprietary information.

(U) Recruiting these individuals allows China to:

- (U//FOUO) Gain access to research and expertise for cutting edge technology
- (U//FOUO) Benefit from years of scientific research conducted in the United States supported by US Government grants and private funding
- (U//FOUO) Severely impact the US economy.

(U) The goal of this SPIN is to provide an overview of the potential threats posed by the Chinese Talent Programs.

(U) CHINA'S TWELFTH FIVE-YEAR PLAN

(U//FOUO) China's National People's Congress approved a new national development program that will last for the next five years. These Five-Year Plans emphasize higher quality growth by determining themes and targets to ensure long-term prosperity. China is currently on its Twelfth "Five-Year Plan" covering 2011 to 2015, which focuses on the following:

1. **New Energy**: Nuclear, wind, and solar power
2. **Energy Conservation and environmental protection**: Energy reduction targets
3. **Biotechnology**: Drugs and medical devices
4. **New Materials**: Rare earths and high-end semiconductors
5. **New Information Technology**: Broadband networks, Internet security infrastructure, and network convergence
6. **High-end equipment manufacturing**: Aerospace and telecom equipment
7. **Clean energy vehicles**

(U) Among the plan's goals is the transformation of China from a manufacturing hub to a world leader in innovation, which will be partly met by an increase in highly skilled workers from 114 million to 180 million by 2020. Additionally, the Chinese Government spending on talent development is expected to increase from 10.75 percent of the country's gross domestic product (GDP) to 15 percent by 2020, which is approximately $1.3 trillion based on the 2014 China GDP. China's talent development program acts as a vehicle to achieve the Five Year Plan's goals.

(U) THOUSAND TALENTS PROGRAM

(U//FOUO) China's most prominent national talent recruitment program is the "Recruitment Program of Global Experts," which is commonly known as the Thousand Talents Program. It focuses on identifying key national-level organizations and associated personnel involved in implementation and management.

(U) Its goal is to recruit ethnic Chinese experts from Western universities, research centers, and private companies to boost China's national capabilities in the science and technology (S&T) fields and to move China forward as an innovative nation. The program also implemented sub-programs for both young and foreign (non-ethnic Chinese) experts.

(U//FOUO) Originally, this program had a five-to-ten year goal of recruiting 2,000 professionals worldwide who could lead innovation and pioneering work in key technologies, and promote the development of emerging industries. However, this program expanded its scope -- recruiting far more than the initial goal of 2,000 individuals -- and extended its life through at least 2020.

(U) In order to be eligible as a candidate for the Thousand Talents Program, an individual must be in a field of study the Chinese Academy of Science (CAS) deems critical or meet the following criteria:

- (U) Expert or scholar with full professorship in a prestigious foreign university or research and development (R&D) institute
- (U) Technical managerial professional in a senior position at an internationally known company or financial institution
- (U) Entrepreneur holding IP rights or key technologies and possesses overseas experience

(U) HUNDRED TALENTS PROGRAM

(U//FOUO) The Hundred Talents Program was launched in 1994 and was China's first overseas-oriented program to recruit high-level talent. The program is exclusively designed for cultivating scientific research personnel at CAS and focuses on attracting a younger talent pool.

(U//FOUO) The primary goal of the program is to cultivate a group of leaders in their areas of specialty to work at various CAS organizations. Although focused on recruiting overseas Chinese, the Hundred Talents Program will accept applicants who are currently in China. These domestic-based applicants must demonstrate internationally-recognized expertise. Most of the Hundred Talents selectees have become "chief scientists" of various 973 Program (National Basic Research Program) projects; "responsible persons" on 863 Program (National High Technology R&D Program) projects; associated with Project 111, which recruits the world's top researchers and scholars regardless of nationality or ethnic origin to work with Chinese universities; directors of state key laboratories or CAS key laboratories; or have taken high-level leadership positions within CAS institutes or offices. Selectees of this program are given 600,000 RMB (about $99,000) for resettlement costs and two million RMB (about $330,000) in startup funding for research.

(U) OTHER TALENTS PROGRAMS

(U//FOUO) The Innovative Talent Promotion Program is another Chinese Government-sponsored program. This program's ultimate goal is to create a cadre of world-class scientists and entrepreneurs who will lead technological innovation and allow China to compete internationally in S&T and strategic emerging industries.

(U//FOUO) The Thousand Youth Talents Program for Distinguished Young Scholars is a development program for young talent. Top candidates are sent to first-class universities overseas to study. These individuals are groomed into business professionals needed for the future development of China.

(U//FOUO) Lastly, there are programs that seek to develop entrepreneurial talent by focusing on building an internationally competitive corporate management cadre. The program plans to cultivate entrepreneurs with "world foresight, strategic thinking, pioneering spirit, and operating capability," and it sets a goal of having 10,000 talented personnel in management who have expertise in strategic planning, capital management, human resources management, finance and accounting, law, etc.

(U) THREAT TO US BUSINESS AND UNIVERSITIES

(U//FOUO) Chinese Talent Programs pose a serious threat to US businesses and universities through economic espionage and theft of IP. The different programs focus on specific fields deemed critical to China, to boost China's national capability in S&T fields. These subject matter experts often are not required to sign non-disclosure agreements with US entities, which could result in lost of unprotected information that jeopardizes contracts or research funding. One of the greatest threats toward these experts is transferring or transporting proprietary, classified, or export-controlled information, or IP, which can lead to criminal charges.

(U//FOUO) The threat not only targets businesses or universities but potentially targets the researchers or scientists themselves. The technology researched or developed not only costs millions of dollars but costs years, if not decades to develop. Additionally, the theft of information or IP creates a risk that someone else could take credit for the researcher's efforts. The information stolen can be recreated, resold or claimed by others, which in turn will cost the originator creditability and potential funding for future endeavors.

(U) Theft of intellectual property is an increasing threat to organizations and can go unnoticed for months or even years. In today's society, technology affords easier access to every aspect of academia and business. Some of these tools have become effective for recruiting, such as social media. Social media websites often display large amounts of personal data, such as who an individual works for, phone numbers, known associates, previous jobs, and locations. Additionally, websites like LinkedIn have full resumes, detailing the history of an individual's achievements and accomplishments.

(U) The FBI assesses each year the United States loses billions of dollars due to technology transfer. While it is important to conduct collaborative research, it is vital for the survival of US businesses and universities that they protect their information and mitigate lost or stolen information.

(U) Areas of Interest for Recruitment:

- Information Technology
- Biotechnology
- Aerospace
- Materials & Manufacturing
- Sensors & Optics
- Energy & Environment
- Basic Sciences

(U) MEDICAL CENTER OF WISCONSIN

(U) Zhao, J. Hua – (DPOB: 1971, China) In February 2013, Zhao, a research assistant at Medical College of Wisconsin (MCOW) under Professor Marshall Anderson, stole three vials of C-25, a compound patented by Anderson and used in his cancer research. Security footage examined during an internal investigation revealed Zhao entering Anderson's office and leaving shortly after.

(U) Zhao was reprimanded previously for placing laboratory data on his personal computer. The internal investigation found research data on C-25. Zhao claimed the data would be used to conduct further studies at Zhejiang University.

He was ordered to remove the data from his computer and place it on an MCOW computer. Additionally, MCOW discovered a posting by Zhao on an Internet site called Researchgate indicating he discovered a cancer fighting compound he wanted to bring back to China.

(U) In March 2013, Zhao was arrested. In addition to the 384 files found on Zhao's personal computer relating to Anderson's research was an application to the National Natural Science Foundation of China that provides funding for many talent programs and to a Chinese foundation claiming he invented C-25 and requesting funding for additional research. This application was an exact translation of the grant application written by Professor Anderson several years earlier. It was also determined that Zhao accessed his MCOW computer remotely on the day he was suspended and attempted to delete the files he stole relating to C-25. Zhao was convicted to time served in August 2013.

(U//FOUO) Zhao had a previous history of disregarding the appropriate handling of university property and had full access to Professor Anderson's lab. His access allowed him the ability to walk in and out of the lab at his own discretion to steal the vials of C-25 and laboratory data. Had C-25 not been patented by Anderson, Zhao could have claimed and patented the cancer-fighting compound for himself. Additionally, Zhao's LinkedIn profile indicated he held a position at Zhejiang University, which has ties to the Thousand Talent Program.

(U) DUKE UNIVERSITY

(U) Liu, Ruopeng – (DPOB: 1983, China) In 2006, Liu, a graduate student at Duke University, worked in the laboratory a US researcher studying metamaterials. Liu had full access to the researcher's lab, which conducted basic and fundamental research. While working for this researcher, Liu arranged meetings between the researcher's lab and Cui Tie Jun, a Chinese program manager associated with Project 111 (focused on basic science and advanced technology by recruiting the best international experts to China to study from). The idea behind this connection was to share ideas, however, the US researcher eventually realized most of the ideas were coming from his lab.

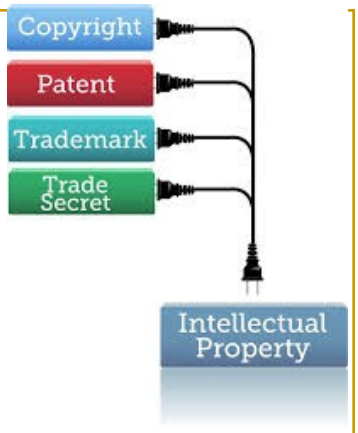
(U) Over the next few years, he discovered pictures and information related to his research used to market a business started by the Liu. The business originally seemed plausible to him, because he knew Liu was applying for positions with Massachusetts Institute of Technology, which tends to favor faculty members who also have an entrepreneurial bent. The information marketed by Liu attracted a Chinese technology company. Additionally, Liu invited two Chinese visitors associated with CUI's lab from Southeast University to visit the lab. The visitors took photographs of all the equipment in the lab, including the make and model, which in turn were used to reproduce the lab in China.

(U) In 2009, the US researcher received a book entitled *Metamaterials: Theory, Design, and Applications* by Cui, Liu, and the researcher that was published in the United States. Unknowingly, the researcher had in fact signed off on some forms and received multiple e-mails regarding the book by relying on Liu's interpretation. At the same time, Liu, Cui, and another Chinese individual collaborated on a research idea based on a paper regarding carpet-cloak theory later published in 2009 in an issue of *Science*. Located in the article is a footnote acknowledging the support from Innovation Technology, National Science Foundation, National Basic Research Program (973) of China, Natural Science Foundation of Jiangsu Province, and Project 111.

(U) While the researcher's lab does not conduct restricted research, it receives funding from the US Department of Defense and US Intelligence Community. Since the research was not restricted, there were no rules against or restrictions on the lab's collaborative research efforts. Liu did not have to sign a non-disclosure agreement. Liu moved back to China after the researcher retracted his recommendation for Liu's employment at Princeton with Dr. Stephen Chou, the head of the nanotechnology laboratory. Liu has reportedly established a research institution in Shenzhen.

(U//FOUO) By convincing the US researcher to collaborate with Cui, Liu was able to freely share information and invite visitors to the lab. Although this was not restricted research, the metamaterials research could have both military and civilian applications. The US researcher risked his research by allowing visitors to come into his lab without personally looking at their background and being too trusting of his scientific relationship with Liu.

(U) HOW TO PROTECT YOUR ORGANIZATION



(U) The first step to protecting your business or university is to identify the threat.

- Who would benefit from your information, processes, or strategies?
- Who are your competitors?
- Have individuals been unusually interested in what you do?

(U) The next step is to identify proprietary or trade secrets or IP. This includes, but is not limited to the manufacturing process, financial information, list of suppliers and customers, chemical formulas, marketing strategies, and R&D data. By understanding the threat and your business or university's critical technologies, it can help you identify methods in which they can be easily stolen. Theft, bribery, espionage, blackmail, hacking, and electronic intercepts are just some of the different methods individuals may use to steal trade secrets.

- (U) Have professors, students, and employees sign non-disclosure agreements.
- (U) Identify foreign personnel who are sponsored by professors/employees.
- (U) Understand agreements between international organizations and US businesses and universities.
- (U) Identify and label or mark IP or sensitive data that is most important to US businesses and universities.
- (U) Identify methods in which professors and employees are contacted (for example, e-mail, social media, conferences) and educate them on what solicitation looks like.
- (U) Report any incidents or concerns to your security office and local FBI field office.

(U) If you wonder about the safety of your research or intellectual property, or the legality of your interactions with China, ask yourself the following questions. If any of the answers concern you, or you would like additional information, please contact your local FBI Strategic Partnership Coordinator or FBI field office.

- (U) Do you collaborate with anyone who is currently in China?
- (U) Do you have any publications? If so, in which journals and with whom? Which institutions are they associated with?
- (U) What type of funding do you have to conduct your research? Where do you obtain your funding?
- (U) Do you belong to any professional societies? If so, which ones and where are the based?
- (U) Do you travel regularly to China? Is it for business or pleasure or both? How long do you stay in China during these trips? Are you working with anyone in China on your research during this time ?
- (U) How do you maintain contact with your laboratory in the United States while in China? Do you contact it via computer (login to laboratory site)?
- (U) Do you plan to return to China permanently? What will you do for employment?
- (U) Where did you attend school? What type of degrees did you earn? How did you apply for a fellowship, post-doctoral position, guest researcher or other employment with your current employer? Did someone you know refer you to this lab, university, or principal investigator?
- (U) What type of research do you conduct? What are the applications of this research? Do you expect to get a patent from this research?
- (U) With whom are you working at your laboratory? Do you collaborate with individuals from other research institutions in the United States or abroad?

Sources

(U) KPMG; China's 12th Five-Year Plan: Overview; 2011; http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf; accessed 04 March 2015.

(U) Online Article; Chinese Academy of Science: Thousand Talents Program; 2012; http://english.ucas.ac.cn/JoinUs/Pages/default.aspx; accessed 04 September 2014.

(U) OSC Analysis 14-024; accessed 06 March 2015.

(U) Wang, Huiyao; China's National Talent Plan: Key Measures and Objectives; 2010; http://www.brookings.edu/research/papers/2010/11/23-china-talent-wang; accessed 06 March 2015.

(U) Robertson, John; Investigating Intellectual Property Crime; 2010; https://intranet.fbinet.fbi/ccrsb/CyD-old/CCS/CCU-3/CCTF_Document_Library/2010%20CCTF%20Conference%20Presentation%20Materials/IPR%20Presentation.ppt; accessed 09 March 2015.

This product was prepared by the FBI Strategic Partnership Unit (CD-4F). Please provide any questions or comments to your local Strategic Partnership Coordinator (SPC) or CD-4F at Strategic_Partnerships@ic.fbi.gov.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

13 June 2018

PIN Number
20180613-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

APT Actors Likely to Target US Cleared Defense Contractors

Summary

APT actors in the near future likely intend to target US Cleared Defense Contractors (CDC) via spear phishing campaigns or network infrastructure compromises, according to recent intelligence. Common spear phish targets may include individuals featured on internet-facing CDC Web sites and high-ranking CDC executives.

FBI has observed APT actors over the past two years precede spear phishing campaigns with open source research of targeted US company websites, particularly sections containing contact information for company officials which include names, titles, telephone numbers, and email addresses. In one case, an APT actor sent spear phishing emails within one-to-two weeks after researching the targeted US company.

Historically, APT actors have a strong desire to collect US defense and scientific intelligence to further their interests and advance strategic goals. As a result, US CDCs and research facilities may likely be targets for cyber adversaries due to their involvement in national security and their close relationship with the US Government.

Most companies publicly share their contact information and high-level management names on their corporate Web pages. Some corporate employees share other forms of personally identifiable information on various social media platforms. Adversaries may use this publicly-posted information to target individuals with the end goal of infecting a corporate network for intelligence collection.

Common techniques used by APT actors include sending well-crafted spear phishing messages tailored to the professional interests of the target, the use of watering holes to redirect visitors to malicious Web sites, and the use of stolen or weak user credentials to exploit a network vulnerability. After a successful compromise, APT actors attempt to expand their access in the network to multiple systems to facilitate information theft.

APT actors have increased their activity over the last several years. Cyber attacks such as WannaCry and NotPetya in the spring and summer of 2017 are examples of increasing APT activity. While WannaCry and NotPetya were not directed at the United States, both had inadvertent negative effects on US systems. The FBI advises companies to be mindful that similar attacks may likely occur in the near future. Previous attacks have coincided with national holidays of cyber targets, such as Constitution Day in Ukraine on 28 June.

For recent guidance on mitigation strategies against spear phishing and network infrastructure targeting, please refer to the following joint technical alerts:

https://www.us-cert.gov/ncas/alerts/TA18-074A

https://www.us-cert.gov/ncas/alerts/TA18-106A

Recommendations:

The FBI recommends providers implement the preventative measures listed below to help secure their systems from attacks:

- Ensure anti-virus software and firmware is up-to-date

- Monitor employee logins outside normal business hours and other anomalous activity
- Close unused ports
- Monitor employee logins outside normal business hours and other anomalous activity
- Provide regular training to employees regarding current social engineering threats, scrutinizing e-mail links and attachments, and pop-ups from attachments requesting enabling certain functions (i.e., macros)
- Brief executives at your company to be extra vigilant and report any suspicious email messages
- Apply extra scrutiny to e-mail messages with links or attachments directed toward executives

This product is marked **TLP:GREEN**. Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**FIGHTING BEARS AND TROLLS:
AN ANALYSIS OF SOCIAL MEDIA COMPANIES AND U.S. GOVERNMENT EFFORTS TO COMBAT RUSSIAN INFLUENCE CAMPAIGNS DURING THE 2020 U.S. ELECTIONS**

by

Elvis M. Chan

September 2021

Co-Advisors: Christopher Bellavita (contractor)
Erik J. Dahl

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
FIGHTING BEARS AND TROLLS: AN ANALYSIS OF SOCIAL MEDIA COMPANIES AND U.S. GOVERNMENT EFFORTS TO COMBAT RUSSIAN INFLUENCE CAMPAIGNS DURING THE 2020 U.S. ELECTIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Elvis M. Chan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense, the FBI, or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This thesis seeks to evaluate the effectiveness of the Russian disinformation campaigns targeting the 2020 U.S. elections and the efforts taken by the U.S. government and social media companies to thwart them. To develop countermeasures for Russian interference activities targeting future American elections, this thesis asks the question:

What impact did the countermeasures taken by the American social media companies and the U.S. government have on Russian social media influence campaigns targeting the 2020 U.S. elections?

This thesis uses a framework developed by Thomas Wilhelm, a U.S. Army researcher, to evaluate Russian hybrid warfare, based on the principles of Andrei Kartapolov, a prominent Russian general. Accordingly, it is used to measure the qualitative impact of the Russian measures and American countermeasures during the 2020 U.S. elections.

This thesis finds that the Russians shifted their tactics from 2016 to 2020. Still, the U.S. government and social media companies effectively impeded their influence campaigns primarily through information sharing and account takedowns, respectively. Because the Russians will continue their influence campaigns to undermine the United States, this thesis provides recommendations to include standardized information sharing and the establishment of a national coordination center.

14. SUBJECT TERMS
propaganda, social media, information operations, information warfare, active measures, foreign influence, influence operations, democracy, social discourse, hybrid warfare, bots, trolls, cyber, psychological operations, Soviet Union, Russia, social media, Facebook, Twitter, Instagram, Google, YouTube, big data, data analytics, micro-targeting, 2020 presidential election

15. NUMBER OF PAGES
149

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Page 1315 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 1316 of 3957

Approved for public release. Distribution is unlimited.

FIGHTING BEARS AND TROLLS: AN ANALYSIS OF SOCIAL MEDIA COMPANIES AND U.S. GOVERNMENT EFFORTS TO COMBAT RUSSIAN INFLUENCE CAMPAIGNS DURING THE 2020 U.S. ELECTIONS

Elvis M. Chan
Assistant Special Agent in Charge, Federal Bureau of Investigation
B.S. Che E., University of Washington, 1993
BS, University of Washington, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2021

Approved by: Christopher Bellavita
Co-Advisor

Erik J. Dahl
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

Page 1317 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 1318 of 3957

ABSTRACT

This thesis seeks to evaluate the effectiveness of the Russian disinformation campaigns targeting the 2020 U.S. elections and the efforts taken by the U.S. government and social media companies to thwart them. To develop countermeasures for Russian interference activities targeting future American elections, this thesis asks the question: What impact did the countermeasures taken by the American social media companies and the U.S. government have on Russian social media influence campaigns targeting the 2020 U.S. elections?

This thesis uses a framework developed by Thomas Wilhelm, a U.S. Army researcher, to evaluate Russian hybrid warfare, based on the principles of Andrei Kartapolov, a prominent Russian general. Accordingly, it is used to measure the qualitative impact of the Russian measures and American countermeasures during the 2020 U.S. elections.

This thesis finds that the Russians shifted their tactics from 2016 to 2020. Still, the U.S. government and social media companies effectively impeded their influence campaigns primarily through information sharing and account takedowns, respectively. Because the Russians will continue their influence campaigns to undermine the United States, this thesis provides recommendations to include standardized information sharing and the establishment of a national coordination center.

Page 1319 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 1320 of 3957

TABLE OF CONTENTS

I. RUSSIA RISES FROM THE ASHES OF THE COLD WAR 1
- A. PROBLEM STATEMENT 2
- B. RESEARCH QUESTION 3
- C. LITERATURE REVIEW 4
  - 1. Russian Online Influence Activities from 2014 to 2020 5
  - 2. Countermeasures by the Private Sector and the U.S. Government 10
  - 3. Framework for Understanding Russian Hybrid Warfare 12
  - 4. Recommendations for Countering Russian Influence Campaigns 15
  - 5. Conclusions from Literature Review 18
- D. RESEARCH DESIGN 19

II. OPENING MOVES – SCOPE AND BACKGROUND 23
- A. SCOPE OF THESIS 24
  - 1. Relevant Time Periods 24
  - 2. Types Of Russian Influence Operations 25
  - 3. Targeted Social Media Platforms 26
- B. RECENT HISTORY – THE CAMPAIGNS FROM 2016 TO 2018 27
  - 1. What Happened During the 2016 U.S. Elections? 29
  - 2. What Happened During the 2018 U.S. Midterm Elections? 43
- C. CONCLUSIONS FROM THE 2016 AND 2018 ELECTIONS 55

III. THE 2020 ELECTIONS – RUSSIAN GAMBIT AND AMERICAN COUNTERPLAY 57
- A. THE IRA AND OTHER PROXIES' SOCIAL MEDIA ACTIVITIES 59
- B. PRIVATE SECTOR COUNTERMEASURES 68
- C. U.S. GOVERNMENT COUNTERMEASURES 75
- D. USING THE KARTAPOLOV FRAMEWORK TO EVALUATE RUSSIAN AND AMERICAN MEASURES IN 2020 80
  - 1. The IRA and Other Proxies – Impact and Evolution 80
  - 2. The Private Sector Companies' Impact and Adaptations 83
  - 3. The U.S. Government's Impact – Transparency and Private Sector Partnerships 85

Page 1321 of 3957

E. VOTER TURNOUT IN THE 2020 ELECTIONS 88
F. CONCLUSIONS FROM THE 2020 U.S. ELECTIONS 89

IV. CONCLUSIONS AND RECOMMENDATIONS TO COUNTER RUSSIA IN THE FUTURE 91
A. CONCLUSIONS – THERE IS NO END GAME 91
B. RECOMMENDATIONS FOR PROTECTING FUTURE ELECTIONS FROM RUSSIAN INTERFERENCE 94
1. Security Measures 95
2. Transparency Measures 99
3. Resiliency Measures 103

LIST OF REFERENCES 107

INITIAL DISTRIBUTION LIST 125

Page 1322 of 3957

LIST OF FIGURES

Figure 1. Kartapolov's Components for Conducting Hybrid Warfare.....15

Figure 2. Facebook Political Advertisement Targeting Hillary Clinton. 29

Figure 3. Facebook Political Ads Targeting Black voters.....32

Figure 4. Facebook Political Ads Targeting Right-Wing Voters. 32

Figure 5. Highlights of Russian and American Actions from 2018 to 2020.....58

Figure 6. An Image from a Facebook Account Controlled by EBLA. 60

Figure 7. Postings from the PeaceData Site. 62

Figure 8. Photos of PeaceData Staff Created by Artificial Intelligence.....62

Figure 9. Posting from the NAEBC Site. 64

Figure 10. NAEBC Cross-platform Posting on Parler. 64

Figure 11. GANS-generated Profile Photos for NAEBC Staff. 65

Figure 12. Breakdown of Secondary Infektion Articles by Topic. 66

Figure 13. Secondary Infektion-made Forged Posting from Marco Rubio.....67

Figure 14. Secondary Infektion-made Forged Letter to John Kerry. 67

Figure 15. Breakdown of Twitter Tweets by Topic for 2019. 71

Page 1323 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 1324 of 3957

LIST OF TABLES

Table 1. Reach of IRA-controlled Social Media Accounts 35

Table 2. Comparison of Black Voter Turnout for Presidential Elections. 40

Table 3. IRA Spending Plan for 2017 and 2018. 44

Table 4. Voter Turnout by Demographic in Midterm Elections. 53

Table 5. Summary of Facebook Takedowns for 2020. 70

Table 6. Summary of Twitter Takedowns for 2020. 73

Table 7. Summary of Google Takedowns for 2020. 74

Table 8. Social Media Account Takedowns between 2016 and 2020. 83

Table 9. Comparison of Overall Voter Turnout for Presidential Elections. 89

Table 10. Security Measures for Countering Russian Information Operations. 96

Table 11. Transparency Measures for Countering Malign Russian Influence. 100

Page 1325 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 1326 of 3957

LIST OF ACRONYMS AND ABBREVIATIONS

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DNC	Democratic National Committee
EBLA	Eliminating Barriers for the Liberation of Africa
FARA	Foreign Agent Registration Act
FSB	Federal Security Service
FS-ISAC	Financial Sector ISAC
GANS	generative adversarial networks
GEC	Global Engagement Center
GRU	Main Directorate of the General Staff of the Russian Armed Forces
HPSCI	U.S. House Permanent Select Committee on Intelligence
ICA	Intelligence Community Assessment
IRA	Internet Research Agency
ISAC	Information Sharing and Analysis
JAR	joint analysis report
NAEBC	Newsroom for American and European Based Citizens
NCSC	National Counterintelligence and Security Center
NDAA	National Defense Authorization Act
ODNI	Office of the Director of National Intelligence
SSCI	U.S. Senate Select Committee on Intelligence

Page 1327 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 1328 of 3957

EXECUTIVE SUMMARY

This thesis uses a systematic framework to evaluate the qualitative effectiveness of the Russian disinformation campaigns and the countermeasures taken by the U.S. government and social media companies to combat the aforementioned campaigns targeting the 2020 U.S. elections. To develop effective countermeasures for Russian interference activities targeting future American elections, this thesis seeks to answer the following question: What impact did the measures taken by the American social media companies and the U.S. government have on Russian social media influence campaigns targeting the 2020 U.S. elections?

Russian operatives working under the auspices of a St. Petersburg-based organization, known as the Internet Research Agency (IRA), created a significant degree of the toxicity on social media during the 2016 U.S. elections.[1] The online social media influence campaign perpetrated by the Internet Research Agency aimed to fan the flames of existing divisive rhetoric, drive a wedge between the many demographic groups in America, and erode confidence in democracy.[2] Russia remains a committed adversary with influence operations continuing to this very day, posing an active threat to American democracy.[3]

Since the end of 2016, federal agencies and private sector organizations, specifically the major American social media companies, have been actively helping to safeguard political campaigns and election infrastructure from computer intrusions through increased cybersecurity and other security measures. To date, most research has focused on quantitative and qualitative analyses of the IRA's influence campaigns. However, this research has not analyzed how the Russian government perceived the effectiveness of its

[1] Robert Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: Department of Justice, 2019), 4, https://www.hsdl.org/?view&did=824221.

[2] Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency* (New York: New Knowledge, 2018), 4.

[3] Miles Parks and Philip Ewing, "Foreign Interference Persists And Techniques Are Evolving, Big Tech Tells Hill," National Public Radio, June 18, 2020, https://www.npr.org/2020/06/18/880349422/foreign-interference-persists-and-techniques-are-evolving-big-tech-tells-hill.

campaigns. Furthermore, the efficacy of the U.S governmental and private sector actions to defend against the IRA's influence campaigns has not been systematically analyzed.

The objectives of this thesis are three-fold: (1) examining the Internet Research Agency and other Russian social media campaigns ahead of the 2020 U.S. elections to determine whether its tactics have shifted since 2016; (2) critically analyzing the private sector and U.S. government's actions to counter the Russian influence activities; and (3) proposing recommendations to safeguard future U.S. elections. The first two objectives are assessed using an analytical framework proposed by Thomas Wilhelm, Director of the U.S. Army's Foreign Military Studies Office. The results of the first two objectives, inform the last objective as well as a review of current literature by scholars and subject matter experts in different fields.

To design a helpful framework for analyzing Russian influence operations, Thomas Wilhelm surveyed the published works and speeches of General Lieutenant Andrei V. Kartapolov. Wilhelm surmised Kartapolov was one of the key architects of current Russian military science and doctrine.[4] Wilhelm believed the framework provided a well-rounded understanding of Russian martial intent and objectives about hybrid warfare from a Russian perspective.[5] Specifically, Kartapolov advocates using asymmetric, non-violent methods to undermine the strengths of Russia's opponents to achieve their strategic goals.[6]

The relevant components of the Kartapolov Framework for analyzing Russian social media-based influence operations against the United States are: (1) spreading discontent in the population; (2) exerting political pressure; and (3) confusing the political leadership.[7] This thesis uses the Kartapolov framework to conduct a qualitative evaluation of the Internet Research Agency's impact and the effectiveness of social media companies and the U.S. government's countermeasures. Specifically, it analyzes American actions to

[4] Tom Wilhelm, "A Russian Military Framework for Understanding Influence in the Competition Period," *Military Review* (2020): 35.

[5] Wilhelm, 38.

[6] Rod Thornton, "The Russian Military's New 'Main Emphasis,'" *RUSI Journal* 162, no. 4 (2017): 18–28, https://doi.org/10.1080/03071847.2017.1381401.

[7] A. V. Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," *Journal of the Academy of Military Science* 51, no. 2 (2015): 36.

determine their effectiveness for countering the three influence-related components of the Kartapolov Framework.

Three main themes emerged from the 2020 U.S elections. First, the Russians continued their efforts to target the U.S. elections but shifted tactics to avoid detection. Second, the social media companies, along with news media and research organizations, successfully identified and disrupted the evolving Russian disinformation campaigns. Third, the U.S. government acted more forcefully in securing the elections, primarily through its information sharing with the social media companies, political organizations, and the American public.

Despite the best efforts of the Russians, social media companies, news media, and research organizations detected, exposed, and disrupted the activities of the Internet Research Agency and other Russian-affiliated online groups. Although America's private sector may have been caught unaware during the 2016 elections, it was on heightened alert ahead of 2020, with the noteworthy efforts of American news outlets and non-governmental organizations exposing Russian disinformation activities and paving the way for the social media companies to shut down their social media accounts.

The U.S. government's response to the Russian influence campaign appeared more robust before the 2020 elections than in the 2016 or 2018 elections. The most important actions taken by the U.S. government may have been the information sharing with the social media companies to expose Russia's different operations and shut down its accounts. In addition, the U.S. government's information-sharing may have helped the social media companies secure their platforms by identifying malign Russian influence activities. The U.S. government's other responses, such as economic sanctions and indictments, provided the American public with factual narratives of the crimes perpetrated by the Russian Federation.

It took the collaborative efforts of the private sector, in the form of social media companies, researcher organizations, and news media, and the public sector, in the form of the executive and legislative branches of the U.S. government, to turn back the Putin-

sanctioned disinformation operations which were targeting the 2020 U.S. elections.[8] Ultimately, the American actions appeared effective in mitigating the Russian online tactics because voters were undeterred and turned out in record numbers for the election.

The 2021 Intelligence Community's annual threat assessment named Russia as one of "the most serious intelligence threats to the United States" and warned that the Russian government would continue its efforts to propagate dissension in the American populace.[9] Based on the evaluation of the Russian actions and the effectiveness of the American responses in the 2020 U.S. elections, this thesis makes recommendations for protecting future elections that have been drawn from experts in the U.S. government, non-governmental organizations, and academic institutions. The three types of possible actions are broadly categorized as security, transparency, and resiliency measures.[10] The proposed security measures include enhanced cybersecurity, enhanced disinformation detection, economic sanctions, information sharing, and the establishment of a fusion center. The transparency measures proposed include a public communications strategy, content labeling standards, updated political advertising and campaign finance laws, and transparent reporting. The resiliency measures suggested include improved media literacy

---

[8] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution (*Washington, DC: Office of the Director of National Intelligence, 2017), 7, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[9] Office of the Director of National Intelligence, *2021 Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2021), 11, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2204-2021-annual-threat-assessment-of-the-u-s-intelligence-community.

[10] Gabriel Cederberg et al., *National Counter-Information Operations Strategy* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019), https://www.belfercenter.org/publication/national-counter-information-operations-strategy; Renée DiResta and Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019* (Palo Alto, CA: Stanford University, 2019), https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks; Angus King and Mike Gallagher, *Cybersecurity Lessons from the Pandemic*, CSC White Paper #1 (Washington, DC: U.S. Cyberspace Solarium Commission, 2020), https://www.solarium.gov/public-communications/pandemic-white-paper; *Report on Russian Active Measures* (Washington, DC: U.S. Congress. House, 2018), https://republicans-intelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf; *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts against Election Infrastructure with Additional Views*, Senate, 116th Cong., 1st Sess. (Washington, DC: U.S. Congress. Senate, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

and critical thinking for the American public.[11] Hopefully, incorporating the proposed measures with existing ones will help repair and strengthen the framework of American democracy for the 21st century.

[11] Michael McFaul, ed., *Securing American Elections* (Palo Alto, CA: Stanford University, Cyber Policy Center, 2019), 8, https://www.hsdl.org/?view&did=827251.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

As I write these acknowledgments, I feel a sense of relief for finishing the program, and sadness for it coming to an end. I am most grateful for all of the people who made this accomplishment possible. My primary reasons for participating in this master's program were to intellectually challenge myself and add academic rigor to all the on-the-job training I have received working on national security matters at the FBI. Both objectives were accomplished handily, thanks to the outstanding instructors and staff at the Naval Postgraduate School.

What I did not account for was undertaking this feat during a once-in-a-lifetime pandemic. While the pandemic has been an unmitigated disaster for the world, it has been a mixed blessing for me. On the one hand, I wonder how much more I would have learned from the instructors and cohort members if we were in person. Experience has taught me that some of the most valuable discussions happen between classes or during sidebar conversations. On the other hand, I have not had to travel for work since the start of the pandemic, which has allowed me to focus on my studies after work and on the weekends. I recognize these are first-world privileges and am thankful.

I was pleasantly surprised by how close I became with my cohort members though I had never met any of them physically. I am very thankful for a few of our colleagues who have helped me along this academic journey. They include Cassie, our president who has been guiding us along like a gaggle of unruly geese; the California contingent of Rich, Ben, and Heather, who have been my supportive teammates on many group projects; Rob, who is the congenial host of Not Quite the Trident Room and a steadying influence on me; Katie, who constantly challenges me and created the infamous Riesner Theory; Ron, who is my younger and intractable ideological twin; and Emily, whose youth belies her insight. To Cohort 2001/2002, I say to you, *satis esse fortis stultum*.

To the Naval Postgraduate School faculty and staff, I am filled with gratitude and thank you for your efforts during this difficult time. I can honestly say that every class challenged me, with some making me feel mentally stretched in ways I did not think were

Page 1335 of 3957

possible. First and foremost, I want to give a hearty thank you to my thesis team. Dr. Erik Dahl's acumen and discernment have focused my writing and made my thesis better. I consider you a kindred spirit in the practice of intelligence analysis and homeland security. Dr. Chris Bellavita's steadfast faith in me and support of my thesis topic has been the wind at my back. I appreciate your advocacy and use of the Socratic method to strengthen my thinking. Marianne Taflinger had the unenviable task of being my writing coach and taking the first crack at shaping my drafts so that they would be presentable to my advisors. Thank you for your patience and constructive feedback. Other instructors who have made a lasting impression on me include Branders, who rolled into class looking like a couple of Hell's Angels but spurred some of the most profound conversations I have ever had, and Paul Smith, who is the old friend in the security business that I just met this year.

To my sisters and brothers at the Federal Bureau of Investigation, I am proud to stand next to you and represent our storied organization. I appreciate the support of my superiors in allowing me to participate in this program, our supervisors who have minded the office when I am away from work, and my colleagues back at headquarters who were in the trenches with me as we worked to protect the 2020 elections. Your fidelity, bravery, and integrity motivate me to continue striving to improve myself.

To my colleagues in the private sector, I am glad that we find common cause with protecting the elections from malign foreign influence and other online threats. I have learned a great deal from you and appreciate your continued efforts to safeguard your platforms. Hopefully, we will get to see each other in person soon.

To my family, I appreciate all of your unflinching support and hope my efforts have made the world a better place in some small way. To my mother and father, thank you for instilling me with my drive for academic excellence and work ethic. To the Ochikubo and Furuya families, thank you for supporting my family and me with all of your time and energy when I decided to make a drastic midlife career change. To both of my daughters, my heart bursts with pride as I watch you grow into independent, fierce, and outspoken women who will positively impact this world in ways I have not imagined. Most importantly, I want to give the deepest thanks to my wife for all of her love, unwavering support, patience, and grace. Without her, none of my accomplishments are possible.

Page 1336 of 3957

I. RUSSIA RISES FROM THE ASHES OF THE COLD WAR

> Over the course of my career, I've seen a number of challenges to our democracy. The Russian government's effort to interfere in our election is among the most serious.
>
> —Robert S. Mueller III, July 24, 2019

This statement from the well-respected former FBI Director underscored the severity of the Russian actions to interfere with the 2016 U.S. elections. After the end of the Cold War and the fall of the Soviet Union in 1991, Russia appeared to have faded from America's collective memory as an adversary.[1] This attitude abruptly changed on June 14, 2016, when a U.S.-based cybersecurity firm named Crowdstrike announced it had investigated intrusions into the computer networks of the Democratic National Committee (DNC) by two Russian hacking groups, code-named "Fancy Bear" and "Cozy Bear."[2] Away from the news media scrutiny, Russian operatives working under the auspices of a St. Petersburg-based organization, known as the Internet Research Agency (IRA), created a significant portion of the toxicity on social media during the presidential campaign season.[3] The "sweeping and sustained" online social media influence campaign perpetrated by the Internet Research Agency aimed to fan the flames of existing divisive rhetoric, drive a wedge between the many demographic groups in America, and erode

[1] Jon Wiener, *How We Forgot the Cold War: A Historical Journey Across America* (Berkeley: University of California Press, 2012), 1, https://books.google.com/books?hl=en&lr=&id=w_Sa-F8DXhgC&oi=fnd&pg=PA1&dq=american+memory+of+the+cold+war&ots=kvRphYu1TG&sig=sVpOOZBAdl0fqcHCskio5uy7tiE#v=onepage&q=american%20memory%20of%20the%20cold%20war&f=false.

[2] Dmitri Alperovitch, "Our Work with the DNC: Setting the Record Straight," *Crowdstrike Blog* (blog), June 5, 2020, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[3] Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 4.

Page 1337 of 3957

confidence in democracy.[4] Russia remains a committed adversary as its influence operations continue to this very day, posing an active threat to American democracy.[5]

A. PROBLEM STATEMENT

While "hack and dump" campaigns, such as the 2016 DNC attack and cyberattacks against election infrastructure, are broadly considered Russia influence operations, the Internet Research Agency's social media influence campaign directly targeted voter confidence in election integrity aimed to harm democracy.[6] As Philip Howard, an Oxford researcher, contends, a healthy democracy relies on trustworthy news media and a climate that allows for civil discourse and consensus-building.[7] The IRA's continued onslaught of fake news and amplification of inflammatory content sowed discord and confusion in the United States. For example, Hillary Clinton received damaging publicity during the campaign season in 2016 when the Main Directorate of the General Staff of the Russian Armed Forces (GRU) and Wikileaks continually leaked stolen content from the Democratic National Committee; the IRA magnified the negative image of her through its dissemination of memes and other negative content on social media platforms, which in turn politically damaged her heading into Election Day, and may have delegitimized her presidency had she been elected.[8] Russia understood that attacks against the elections

---

[4] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 4.

[5] Parks and Ewing, "Foreign Interference Persists And Techniques Are Evolving, Big Tech Tells Hill."

[6] Sarah Birch, "Perceptions of Electoral Fairness and Voter Turnout," *Comparative Political Studies* 43, no. 12 (December 1, 2010): 1601–22, https://doi.org/10.1177/0010414010374021; Kellie J. Weir, "Safeguarding Democracy: Increasing Election Integrity through Enhanced Voter Verification" (master's thesis, Naval Postgraduate School, 2018), https://www.hsdl.org/?view&did=811383.

[7] Philip N. Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018* (Oxford, UK: University of Oxford, Computational Propaganda Research Project, 2019), 39, https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs.

[8] Allon J. Uhlmann and Stephen McCombie, "The Russian Gambit and the U.S. Intelligence Community: Russia's Use of Kompromat and Implausible Deniability to Optimize Its 2016 Information Campaign against the U.S. Presidential Election," *Library Trends* 68, no. 4 (2020): 684, https://doi.org/10.1353/lib.2020.0017.

Page 1338 of 3957

struck at the heart of American democracy because this process expresses the people's will and gives the U.S. government legitimacy.[9]

Since the end of 2016, federal agencies and private sector organizations, specifically the major American social media companies, have been actively helping to safeguard political campaigns and election infrastructure from computer intrusions through increased cybersecurity and other security measures.[10] To date, most research has focused on quantitative and qualitative analyses of the IRA's influence campaigns. However, this research has not analyzed how the Russian government itself perceived the effectiveness of the campaigns in achieving their goals. Furthermore, the efficacy of the aforementioned governmental and private sector actions to defend against the IRA's influence campaigns has not been studied much in a methodical fashion. This thesis seeks to use a systematic framework to evaluate the qualitative effectiveness of the Russian disinformation campaigns and the countermeasures taken by the U.S. government and social media companies to combat the aforementioned campaigns targeting the 2020 U.S. elections. In summation, Russian influence operations' continual assault will weaken American democracy over the long term if not effectively countered.

B. RESEARCH QUESTION

To develop effective countermeasures for Russian interference activities targeting future American elections, this thesis seeks to answer the following question: What impact did the countermeasures taken by the American social media companies and the U.S. government have on Russian social media influence campaigns targeting the 2020 U.S. elections?

---

[9] Gregory A. Miller et al., *Critical Democracy Infrastructure: Protecting American Elections in the Digital Age Threats, Vulnerabilities, and Countermeasures as a National Security Agenda*, 2nd ed. (Palo Alto, CA: OSET Institute, 2020), 9, https://trustthevote.org/wp-content/uploads/2020/05/01May20_CDI-2nd.pdf.

[10] Federal Bureau of Investigation, "Protected Voices," Federal Bureau of Investigation, accessed August 5, 2020, https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices; Facebook, "Facebook - Preventing Election Interference," About Facebook, 2020, https://about.fb.com/actions/preventing-election-interference/; Google Threat Analysis Group, "Google Safety & Security," *Google* (blog), accessed May 27, 2020, https://blog.google/technology/safety-security/; Twitter, "Elections Integrity: We're Focused on Serving the Public Conversation," About Twitter, 2020, https://about.twitter.com/en_us/advocacy/elections-integrity.html.

Page 1339 of 3957

C. LITERATURE REVIEW

This literature review analyzes the leading scholarly and expert debates on the Internet Research Agency and other Russia-backed social media activities targeting the U.S. elections from 2014 to 2020, the countermeasures taken by American social media companies and the U.S. government, a framework for understanding the objectives of Russian hybrid warfare, and the recommendations to counter Russian influence activities provided by subject matter experts in a variety of fields. Russian influence campaigns, known as "active measures," have been in existence since the inception of the Soviet Union over 100 years ago.[11] Prior research in this topic drew primarily from the ranks of history, political science, public policy, and international studies. An extensive survey of the current academic literature indicates that the types of researchers drawn to the field of foreign influence campaigns have recently broadened due to the Internet Research Agency's success in employing social media platforms to conduct influence campaigns targeting the 2016 U.S. elections. Presently, scholarly analyses also come from researchers in the fields of computer science, data analytics, and communications. This thesis attempts to evaluate the efficacy of the aforementioned actions to determine if finetuning or a wholesale change in tactics is required to counteract future Russian influence campaigns.

The literature review will be comprised of four parts. The first part examines the studies of Russian online influence campaigns from 2014 to 2020. The sources for this topic include reports and papers by the U.S. government, think tanks, private research firms, academic researchers, and news media. The second part examines the documents which analyze or disclose countermeasures taken by the American social media companies, specifically Facebook, Google, and Twitter, and the U.S. government. The sources include government reports and statements, academic research papers, private research firm reports, think tanks papers, the social media companies' transparency reports, and news media reporting. The third part examines a framework for understanding the objectives of Russian hybrid warfare. The sources primarily include articles and research papers from academic and military institutions. The fourth part examines recommendations for

[11] *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel I: Hearing before the Select Committee on Intelligence*, Senate, 115th Cong., 1st sess., March 20, 2017, 10.

Page 1340 of 3957

countering future Russian online influence campaigns. The sources for this topic include Congressional reports, think tank papers, academic research papers, and private research companies' reports. The literature review has revealed an abundance of source materials covering the activities surrounding the 2016 and 2018 U.S. elections. At the time of this thesis, there have not been many scholarly works published examining Russia's interference against the 2020 U.S. elections.

1. Russian Online Influence Activities from 2014 to 2020

Groups of investigators and scholars provide a critical review and analysis of Russian online influence activities and tactics vis-à-vis the 2016 U.S. election. The U.S. Intelligence Community Assessment (ICA) issued in January 2017 encapsulated the Executive Branch of the U.S. government's consensus judgment that the Russian Federation endeavored to erode public confidence in the U.S. elections and favor one presidential candidate over another.[12] Since that ICA was published, an abundance of literature into the IRA's 2016 to 2020 activities has been written by governmental entities, non-governmental organizations, and academic researchers.

Both the U.S. government's executive and legislative branches conducted investigations into the Russian interference in the 2016 U.S. elections, which included the IRA's social media campaigns. The foundational work detailing the IRA's actions during this timeframe may be the 2019 report from Robert Mueller III, the former FBI Director appointed by the Department of Justice as the Special Counsel to investigate Russian interference in the 2016 U.S. elections.[13] This report resulted from approximately two years of work by the Special Counsel's Office and the analysis of a multitude of evidence collected through legal processes and interviews.[14] Mueller and his team had two main findings regarding the Russian influence campaign. First, the report found that the IRA's

[12] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution* (Washington, DC: Office of the Director of National Intelligence, 2017), 7, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[13] Robert Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: Department of Justice, 2019).

[14] Department of Justice, "Special Counsel's Office," Department of Justice Special Counsel's Office, October 16, 2017, https://www.justice.gov/sco.

Page 1341 of 3957

social media campaign aimed to sow discord in the U.S. elections but pivoted to favoring Donald Trump when it became apparent he would be the Republican presidential nominee.[15] Second, Mueller's team concluded that the hack and dump attack against the DNC was intended to harm Hillary Clinton's presidential campaign.[16]

The intelligence committees for both houses of Congress also issued reports regarding Russian interference in the 2016 U.S. elections. Of the two, the U.S. Senate Select Committee on Intelligence (SSCI) report had bipartisan approval from the committee members when it was published. Its findings coincided with the Special Counsel's report.[17] The U.S. House Permanent Select Committee on Intelligence (HPSCI) report was issued by the Republican majority over the Democratic committee members' dissent. The HPSCI majority and minority reports concluded that the Russians had interfered with the elections through the cyberattack against the DNC and the IRA's social media campaigns.[18] The majority report neglected to mention that these two operations were intended to damage the Clinton campaign and favor the Trump campaign, whereas the minority report highlighted the majority's omission and suggested partisan politics explained the omission.[19]

In August 2020, the State Department's Global Engagement Center published a report, which exposed Russia's current disinformation strategy and tactics.[20] Though the report did not address the Russian activities targeting the 2016 U.S. elections, it described

---

[15] Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 4.

[16] Mueller, 4.

[17] *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures, Campaigns, and Interference In the 2016 U.S. Election, Volume 2: Russia's Use Of Social Media With Additional Views*, Senate, 116th Cong., 1st Sess. (Washington, DC: U.S. Congress. Senate, 2019), 4, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[18] *Report on Russian Active Measures*, 98.

[19] *Report of the House Permanent Select Committee on Intelligence on Russian Active Measures Together with Minority Views*, H.Rept 115–1110 (Washington, DC: Government Publishing Office, 2019), 257, https://www.congress.gov/115/crpt/hrpt1110/CRPT-115hrpt1110.pdf.

[20] Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem* (Washington, DC: Department of State, 2020), https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

Page 1342 of 3957

Russian online influence operations, the online ecosystem that Russia was aiming to cultivate, and framed the IRA's current activities as a continuation of the Russian active measures strategy.[21] The State Department and Special Counsel's Office reports, coupled with the Congressional intelligence committee reports, represented the U.S. government's understanding of Russian disinformation strategy in general and the IRA's role within the broader Russian influence enterprise.

In March 2021, the Office of the Director of National Intelligence (ODNI) issued an unclassified version of the intelligence community assessment summarizing foreign state-sponsored threats to the 2020 U.S. elections.[22] In particular, the ODNI's report provided a succinct but comprehensive overview of the Russian influence campaign, which focused on damaging the Biden presidential campaign and favoring the Trump campaign.[23] In April 2021, the ODNI issued an unclassified version of the Intelligence Community's annual worldwide threat assessment, highlighting Russian influence operations as a persistent threat to the United States.[24] Reporting from the ODNI represents the collective efforts of all 18 organizations which comprise the U.S. Intelligence Community.[25]

Another corpus of literature written by non-governmental and academic researchers tended to be more quantitively detailed in its findings of the IRA than governmental counterparts as they delved into statistical analyses of social media activities. Researchers from the New Knowledge private research firm, now known as Yonder, conducted a comprehensive analysis of the IRA's activities in 2016 and authored a report at the request

---

[21] Global Engagement Center.

[22] Office of the Director of National Intelligence, "Intelligence Community Assessment on Foreign Threats to the 2020 U.S. Federal Elections," Intelligence Community Assessment (Washington, DC, March 16, 2021), https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2192-intelligence-community-assessment-on-foreign-threats-to-the-2020-u-s-federal-elections.

[23] Office of the Director of National Intelligence, 2–5.

[24] Office of the Director of National Intelligence, *2021 Annual Threat Assessment of the U.S. Intelligence Community*, 11.

[25] Office of the Director of National Intelligence, "Members of the IC," Office of the Director of National Intelligence, accessed April 27, 2021, https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

Page 1343 of 3957

of the Senate Select Committee on Intelligence.[26] Renee DiResta and her colleagues conducted a highly detailed qualitative and quantitative analysis of all the social media data submitted to SSCI by Facebook, Google, and Twitter. The data encompassed the IRA's activities from about 2015 to 2018. Their findings regarding the intent of the IRA's social media campaign and the cyberattack against the DNC aligned with the Special Counsel's and SSCI's reports.[27] DiResta et al. go beyond the government reports' findings and conclude that the Russians actively attempted to suppress voter turnout, especially among black voters, and foment insurrectionist sentiment against different levels of American government.[28]

Philip Howard, a University of Oxford researcher, also had the opportunity to analyze the aforementioned social media data provided to SSCI. Howard and his colleagues conducted a statistical analysis of the social media data, to include an in-depth examination of the IRA's strategy and tactics.[29] Howard, who along with Samuel Woolley, had previously coined the phrase "computational propaganda" to describe the IRA's cyber covert operation activities, also found that the IRA's social media campaign was designed to interfere in the 2016 U.S. elections, specifically favoring Trump over Clinton.[30] Their report went further than prior research by describing the specific targeting of different demographic groups to elicit particular responses; i.e., promoting right-wing turnout for Trump, discouraging black voters from voting or civic engagement, and amplifying the differences between the ideologically progressive and conservative.[31]

---

[26] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*.

[27] DiResta et al., 4.

[28] DiResta et al., 8.

[29] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*.

[30] Samuel C. Woolley and Philip N. Howard, "Political Communication, Computational Propaganda, and Autonomous Agents," *National Science Foundation Public Access Repository*, September 3, 2016, 6; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3; Woolley and Howard, "Political Communication, Computational Propaganda, and Autonomous Agents," 3.

[31] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 18.

Page 1344 of 3957

More recently, Robert Walker examined the IRA's online activities in his 2019 master's thesis at the Naval Postgraduate School.[32] His work's primary focus was to evaluate the purpose and impact of the IRA's social media content, coming to the same conclusions as his predecessors.[33] Unlike the previously mentioned researchers, Walker also examined the countermeasures taken by private sector companies and the U.S. government from 2016 to 2018 to assess their impact and found them to be partially effective.[34] These researchers did not have the same political considerations or constraints as governmental investigators to examine and make qualitative judgments about the intent of the IRA's activities and motivations.

Despite a broad agreement within the United States that the Russians attempted to interfere in the 2016 U.S. elections, some conservative American media have disputed the impact these efforts had on the election outcome. In a *New York Magazine* article, Margaret Hartmann, senior editor, stated, "the general consensus is that liberals are overstating the significance of Russia's alleged meddling in an effort to shift the blame for their loss from Hillary Clinton, and undermine Trump's presidency."[35] A 2018 poll taken by British marketing research firm YouGov found that only 37% of Republicans believed Russia interfered with the 2016 U.S. elections.[36] This researcher's extensive literature search could not find any scholars, private research organizations, or prominent conservative think tanks who had authored papers discussing the Russian interference in the 2016 U.S. elections, the Internet Research Agency's social media activities, or policy recommendations for countermeasures. The negative results of this query suggest that this topic did not rate as relevant to these organizations.

---

[32] Robert E. Walker, "Combating Strategic Weapons of Influence on Social Media" (master's thesis, Naval Postgraduate School, 2019), http://hdl.handle.net/10945/62826.

[33] Walker, 69–79.

[34] Walker, 89–100.

[35] Margaret Hartmann, "How Conservatives View Russia's Alleged Meddling in the U.S. Election," *New York Magazine*, December 16, 2016, https://nymag.com/intelligencer/2016/12/how-the-right-is-talking-about-russias-election-meddling.html.

[36] Kathy Frankovic, "Republicans Still Not Convinced of Russian Election Meddling," YouGov, August 10, 2018, https://today.yougov.com/topics/politics/articles-reports/2018/08/10/republicans-still-not-convinced-russian-election-m.

Page 1345 of 3957

2. Countermeasures by the Private Sector and the U.S. Government

The Internet Research Agency appeared to conduct their influence activities undetected on the major social media platforms, specifically those belonging to Facebook, Google, and Twitter, before and during the 2016 U.S. elections.[37] Thus, the social media companies did not pursue any policy changes or take any actions to thwart the influence campaign. In October 2016, the Department of Homeland Security (DHS) and Office of the Director of National Intelligence publicly blamed the Russian Federation for hacking the Democratic National Committee.[38] Subsequently, the FBI and ODNI issued a joint analysis report (JAR), providing more details to the previously published joint statement.[39] The JAR attributed the 2016 DNC hack to two Russian hacking groups, known as APT28 and APT29, and provided technical details to allow organizations to safeguard themselves from these types of computer intrusions.[40] Typically, the U.S. government does not publicly disclose foreign actors' tradecraft because it can reveal sensitive sources and methods used to acquire this information. Likely, the significance of the DNC hack and public pressure prompted the U.S. government to supplement its initial October 2016 statement.[41]

During the time frame after the 2018 U.S. elections and before the 2020 U.S. elections, private research firms and academic research centers played a more prominent role as the social media companies decided to partner with them. These research

---

[37] Cecilia Kang, Nicholas Fandos, and Mike Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill," *New York Times*, October 31, 2017, https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html.

[38] Department of Homeland Security and Office of the Director of National Intelligence, *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security* (Washington, DC: Department of Homeland Security and Office of the Director of National Intelligence, 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[39] Department of Homeland Security and Federal Bureau of Investigation, *GRIZZLY STEPPE – Russian Malicious Cyber Activity* (Washington, DC: Department of Homeland Security and Federal Bureau of Investigation, 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

[40] Department of Homeland Security and Federal Bureau of Investigation, 5–10.

[41] Chris Strohm, "Russian Hacking Began as 'Grizzly Steppe,'" *Chicago Tribune*, December 30, 2016, sec. Nation & World, https://www.chicagotribune.com/nation-world/ct-russian-hack-grizzly-steppe-20161230-story.html.

Page 1346 of 3957

organizations were pivotal in identifying the Internet Research Agency's activities and its various influence campaigns. The two noteworthy organizations were Graphika and the Stanford Internet Observatory. In 2020, Graphika issued a series of reports that exposed Russian influence operations' activities across different platforms. The organization coordinated with the social media companies that shut down IRA-controlled accounts. It discovered that the IRA had made fake left-wing and right-wing news sites to amplify the existing discourse on hot-button topics, such as governmental corruption, gun control, and racial discrimination.[42] The Graphika researchers concluded that the IRA made these sites to help them target people through their ideologies, similar to their tactics in 2016.[43] The Stanford Internet Observatory was led by Alex Stamos, formerly Facebook's Chief Security Officer, and Renee DiResta, one of the researchers retained by SSCI to investigate Russian interference in 2016. The Stanford Observatory collaborated with the social media companies to identify Russian influence campaigns, which the companies would subsequently disrupt through account takedowns and content removal.[44] The Stanford researchers identified influence operations conducted by the GRU and IRA in Africa, which mostly followed prior Russian influence campaign tactics.[45] These two instances showed the social media companies partnering with different research organizations to identify and disrupt various foreign influence campaigns, likely to avoid duplicating efforts and spread the workload.

---

[42] Ben Nimmo et al., "IRA Again: Unlucky Thirteen" (New York, NY: Graphika, September 2020), https://public-assets.graphika.com/reports/graphika_report_ira_again_unlucky_thirteen.pdf; Jack Stubbs, "Exclusive: Russian Operation Masqueraded as Right-Wing News Site to Target U.S. Voters - Sources," Reuters, October 1, 2020, https://www.reuters.com/article/usa-election-russia-disinformation-idUSKBN26M5OP.

[43] Nimmo et al., "IRA Again: Unlucky Thirteen," 24; Stubbs, "Exclusive."

[44] DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*; Stanford Internet Observatory, "Analysis of June 2020 Twitter Takedowns Linked to China, Russia, and Turkey," *Stanford Internet Observatory* (blog), June 11, 2020, https://cyber.fsi.stanford.edu/io/news/june-2020-twitter-takedown.

[45] DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*; Shelby Grossman, Daniel Bush, and Renée DiResta, "Evidence of Russia-Linked Influence Operations in Africa," *Stanford Internet Observatory* (blog), October 30, 2019, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf.

3. Framework for Understanding Russian Hybrid Warfare

The concept of Russian hybrid warfare was devised by Western experts around 2014 to describe Russia's use of conventional military force and unconventional means, specifically cyberattacks and information operations, in its incursions into Crimea, Eastern Ukraine, and Syria.[46] A review of current literature determined that the Russian military officers who are believed to have contributed the most to the Russian hybrid warfare concept were General Valery Gerasimov, Chief of the Russian Federation's General Staff, Lieutenant General S. A. Bogdanov, a retired General Staff officer, and Lieutenant General Andrei V. Kartapolov, currently Russia's Deputy Minister of Defense and the former head of the Russian General Staff's Main Operational Directorate.[47] Of these individuals, Gerasimov was most widely attributed to have created modern Russian hybrid warfare because of a heavily cited article he wrote in February 2013 to describe his thoughts on 21st-century wars.[48] In 2014, a British researcher, Mark Galeotti, coined the term "The

---

[46] Ofer Fridman, "On the 'Gerasimov Doctrine': Why the West Fails to Beat Russia to the Punch," *PRISM* 8, no. 2 (2019): 101.

[47] Viorel Barbu, "The Hybrid War in the East-West Paradigm," in *Strategic Changes in Security and International Relations*, ed. Dorin Corneliu Plesçan et al., vol. XVI, Part 2 (16th International Scientific Conference, Bucharest, Romania: "Carol I" National Defence University, 2020), 101–12, https://www.strategii21.ro/A/2020-04.%20STRATEGIC%20CHANGES%20IN%20SECURITY%20AND%20INTERNATIONAL%20RELATIONS/FSA_2020_VOLUMUL%202.pdf#page=102; Elizabeth Bodine-Baron et al., *Countering Russian Social Media Influence* (Santa Monica, CA: RAND Corporation, 2018), https://doi.org/10.7249/RR2740; Sandor Fabian, "The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy," *Defense & Security Analysis* 35, no. 3 (2019): 308–25, https://doi.org/10.1080/14751798.2019.1640424; Fridman, "On the 'Gerasimov Doctrine'"; Mark Galeotti, "The Mythical 'Gerasimov Doctrine' and the Language of Threat," *Critical Studies on Security* 7, no. 2 (2019): 157–61, https://doi.org/10.1080/21624887.2018.1441623; Krisztian Jojart, "Russia Military Thinking and the Hybrid War," *Scientific Periodical of the Hungarian Military National Security Service*, no. 1 (2019): 82; Nina A. Kollars and Michael B. Petersen, "Feed the Bears, Starve the Trolls: Demystifying Russia's Cybered Information Confrontation Strategy," *The Cyber Defense Review* Special edition (2019): 145–60; Sarah O'Connor et al., *Cyber-Enabled Foreign Interference in Elections and Referendums*, Policy Brief Report No. 41 (Canberra, Australia: Australian Strategic Policy Institute, 2020), https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums; Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *Journal of Slavic Military Studies* 29, no. 4 (2016): 554–75, https://doi.org/10.1080/13518046.2016.1232541; Timothy Thomas, "The Evolving Nature of Russia's Way of War," *Military Review* 97, no. 4 (August 2017): 34–42; Thornton, "The Russian Military's New 'Main Emphasis'"; Wilhelm, "A Russian Military Framework."

[48] Valery Gerasimov, "The Value of Science in Prediction," *Military-Industrial Kurier*, February 27, 2013, https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf.

Page 1348 of 3957

Gerasimov Doctrine" to encapsulate this evolution in Russian military thinking.[49] Over the next five years, the Gerasimov Doctrine was referenced or cited in hundreds of scholarly works.[50] In 2019, Galeotti gave a mea culpa when he clarified that the term was meant to be a placeholder for the changing thoughts about Russian military strategy.[51] Galeotti pointed out that Gerasimov was a career armored division officer and not considered a military science theoretician.[52] Other Russian experts also dismissed the Gerasimov Doctrine as a model for understanding how Russia incorporated information operations into its conventional warfare strategy.[53]

Like Gerasimov, Lieutenant General Bogdanov and a colleague wrote an article about hybrid warfare called the "New Generation War."[54] In this article published in February 2013, Bogdanov discussed the need for information technology and information operations superiority, as it perceived the United States and other Western countries were already using technology-enabled psychological warfare to target Russia.[55] Bogdanov believed these information operations could internally undermine a country's ability to govern and leave it vulnerable to conventional military force.[56] However, since the publication of that article, Bogdanov has not mentioned the term "New Generation War" in his subsequent articles.[57] Later on, Bogdanov would use a different term for hybrid warfare, popularized by Lieutenant General Kartapolov.[58]

---

[49] Galeotti, "The Mythical 'Gerasimov Doctrine' and the Language of Threat."

[50] Galeotti.

[51] Galeotti.

[52] Galeotti.

[53] Fridman, "On the 'Gerasimov Doctrine,'" 101; Fabian, "The Russian Hybrid Warfare Strategy," 311; Kollars and Petersen, "Feed the Bears, Starve the Trolls"; Thomas, "The Evolving Nature of Russia's Way of War."

[54] S.G. Chekinov and S.A. Bogdanov, "The Nature and Content of New Generation War," *Military Thought*, no. 4 (February 2013): 12–23.

[55] Chekinov and Bogdanov; Thomas, "The Evolving Nature of Russia's Way of War," 39.

[56] Kollars and Petersen, "Feed the Bears, Starve the Trolls," 147.

[57] Thomas, "The Evolving Nature of Russia's Way of War," 41.

[58] Thomas, 41.

In 2015, Lieutenant General Kartapolov published an article and gave a speech at the Russian Academy of Military Science about hybrid warfare, which he described as "New-Type Warfare."[59] Specifically, Kartapolov discussed using asymmetric means, such as cyber operations and other forms of political pressure, to weaken an adversarial state's military strength.[60] What differentiates Kartapolov from Gerasimov and Bogdanov was the specific manner in which he laid out the elements for successfully waging New-Type Warfare.[61] Multiple Western scholars consider Kartapolov's article and speech to be a roadmap for the current Russian military thought and practice of hybrid warfare.[62] Figure 1 shows a graphic from the Kartapolov article, which describes the tactics for conducting a New-Type War. In particular, Thomas Wilhelm, an American military scholar, has devised a framework for understanding Russian influence operations based on his analyses of multiple works by General Kartapolov, which will be discussed in further detail in the Research Design section of this thesis.[63]

[59] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods"; Thomas, "The Evolving Nature of Russia's Way of War," 38.

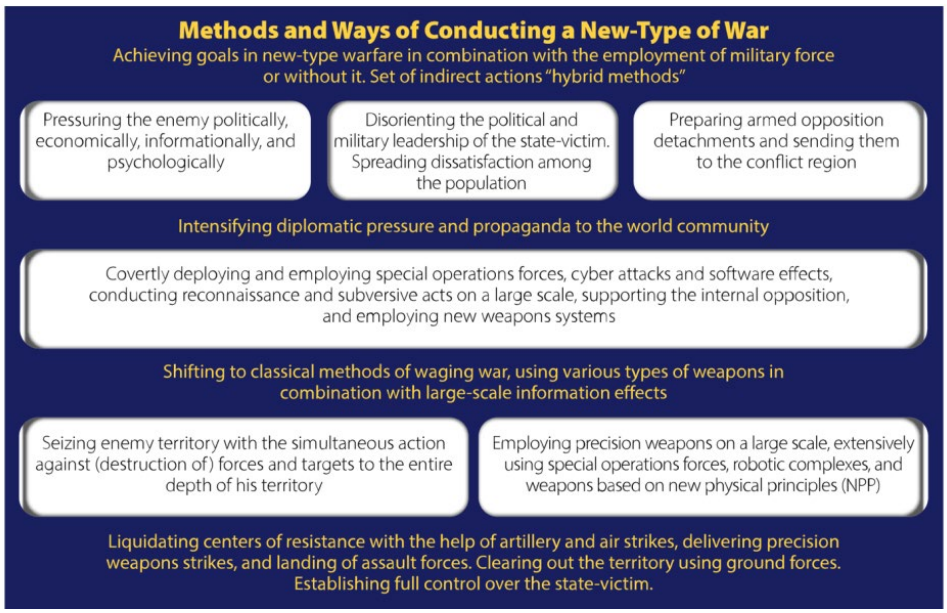
[60] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods"; Kollars and Petersen, "Feed the Bears, Starve the Trolls," 147.

[61] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 35.

[62] Barbu, "The Hybrid War in the East-West Paradigm," 109; Jojart, "Russia Military Thinking and the Hybrid War," 19; Kollars and Petersen, "Feed the Bears, Starve the Trolls," 147; Thomas, "The Evolution of Russian Military Thought"; Thomas, "The Evolving Nature of Russia's Way of War," 41; Thornton, "The Russian Military's New 'Main Emphasis,'" 23; Wilhelm, "A Russian Military Framework," 33.

[63] Wilhelm, "A Russian Military Framework," 33.

Figure 1. Kartapolov's Components for Conducting Hybrid Warfare.[64]



4. Recommendations for Countering Russian Influence Campaigns

Recommendations for countering Russian malign influence operations primarily come from three sectors: (1) the U.S. government, (2) non-governmental organizations such as think tanks, and (3) researchers affiliated with academic institutions. The intelligence committees for both houses of Congress provided recommendations in the reports, which summarized their investigations of Russian interference in the 2016 U.S. elections. The House Permanent Select Committee on Intelligence report's recommendations focused on information sharing between election-related stakeholders, improved cybersecurity for election information infrastructure, and potential legislative actions to enhance cybersecurity.[65] The Senate Permanent Select Committee on Intelligence report's recommendations discussed the Executive Branch using a suite of deterrents to dissuade foreign influence in U.S. elections, such as sanctions, diplomatic pressure, and cyber operations, enhanced cybersecurity measures for election

[64] Source: Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 35; Thomas, "The Evolution of Russian Military Thought," Appendix 1.

[65] H.R., *Report on Active Measures*, 120–22.

infrastructure, and replacing outdated election equipment.[66] All of these recommendations may broadly be characterized as security measures.

Like the Congressional reports, various policy think tanks have proposed a series of recommendations to counter Russian influence campaigns. The RAND Corporation suggested a three-pronged set of activities: (1) targeting the Russian government through sanctions, diplomacy, and pro-democracy programs; (2) identifying and disrupting the activities of the Internet Research Agency and other proxies through information sharing and improved detection technologies; and (3) disrupting the effectiveness of social media amplification channels through technology enhancements and policy changes.[67] Similar to the third prong of RAND's recommendations, the German Marshall Fund was highly focused on improved transparency through better information-sharing between companies and better labeling state-sponsored content.[68] Looking at the environment from a more holistic perspective than RAND or the German Marshall Fund, the Belfer Center advocated for a national strategy for countering information operations, to include increased transparency to attribute and reveal Russian influence operations, leveraging all facets of the U.S. government to disrupt these operations, increased engagement with allies to counter influence operations, and better cooperation between the U.S. government and social media companies.[69] In contrast to the other organizations, the Belfer Center also advocated for improved media literacy in the nation's education system.[70] In summary, the writers' consensus viewpoint from the literature review is that enhanced security, transparency, and resiliency are crucial to combating malign Russian influence in elections.

As another group of outside observers of social media influence campaigns, academic researchers provided practical proposals based on their analysis of the IRA's

---

66 *Russian Active Measures Campaigns: Volume 1*, 55–60.

67 Bodine-Baron et al., *Countering Russian Social Media Influence*, 12.

68 Bradley Hanlon, *A Long Way to Go - Analyzing Facebook, Twitter, and Google's Efforts to Combat Foreign Interference*, Policy Brief No. 41 (Washington, DC: German Marshall Fund of the United States, 2018), 1, https://securingdemocracy.gmfus.org/wp-content/uploads/2018/12/A-Long-Way-to-Go-Analyzing-Facebook-Twitter-and-Googles-Efforts-to-Combat-Foreign-Interference.pdf.

69 Cederberg et al., *National Counter-Information Operations Strategy*, 11–12.

70 Cederberg et al., 12.

Page 1352 of 3957

tactics and activities. These proposals may have added weight because they are in peer-reviewed publications. Both DiResta and Howard's academic research teams, from Stanford University and Oxford University respectively, provided wide-ranging proposals involving collaboration between relevant stakeholders to counter current and future Russian influence campaigns.[71] These recommendations included information sharing between private sector companies and the government, better policing and content moderation by the social media companies, and critically thinking about how future technologies can influence campaigns.[72]

In contrast to DiResta and Howard's teams, researchers from the Harvard Kennedy School concentrated their recommendations on social media companies.[73] Specifically, the Harvard researchers focused on policy improvements for the social media companies concerning increased transparency for taking down content, better content moderation, labeling state-sponsored content, providing links to reliable sources of information, and focusing on their users' rights and privacy.[74] Kate Starbird, a University of Washington researcher, agreed on the critical nature of better content moderation by the social media companies but expressed concern about the potential curtailment of free speech.[75] In a completely different vein, Canadian researchers Barry Cartwright et al. believe advanced

---

[71] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 101; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 40.

[72] DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1–2.

[73] Deen Freelon and Tetyana Lokot, "Russian Disinformation Campaigns on Twitter Target Political Communities across the Spectrum. Collaboration between Opposed Political Groups Might Be the Most Effective Way to Counter It.," *Harvard Kennedy School Misinformation Review* 1, no. 1 (2020): 2, https://doi.org/10.37016/mr-2020-003.

[74] Freelon and Lokot, 2.

[75] Kate Starbird, Ahmer Arif, and Tom Wilson, "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations," *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 2019): 19, https://doi.org/10.1145/3359229.

Page 1353 of 3957

technology, specifically artificial intelligence, will be vital for detecting and combating foreign influence campaigns.[76]

A review of the literature revealed some trends among the different sectors, which provided recommendations. The Congressional recommendations focused on security measures such as enhanced cybersecurity, economic sanctions, and cyber operations.[77] The think tank recommendations ran the gamut from security measures similar to Congressional recommendations to transparency measures, such as promoting public communications about disinformation campaigns by the U.S. government, to resilience measures, such as improved media literacy.[78] Academic literature generally supported the same security, transparency, and resiliency measures favored by think tanks and public policy organizations.[79]

5. Conclusions from Literature Review

A review of all the relevant literature makes clear that Russia has and will continue to persist as an adversarial nation-state seeking to destabilize American democracy. The current online influence campaigns being conducted by Russian actors are an extension of Soviet-era psychological warfare operations, amplified by 21st-century social media platforms. The sources providing recommendations to counter these malign influence operations include academia, private sector, government, think tanks, and other non-

---

[76] Barry Cartwright, George Weir, and Richard Frank, "Fighting Disinformation Warfare with Artificial Intelligence: Identifying and Combatting Disinformation Attacks in Cloud-Based Social Media Platforms," in *CLOUD COMPUTING 2019 Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization*, ed. Bob Duncan et al. (Cloud Computing 2019, Venice, Italy: IARIA, 2019), 73–77, https://www.researchgate.net/publication/333024381_CLOUD_COMPUTING_2019_Proceedings_of_the_Tenth_International_Conference_on_Cloud_Computing_GRIDs_and_Virtualization.

[77] *Report on Russian Active Measures*, 121–27; *Russian Active Measures Campaigns: Volume 1*, 54–57.

[78] Cederberg et al., *National Counter-Information Operations Strategy*, 11–12; William Marcellino et al., *Foreign Interference in the 2020 Election: Tools for Detecting Online Election Interference* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RRA704-2.html.

[79] DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1–2; Darren L. Linvill and Patrick L. Warren, "Engaging with Others: How the IRA Coordinated Information Operation Made Friends," *Harvard Kennedy School Misinformation Review* 1, no. 2 (April 2020): 2, https://doi.org/10.37016/mr-2020-011.

Page 1354 of 3957

governmental organizations. The variety of sources and input indicates that a whole-of-society approach utilizing a range of security, transparency, and resiliency measures will be necessary to combat Russian influence operations.

D. RESEARCH DESIGN

The objectives of this thesis are three-fold: (1) examining the Internet Research Agency and other Russian social media campaigns ahead of the 2020 U.S. elections to determine whether its tactics have shifted since 2016; (2) critically analyzing the private sector and U.S. government's actions to counter the Russian influence activities; and (3) proposing recommendations to safeguard future U.S. elections. The first two objectives will be assessed using an analytical framework proposed by Thomas Wilhelm, Director of the U.S. Army's Foreign Military Studies Office. The last objective will be informed by the results of the first two objectives, as well as a review of current literature by scholars and subject matter experts in different fields.

To design a useful framework for analyzing Russian influence operations, Thomas Wilhelm surveyed the published works and speeches of General Lieutenant Andrei V. Kartapolov. Wilhelm surmised Kartapolov was one of the key architects of current Russian military science and doctrine, specifically the aforementioned "New-Type War."[80] Wilhelm believed the framework provided a well-rounded understanding of Russian martial intent and objectives about hybrid warfare through a Russian perspective.[81] Specifically, Kartapolov advocates utilizing asymmetric, non-violent methods to undermine the strengths of Russia's opponents to achieve their strategic goals.[82] Kartapolov highlighted ten components for conducting hybrid warfare, herein referred to as the Kartapolov Framework: (1) spreading discontent in the population; (2) exerting political pressure; (3) confusing the political leadership; (4) use of new and advanced weaponry; (5) train and arm opposition forces; (6) utilization of special military forces

[80] Tom Wilhelm, "A Russian Military Framework for Understanding Influence in the Competition Period," *Military Review* (2020): 35.

[81] Wilhelm, 38.

[82] Thornton, "The Russian Military's New 'Main Emphasis.'"

Page 1355 of 3957

behind enemy lines; (7) commit large scale subversive acts to destabilize to the enemy; (8) shift to conventional warfare after softening the enemy; (9) destroy the enemy and seize territory concurrently; and (10) use airstrikes and artillery to destroy any focal points of resistance to establish complete control of the territory.[83]

The relevant components of the Kartapolov Framework for analyzing Russian social media-based influence operations against the United States are: (1) spreading discontent in the population; (2) exerting political pressure; and (3) confusing the political leadership.[84] This thesis will use the Kartapolov framework to conduct a qualitative evaluation of the Internet Research Agency's impact and the effectiveness of social media companies and the U.S. government's countermeasures. To assess the social media companies and the U.S. government's actions to counter Russian influence activities, this thesis will also employ the Kartapolov framework. Specifically, the American actions will be analyzed to determine their effectiveness for countering the three influence-related components of the Kartapolov Framework. In particular, a qualitative analysis will evaluate American efforts to counter the spread of discontent in the American populace, defuse political pressure, and stop confusion in political leadership. The analysis will be dependent on publicly available information.

The review of the private sector countermeasures to the IRA's influence campaign will be based on examining three sources of information. Private sector actions, specifically those of the "Big Three" social media companies of Facebook, Google, and Twitter, are tracked and reviewed by academic researchers and non-governmental organizations.[85] These two groups write reports or papers based on their findings. An example of this type of information is a recently published paper examining Twitter's account suspensions related to the 2020 U.S. elections by researchers from the University of New Mexico and

[83] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 35.

[84] Kartapolov, 36.

[85] Ryan Robinson, "7 Top Social Media Sites in 2020," Adobe Spark, accessed July 21, 2021, https://www.adobe.com/express/learn/blog/top-social-media-sites.

Page 1356 of 3957

the Georgia Institute of Technology.[86] The social media companies have also regularly made public announcements of their actions to combat foreign influence activities. These types of information will be used to assess the impact of the private sector's countermeasures.

The review of U.S. government countermeasures will rely only on publicly available, unclassified information. Although classified reporting on U.S. government actions likely exists, these sources will fall outside this thesis's scope. In certain instances, different facets of the U.S. Government generates unclassified reports, such as those produced by the different committees in Congress or various executive branch agencies. In other circumstances, the U.S. government will make public statements or unseal legal documents such as indictments or arrest affidavits. On occasion, the news media will also leverage their sources to reveal U.S. government actions. These types of information will be used to assess the impact of the U.S. government's countermeasures.

Recommendations for safeguarding future U.S. elections will be informed by the aforementioned analyses of actions taken by the private sector and the U.S. government and a review of advice provided by subject matter experts in various fields. These experts comprise academic scholars, researchers from non-governmental organizations, and U.S. government officials from both the legislative and executive branches. The diverse experiences and perspectives should provide a robust set of recommendations for a whole-of-society approach to secure elections.

In summation, the examination of the Internet Research Agency's social media campaigns ahead of the 2020 U.S. elections will rely primarily on exploring literature produced by four groups: academic researchers, non-governmental research organizations, reports from the social media companies, and U.S. government investigatory reports. Although offering different perspectives, these subject matter experts provide the most reliable analysis and assessment of the Russian influence activities.

---

[86] Farhan Asif Chowdhury et al., "Examining Factors Associated with Twitter Account Suspension Following the 2020 U.S. Presidential Election," *ArXiv* 2101, no. 09575 (January 23, 2021), https://arxiv.org/pdf/2101.09575.pdf.

Page 1357 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 1358 of 3957

II. OPENING MOVES – SCOPE AND BACKGROUND

> We're all targets of a sophisticated and capable adversary and we must engage in a whole-of-government approach to combat Russian active measures.
>
> — Richard Burr, March 30, 2017

In the Russian Federation, President Vladimir Putin, who has been in power since 2000, makes every major decision.[87] As a former senior-level KGB officer, Putin holds antagonistic views of liberal democracies in general and the United States in particular.[88] Michael McFaul, former U.S. Ambassador to Russia, assessed that Putin sees the United States as "a hostile power and a serious threat to Russian national interests."[89] As such, Putin perceives himself to be in an ideological struggle "between conservative, Christian, sovereign values—which he embraces—and decadent, liberal, multilateral ideas championed by many Western governments, including first and foremost the United States."[90] Harkening back to Soviet-era information operations, Putin recognized the advent of online social media platforms as an avenue to target U.S. elections.[91] The Russian influence operations started before the 2016 U.S. elections and continued through the 2020 U.S. elections.

Before delving into the nuances of the Russian online social influence campaigns targeting the 2020 U.S. elections, this chapter outlines the scope of the issue to be studied in this thesis, the recent history motivating these influence campaigns, a review of Russian and American measures during the 2016 and 2018 U.S. elections, and an analysis of the effectiveness of these measures using the Kartapolov Framework.

---

87 Timothy J. Colton and Michael McFaul, "Russian Democracy under Putin," *Problems of Post-Communism* 50, no. 4 (July 2003): 13, https://doi.org/10.1080/10758216.2003.11656043.

88 S., *Russian Active Measures*, 14.

89 McFaul, *Securing American Elections*, 11.

90 McFaul, 11.

91 Starbird, Arif, and Wilson, "Disinformation as Collaborative Work," 4.

Page 1359 of 3957

A. SCOPE OF THESIS

The current Russian information operations targeting U.S. elections can trace their roots to Soviet-era propaganda and disinformation campaigns.[92] Because of the immense longevity and scale of these Russian information operations, it is essential to frame what will be discussed within the confines of this thesis. The critical components to be bounded are time periods covered, types of influence operations, and the social media platforms to be examined.

1. Relevant Time Periods

On March 30, 2017, Eugene Rumer, Senior Fellow at the Carnegie Endowment for International Peace, testified before the Senate Select Committee on Intelligence and described active measures as a century-old suite of information warfare tools continuously being used by Russia to advance its ideological objectives and erode the stability of its liberal democratic rivals.[93] The use of disinformation campaigns, i.e., intentionally propagating false or misleading information, is one of the primary tools in their portfolio.[94] Soviet-era active measures evolved and are now "enabled by technology and adapted for a globalized world, their modern incarnations are much more sinister, with far greater range and speed – and, through the Internet, able to influence popular opinion on a scale never before possible."[95] However, it was only around the 2016 U.S. elections when the Russians deployed these large-scale online disinformation campaigns against the American democratic system.[96] Therefore, this thesis will focus on Russian activities from three distinct periods: (1) preceding and during the 2016 U.S. elections, (2) after the 2016 U.S. elections to preceding the 2018 U.S. midterm elections, and (3) after the 2018 U.S. midterm elections to the 2020 U.S. elections.

---

[92] Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections: The Quarterly Journal* 15, no. 1 (2016): 8, https://doi.org/10.11610/Connections.15.1.01.

[93] S., *Russian Active Measures*, 10.

[94] S., *Russian Active Measures*, 10.

[95] Abrams, "Beyond Propaganda," 8.

[96] Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 22.

Page 1360 of 3957

2. Types Of Russian Influence Operations

The Russian influence operations directed at the 2016 U.S. Presidential elections are broadly divided into three categories, the last of which will be within the scope of this thesis.[97] The first category is "hack and dump," wherein Russian hackers breached the DNC computer networks, stole data, and then disseminated it via different online platforms such as WordPress, Twitter, and Wikileaks.[98] The second category is attempted hacks on the actual voting systems in each state. The systems include voter registration databases and online polling equipment. The last category, as described by researchers from New Knowledge, is the "sweeping and sustained" online social media influence campaign perpetrated by the Internet Research Agency "consisting of various coordinated disinformation tactics aimed directly at U.S. citizens, designed to exert political influence and exacerbate social divisions in U.S. culture."[99]

Online social media influence campaigns conducted by the Internet Research Agency and other Russian-backed organizations will be the focus of this thesis because they have a significant and continuing impact on Americans and democracy. In contrast, the other two types of Russian influence operations, focused on political campaigns and election infrastructure, are only germane to Americans every two years during election seasons. Since the 2016 election, federal agencies and private sector organizations have been actively helping to safeguard political campaigns and election infrastructure from computer intrusions through increased cybersecurity and other security measures. Arguably, campaigns and election systems are better protected now than they were in 2016. Though regularly occurring on a biennial basis, American engagement with the electoral process is little compared to their daily, and sometimes hourly, social media engagement.

In 2019, about 70 percent of all Americans had at least one social media account and used the Internet between 30 minutes to two hours per day.[100] This statistic means the

---

[97] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 4.

[98] DiResta et al., 4.

[99] DiResta et al., 4.

[100] J. Clement, "Social Media Usage in the United States," Statista, May 19, 2020, https://www.statista.com/topics/3196/social-media-usage-in-the-united-states/.

Page 1361 of 3957

IRA has daily opportunities to reach out to Americans via social media newsfeeds or posts. Due to First Amendment constraints, federal agencies have little involvement in Americans' usage of social media. Couple this with the fact that social media companies have a vested interest in keeping American users on their platforms. For the most part, Americans are left to fend for themselves on social media platforms.

Research has shown mixed results regarding people's usage of social media. On the one hand, social media usage positively correlates with increased political engagement.[101] On the other hand, users tend to stay on social media platforms longer when engaged with content that conforms to their own opinions, whether factual or not.[102] The social media companies understand this phenomenon and finetune their algorithms to keep feeding content they think users want.[103] The IRA could take advantage of this behavior by inserting itself into the social media ecosystem and working to sow discord and erode the American public's trust in democratic institutions.

3. Targeted Social Media Platforms

Despite a vast array of social media platforms, Russians primarily targeted these three of the four most visited ones: #1 – YouTube, a Google subsidiary, #3 – Twitter, and #4 - Facebook.[104] Wikipedia is the #2 most visited website, but not a social media platform and heavily moderated, unlike the other sites.[105] Whereas previous studies focused on discrete periods around a single election (2016, 2018, or 2020), this thesis will review and analyze Russian activities across the entire time when the IRA and other Russian-backed groups have targeted the United States with its social media influence campaigns. The term,

---

101 Sebastián Valenzuela, "Unpacking the Use of Social Media for Protest Behavior: The Roles of Information, Opinion Expression, and Activism," *American Behavioral Scientist* 57, no. 7 (July 2013): 923, https://doi.org/10.1177/0002764213479375.

102 Armin A. Rad, Mohammad S. Jalali, and Hazhir Rahmandad, "How Exposure to Different Opinions Impacts the Life Cycle of Social Media," *Annals of Operations Research* 268, no. 1 (2018): 88, https://doi.org/10.1007/s10479-017-2554-8.

103 Rad, Jalali, and Rahmandad, 89.

104 DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 6.

105 Joshua Hardwick, "Top 100 Most Visited websites by Search Traffic (as of 2020)," *Ahrefs* (blog), May 12, 2020, https://ahrefs.com/blog/most-visited-websites/.

Page 1362 of 3957

private sector companies, will refer to the three companies whose social media platforms were the most heavily used by the Russians for their influence operations. Understanding the IRA's activities across this period may reveal the efficacy of actions taken by the private sector companies and the U.S. government in response to the IRA's efforts.

B. RECENT HISTORY – THE CAMPAIGNS FROM 2016 TO 2018

Around 2014, Putin tapped his close ally Yevgeniy Prigozhin to conduct influence operations against the American public.[106] Prigozhin, recognized as "Putin's Chef," is a Russian oligarch who owns a conglomerate known as Concord Management, with subsidiaries in various businesses, including catering.[107] Project Lakhta is the umbrella term for Prigozhin-owned firms focused on domestic and overseas influence operations. By September 2016, the monthly operating budget of Project Lakhta was the equivalent of $1.25 million.[108] One of the businesses under Project Lakhta is the Internet Research Agency, founded around 2013 in St. Petersburg, Russia, to be a sophisticated marketing and influence firm. Organized like a legitimate business, its management group oversees various departments, including finance, information technology, search engine optimization, data analysis, and graphics.[109] Before targeting Americans, IRA employees engaged in around-the-clock influence operations directed at Russian and Ukrainian citizens.[110] In April 2014, a new department called the "Translator Project" was formed to conduct online activities against Americans on the American social media platforms of Twitter, Facebook, Instagram, and YouTube.[111] By July 2016, IRA assigned more than 80 employees to the Translator Project.[112] These machinations showed the Russian

---

106 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 5.

107 U.S. vs. Internet Research Agency LLC, No. 18-cr-00032-DLF (U.S. District Court for the District of Columbia February 16, 2018).

108 U.S. vs. Internet Research Agency LLC at 7.

109 U.S. vs. Internet Research Agency LLC at 5.

110 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

111 U.S. vs. Internet Research Agency LLC at 6.

112 U.S. vs. Internet Research Agency LLC at 6.

Page 1363 of 3957

Federation's commitment of personnel and resources to pursue this type of covert online campaigning.

President Putin's initial strategy appeared to be inflaming the existing discord in the American populace and eroding public confidence in American institutions such as free speech and the electoral process. Still, that strategy evolved as it became clear who the nominees would be. By June 2016, Hillary Clinton was the presumptive Democratic nominee and frontrunner for president. Putin was known to despise Clinton during her tenure as Secretary of State during the Obama Administration.[113] She seemed to be the ideological opposite of Putin. Clinton believed in multilateral international cooperation, wanted to strengthen NATO, desired increased sanctions for Russia's occupation of Crimea, and advocated for fair elections and greater freedoms within Russia.[114] Putin may have sensed that Donald Trump's rise as a legitimate candidate offered an avenue to advance his anti-American agenda. Putin's strategy evolved as the presidential campaign season continued through the summer, supporting Trump as its centerpiece.[115] The Russian covert influence operation pivoted to helping the Trump campaign, in addition to its continued efforts to tear down the Clinton campaign.[116] An IRA-purchased political advertisement on Facebook reflected its efforts to target Clinton in Figure 2. This behavior showed the adaptability of the Russians to make use of contemporaneous events for their advantage.

---

[113] McFaul, *Securing American Elections*, 14.

[114] McFaul, 14.

[115] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions*, 7.

[116] Mueller, "Report on The Investigation into Russian Interference in the 2016 Presidential Election," 5.

Figure 2. Facebook Political Advertisement Targeting Hillary Clinton.[117]

1. What Happened During the 2016 U.S. Elections?

The Russian influence campaigns utilizing American social media platforms started around 2013 and extended through the 2016 U.S. elections.[118] Reviewing the Russian measures and the countermeasures taken by the private sector companies and the U.S. government during this time sets up the baseline for comparison to the Russian and American activities during the 2020 U.S. elections. Moreover,

[117] Source: "HPSCI Minority Open Hearing Exhibits," Permanent Select Committee on Intelligence, accessed March 20, 2021, https://intelligence.house.gov/hpsci-11-1/hpsci-minority-open-hearing-exhibits.htm.

[118] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

examining these actions across three separate elections may reveal trends and evolutions in tactics by the Russians and Americans.

a. The IRA's Social Media Activities

Before the 2016 U.S. Elections, the Internet Research Agency's influence operations against the American public encompassed three lines of effort. First, IRA employees made and maintained fake user accounts and pages on social media platforms that covered a range of political issues.[119] For these accounts and pages, the IRA employees generated organic content to ingratiate themselves with online communities and amplify or steer the themes discussed in these communities. Second, IRA employees used social media bots, i.e., computer programs which control social media accounts, to amplify existing content.[120] Third, IRA employees covertly purchased online advertisements from social media companies to enhance their organic content and drive online traffic to sites controlled by them.[121] In the marketing world, advertisements are known as "paid content." In contrast, organic content refers to unpaid messaging generated by people that helped foster support for a product or brand through voluntary and spontaneous recommendations by users.[122] Although the IRA employees were being paid, they impersonated regular users on the social media platforms so their messaging could look authentic. Ironically, Russians masqueraded as Americans and weaponized free speech to foment division and corrode Americans' faith in such speech.

For the first line of effort, the IRA managed its influence operations like a digital marketing campaign.[123] It created false personas and imitated activist groups on the left and right sides of the political spectrum. These personas and groups extended across

---

[119] U.S. vs. Internet Research Agency LLC at 14.

[120] Dhiraj Murthy et al., "Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital," *International Journal of Communication* 10 (2016): 4.

[121] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 17.

[122] Nicole A. Buzzetto-More, "Social Media and Prosumerism," *Issues in Informing Science and Information Technology* 10 (July 2013): 75.

[123] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

multiple social media platforms.[124] Philip Howard, University of Oxford researcher, opined that "users were more likely to assume the credibility of the false organizations set up by the IRA with a presence across multiple platforms, operating websites, YouTube channels, Facebook pages, Twitter accounts, and even PayPal accounts set up to receive donations."[125] Viewers believed these were legitimate because of the extraordinary efforts the personas and groups had taken. To finetune its messaging, IRA employees visited the United States in 2014 to learn about American culture, gather intelligence, and take photographs later used to enhance the authenticity of their false online personas.[126] The care the IRA took showed its deep commitment and calculation in its endeavors to harness American-style free speech to undermine trust in democracy.

When reviewing the IRA-generated Facebook content, some themes emerge. First, on the left end of the political spectrum, the IRA's efforts targeted minority groups to suppress voter turnout.[127] Topics of messaging included anti-government rhetoric, boycotting the election, following the wrong voting procedures, and scaring voters from showing up at polling locations.[128] Figure 3 illustrates an example of IRA-purchased political advertisements on Facebook with anti-government messaging targeting black voters. Second, on the right end of the political spectrum, the IRA promoted conspiracy theories, stopping legal and illegal immigration, protecting gun rights and religious freedom, and other relevant issues for conservatives (see Figure 4).[129] Again, the efforts were presumably targeting conservatives to drive up voter turnout.

---

[124] F. Sattelberger, "Optimising Media Marketing Strategies in a Multi-Platform World: An Inter-Relational Approach to Pre-Release Social Media Communication and Online Searching.," *Journal of Media Business Studies* 12, no. 1 (2015): 66, https://doi.org/10.1080/16522354.2015.1027117.

[125] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 8.

[126] Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 14.

[127] Linvill and Warren, "Engaging with Others," 2.

[128] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3.

[129] Howard et al., 3.

Page 1367 of 3957

Figure 3. Facebook Political Ads Targeting Black voters.[130]

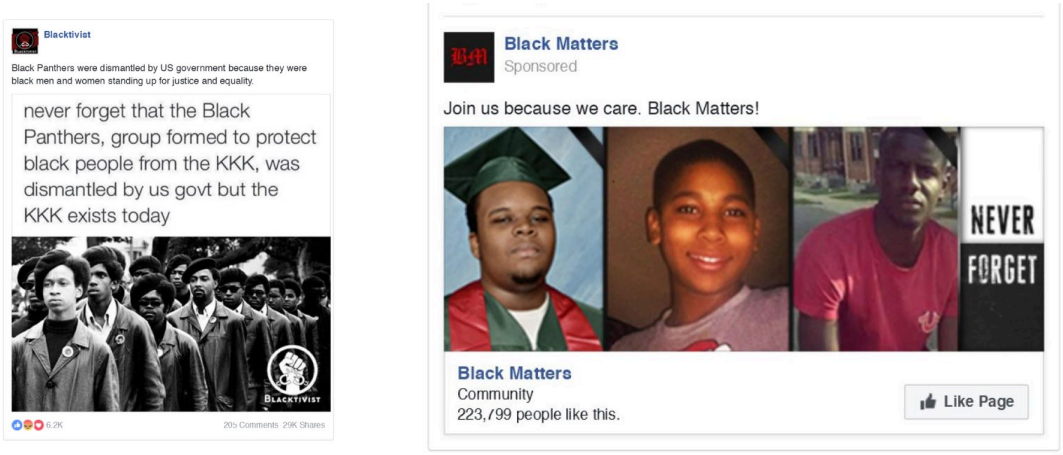
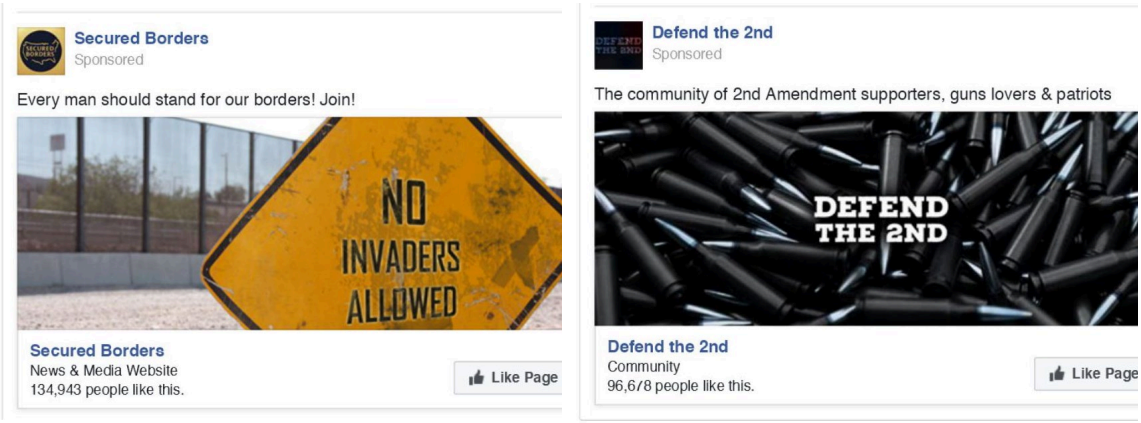


Figure 4. Facebook Political Ads Targeting Right-Wing Voters.[131]



The ratios of IRA-generated content on Facebook changed through the course of 2016. In the first half of 2016, over half of all the most active IRA-made Facebook accounts targeted right-wing audiences with posts discussing the topics referenced above.[132] This phenomenon happened before Trump had won the Republican presidential nomination. Explicit mentions of Trump increased by mid-2016 after he secured the nomination and

130 Source: "HPSCI Minority Open Hearing Exhibits."

131 Source: "HPSCI Minority Open Hearing Exhibits."

132 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 33.

Page 1368 of 3957

focused on amplifying the anti-immigrant rhetoric, which was a hallmark of the Trump campaign.[133] Howard summed up his analysis by stating it was "clear that the IRA sought to energize conservatives around Trump's campaign and encourage the cynicism of other voters in an attempt to neutralize their vote."[134] Howard's examination concluded that the Russians sought to elicit specific behavior, namely encouraging right-wing voters to turn out for Trump and discouraging left-wing and minority voters from going to the polls.[135]

A review of Twitter activities in 2016 showed similar behavior to the IRA's activities on Facebook.[136] In further support of the idea that the IRA treated its influence operations as a marketing campaign, Josephine Lukito, a University of Wisconsin researcher, observed the IRA posting messages on Reddit before similar messages appeared on Twitter.[137] Lukito assessed that the IRA could have been using Reddit to test message resonance before deployment to Twitter.[138] From July 2, 2015 to May 31, 2017, there were about 1.9 million tweets but only 12,603 Reddit posts.[139] Lukita noted that "Twitter's centrality to the IRA's campaign may also explain why more content was produced on Twitter relative to Reddit."[140] Lukita suggested that Reddit's usage may have been a "trial balloon" and opined it could be evidence of the IRA treating their social media influence operation like a marketing campaign.[141] One of the campaign's central goals appeared to be influencing voter turnout during the elections, which was similar to what Philip Howard had concluded.[142]

---

[133] Howard et al., 33.

[134] Howard et al., 32.

[135] Howard et al., 3.

[136] Howard et al., 27.

[137] Josephine Lukito, "Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017," *Political Communication* 37, no. 2 (2020): 249, https://doi.org/10.1080/10584609.2019.1661889.

[138] Lukito, 249.

[139] Lukito, 249.

[140] Lukito, 249.

[141] Lukito, 238.

[142] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 19.

In contrast to the IRA activities on Facebook and Twitter, the YouTube videos provided by Google to the Senate Select Committee on Intelligence revealed that most of them were used to target African Americans.[143] It is unclear why the IRA chose this platform to target African Americans specifically. However, because Google provided only a limited amount of data for public research, making any general conclusions regarding IRA activities on Google's platforms is difficult.[144] YouTube is the most visited site in the United States, mainly used for broadcasting videos.[145] It does not facilitate two-way communications as quickly as the other two platforms.[146] As on the other two platforms, the Senate Intelligence Committee assessed the intent of the YouTube videos might have been to suppress black voter turnout since the YouTube videos were primarily targeted at African Americans.[147]

The sheer magnitude of the IRA's social media campaign targeting the United States was unparalleled in the digital age. Researchers retained by the SSCI estimated the IRA had uploaded over 1,000 videos on YouTube and reached a significant number of American users: 59 percent on Facebook, 19 percent on Instagram, and two percent on Twitter.[148] In table 1, the Special Counsel's Office estimated the number of people reached by a Facebook posting or a Twitter tweet. Although the ultimate number of individual American voters influenced by the IRA remains unclear, table 1 reveals the scale of the reach by the social media platforms.

---

143 Howard et al., 18.

144 Howard et al., 9.

145 Hardwick, "Top 100 Most Visited websites by Search Traffic (as of 2020)."

146 Hardwick.

147 *Russian Active Measures Campaigns: Volume 2*, 6.

148 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

Table 1. Reach of IRA-controlled Social Media Accounts[149]

Social Media Platform	Number of Accounts	Number of Users Reached
Facebook	470	126,000,000
Twitter	3,814	1,400,000

For the second line of effort, the IRA amplified real user accounts whose identities, behavior, and content aligned with the IRA's strategic goals.[150] Clemson University researchers discovered over 100,000 real user accounts amplified by IRA-controlled social media bots.[151] They noted the IRA-targeted accounts with fewer followers for amplification and speculated these types of accounts would generate less scrutiny from the social media companies or perhaps wanted to increase these accounts' prominence to serve their ends. Immediately before and after the 2016 U.S. elections, the IRA changed from generating its own original content to amplifying real users' messages. The IRA may have presumed that real users' posts would be more impactful and resonant with American viewers.[152] This shift showed the IRA's continued evolution to maximize its effectiveness.

For the third line of effort, the IRA purchased online advertisements from the social media companies to complement its other activities.[153] In 2016, the IRA spent about $100,000 on Facebook and $5,000 on Google.[154] Twitter noted that the Kremlin-controlled media site, Russia Today, spent about $274,000 in online advertisements to

149 Adapted from Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 15.

150 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 26.

151 Linvill and Warren, "Engaging with Others," 3.

152 Linvill and Warren, 3.

153 U.S. Congress. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns: Volume 2*, 7.

154 Patrick Savage, *Russian Social Media Information Operations: How Russia Has Used Social Media to Influence U.S. Politics* (Washington, DC: American Security Project, 2017), 1, https://www.hsdl.org/?view&did=808713.

promote over 1,800 tweets on its platform.[155] The IRA was very tactical in its advertising campaign. Using "race, ethnicity, and self-identity" as categories allowed it to use Facebook and Instagram to target specific demographic groups.[156] Then, it would run advertising targeting each of these demographic groups to drive users to IRA-created social media content.[157] The IRA employed different tactics for the purchase of Google online advertisements. In this case, Google ads guided users to various IRA-controlled websites and domains.[158] Marketing research indicates organic content has more resonance than paid content (i.e., advertisements).[159] Since the IRA's online advertising campaign primarily drove users to the organic content, evaluating its success is difficult. The Senate Select Committee on Intelligence concluded that the advertisements were not a vital component of the IRA's campaign.[160] However, the IRA used different techniques to further its social media influence operation, showing flexibility and adaptability.

b. Private Sector Countermeasures

In broad terms, organizations may take three categories of actions to counter influence operations: security, transparency, and resiliency. Security measures involve the monitoring, detection, and neutralization of threats. Transparency measures comprise information sharing to relevant stakeholders, whether between organizations, organizations and individuals, or the general public. Transparency measures also promote trust by allowing people to see what is going on. Finally, resiliency measures involve taking steps to be able to recover quickly from adverse situations.

During and immediately after the 2016 U.S. elections, the Big Three social media companies of Facebook, Google, and Twitter were utterly unaware of the IRA's massive

---

155 Savage, 1.

156 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 17.

157 Howard et al., 17.

158 Howard et al., 17.

159 Buzzetto-More, "Social Media and Prosumerism," 75.

160 S., *Russian Active Measures Campaigns: Volume 2*, 7.

Page 1372 of 3957

influence campaign across all of their platforms.[161] The social media companies had no countermeasures in place to mitigate or disrupt the IRA's activities. Even if they had been aware, whether the social media companies would have taken any serious actions cannot be known for sure. Comments from Mark Zuckerberg, Founder and Chief Executive Officer of Facebook, on November 11, 2016, exemplified the companies' mindset when he famously said the notion that fake news would have any impact on the presidential elections was "a pretty crazy idea."[162] The social media companies took no security, transparency, or resilience measures. Ultimately, they offered no resistance to the IRA's malign activities during the 2016 U.S. elections.

c. U.S. Government Countermeasures

The private sector and U.S. government's efforts were disconnected ahead of the 2106 elections. Although U.S. government agencies, such as the FBI, monitored Russian influence operations, none of their acquired intelligence was relayed to the social media companies to protect their platforms.[163] Ambassador McFaul noted that cooperation between the technology companies and the U.S. government was "almost non-existent" before the 2016 U.S. Elections in the post-Snowden leak era.[164] This condition showed an almost complete lack of transparency between the two entities.

The U.S. government's attempts at security or transparency measures did not come until late into the presidential campaign season. The first official statement regarding the 2016 elections from the U.S. government came on October 7, 2016, when the Department of Homeland Security and Office of the Director of National Intelligence issued a one-page joint statement attributing the hack of the DNC and multiple hacking attempts against state election infrastructure to the Russian Federation.[165] However, the statement provided no technical details and only general cybersecurity guidance. The joint statement's intended

---

[161] McFaul, *Securing American Elections*, 43.

[162] Shahani, "Zuckerberg Denies Fake News on Facebook Had Impact on The Election."

[163] McFaul, *Securing American Elections*, 43.

[164] McFaul, *Securing American Elections*, 43.

[165] "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security."

Page 1373 of 3957

effect may have been to inform the American electorate of malign actions being taken by Russia. Though such an effect was probably diminished because on the same day, the media was focused on the breaking news that Donald Trump had made lewd comments about women to Entertainment Tonight reporter Billy Bush in 2005 when the *Washington Post* released a video of their conversation.[166]

The second set of transparency and security-related actions from the U.S. government came on December 29, 2016, which was well after the elections. As an act of transparency, the FBI and DHS issued a joint action report titled "GRIZZLY STEPPE—Russian Malicious Cyber Activity." The report provided an overview of the Russian hacking activities ahead of the election and shared technical details.[167] If the U.S. government had provided this information ahead of the elections, especially the technical details, it could have helped political organizations and campaigns safeguard their computer networks and electronic devices. As another security and transparency action by the U.S. government, the Department of the Treasury publicly sanctioned nine Russians and two Russian intelligence agencies, the Federal Security Service (FSB) and the General Military Intelligence Directorate, for election-related cybercrimes.[168] It also sanctioned two Russian hackers for financial cybercrimes under the same executive order (E.O. 13694).[169] The purpose of these sanctions was to expose the American public to all of the Russian activities directed against the U.S. elections. Other sanctions such as those imposed by the Magnitsky Act have illuminated Russian oligarchs' and bureaucrats' corrupt financial dealings while relinquishing their ill-gotten funds.[170] Although these actions showed a proportional response from the U.S. government, the effect of such

---

166 THR Staff, "Donald Trump Caught on Hot Mic in 2005 Talking About Women: 'When You're a Star, They Let You Do It,'" News, Hollywood Reporter, October 7, 2016, https://www.hollywoodreporter.com/news/donald-trump-caught-hot-mic-936343.

167 Department of Homeland Security and Federal Bureau of Investigation, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*.

168 Dianne E. Rennack, *U.S. Sanctions on Russia: An Overview*, CRS Report No. IF10779 (Washington, DC: Congressional Research Service, 2018), https://www.hsdl.org/?view&did=813693.

169 Rennack.

170 Julia Ioffe, "Why Does the Kremlin Care So Much about the Magnitsky Act?," *The Atlantic*, July 27, 2017, https://www.theatlantic.com/international/archive/2017/07/magnitsky-act-kremlin/535044/.

actions as a deterrent for future Russian meddling in U.S. elections remains indeterminate. U.S. economic sanctions imposed after the annexation of Crimea did not deter Russia from its occupation of certain parts of Eastern Ukraine but may have curtailed further encroachment into Ukraine.[171]

During this period, the last transparency action from the U.S. government came on January 6, 2017, when the ODNI issued a supplemental report to the previously published GRIZZLY STEPPE report. This report aimed to lay out the U.S. government's analytical process and provide additional details justifying the attribution of election interference to the Russian Federation.[172] Unfortunately, whether this belated disclosure meaningfully affected public discourse or Americans' understanding of the activities surrounding the 2016 U.S. Elections is nebulous at best.

d. Using the Kartapolov Framework to Evaluate Russian & American Measures in 2016

As mentioned in the Research Design section, Thomas Wilhelm, Director of the U.S. Army's Foreign Military Studies Office, developed a framework to understand how asymmetric techniques fit within the Russian philosophy of warfare to achieve its goals. This framework was inspired by Wilhem's analysis of the writings and speeches of Russian Deputy Minister of Defense, Andrei V. Kartapolov.[173] Using the Kartapolov Framework offers an organized structure to evaluate the effectiveness of the Russian measures and American countermeasures. As a reminder, the relevant elements of the Kartapolov Framework for analyzing Russian social media-based influence operations against the United States are: (1) spreading discontent in the population; (2) exerting political pressure; and (3) confusing the political leadership.[174] These elements will be used to gauge the effectiveness of the Russian measures targeting the 2016 elections. In addition, the

---

171 Nigel Gould-Davies, "Russia, the West and Sanctions," *Survival* 62, no. 1 (January 2, 2020): 19, https://doi.org/10.1080/00396338.2020.1715060.

172 Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions*.

173 Wilhelm, "A Russian Military Framework," 35.

174 Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 36.

Page 1375 of 3957

American countermeasures will be assessed in terms of their effectiveness in mitigating the aforementioned elements.

The critical elements of the Kartapolov Framework can easily be superimposed on the 2016 activities of the IRA's campaign in a step-by-step fashion.[175] The first element, spreading discontent in the population, described the IRA's precise method of targeting different demographic groups with fake content, amplifying actual user content, and purchasing advertising. Researchers concluded that IRA's tailored messaging aimed to motivate conservatives to vote while suppressing liberals, specifically black voters.[176] A record number of Americans voted in 2016, but Black voter turnout dropped from its 2012 levels.[177] Table 2 below illustrates the decreased Black voter turnout levels. The Pew Research Center said voter turnout percentages among the other racial demographics stayed about the same.[178]

Table 2. Comparison of Black Voter Turnout for Presidential Elections.[179]

Election Year	Black Voter Turnout
2012	66.6%
2016	59.6%
Change	**-7.0%**

A direct correlation between the IRA's activities and lower Black voter turnout cannot be determined within the scope of this thesis. American voters' motivations to vote

175 Wilhelm, "A Russian Military Framework," 35.

176 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 39.

177 Jens Manuel Krogstad and Mark Hugo Lopez, "Black Voter Turnout Fell in 2016, Even as a Record Number of Americans Cast Ballots," FactTank: News in the Numbers, May 12, 2017, https://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/.

178 Krogstad and Lopez.

179 Adapted from Krogstad and Lopez.

Page 1376 of 3957

or not vote are myriad and not always easy to discern. Chryl Laird, Bowdoin College professor, suggested that Black voter turnout fell in 2016 because the Black community did not have the same incentives to vote as they did in 2008 and 2012 when there was a Black candidate for president.[180] It is still unclear whether the IRA's operation contributed to the record number of Americans voting or suppressing turnout among Black voters in 2016. What is clear is that the IRA deliberately intended to influence American voters' behavior regarding the elections and possibly eroded their faith in the electoral process.

For the second element of the framework, exerting political pressure, the IRA's efforts seemed to impact the U.S. government as its responses appeared delayed and muted. After the Senate Intelligence Committee issued its report reviewing the response of the Obama Administration to the Russian interference, Senator Richard Burr commented that they were "frozen by 'paralysis of analysis,' hamstrung by constraints both real and perceived; Obama officials debated courses of action without truly taking one."[181] In this report, the Senate Intelligence Committee noted that the FBI and DHS did not provide the general public or state and county election officials with notifications about the malicious cyber activities until the late summer of 2016.[182] Because the activities were not attributed to Russia, these notifications would not have drawn much scrutiny.[183] The third element of the framework, confusing political leadership, appeared in one of the SSCI report findings, which noted that government officials were conflicted about making public announcements for fear of feeding the political narratives about insecure or fraudulent elections.[184]

The social media companies were utterly caught by surprise and had no awareness of the malign Russian influence activities on their platforms. As such, they did not take any

---

[180] Chryl Laird, "Why Black Voter Turnout Fell in 2016," Vox, January 15, 2020, https://www.vox.com/mischiefs-of-faction/2018/1/15/16891020/black-voter-turnout.

[181] Tucker Higgins, "Obama Response to 2016 Russian Election Meddling Had 'many Flaws,' Senate Report Finds," CNBC, February 6, 2020, https://www.cnbc.com/2020/02/06/obama-response-to-2016-russian-meddling-had-many-flaws-senate-report.html.

[182] *Russian Active Measures Campaigns: Volume 1*, 4.

[183] S., *Russian Efforts against Election Infrastructure*, 4.

[184] S., *Russian Efforts against Election Infrastructure*, 4.

action against the Internet Research Agency's influence campaign in 2016. Instead, these companies allowed the IRA free rein to achieve the relevant elements of the Kartapolov Framework. However, later on, intense pressure from U.S. lawmakers and the media would eventually force the social media companies to examine what had taken place on their platforms and strive to ensure it did not happen in the future.[185]

Reviewing the U.S. government's countermeasures through the Kartapolov Framework revealed its ineffectiveness to counter the Internet Research Agency's efforts. For the first element of the framework, the IRA had an unfettered ability to conduct information operations on social media and spread discontent throughout the American population. Not until October 2016 did the U.S. government take any action. However, the one-page statement from DHS and the ODNI attributing election interference to Russia did not make an impression with Americans as news media reporting on the tawdry revelations of the Trump discussion on the Entertainment Tonight video and the hacked emails from John Podesta likely overwhelmed all other news coverage.[186]

For the second element, the Russian activities appeared to exert tremendous political pressure on the Obama White House. Multiple news media outlets reported that in the summer of 2016, President Obama was reluctant to take explicit actions because he did not want to appear to be influencing the election in favor of Clinton.[187] By the same token, the third element involved confusing the political leadership. Whether the IRA's tactics perplexed the Obama administration is moot because the delayed governmental

---

185 *Report on Russian Active Measures*; *Report of the House Permanent Select Committee*; March 20, 2017; *Russian Active Measures Campaigns: Volume 1*; *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, S.Rpt. 115–21 (Washington, DC: Government Publishing Office, 2018), https://www.hsdl.org/?view&did=806949; *Mass Violence, Extremism, and Digital Responsibility: Hearing before the Committee on Commerce, Science, and Transportation*, Senate, 116th Cong., 1st sess., September 18, 2019, https://www.commerce.senate.gov/2019/9/mass-violence-extremism-and-digital-responsibility.

186 Devlin Barrett and Damian Paletta, "FBI Suspects Russia in Hack of John Podesta Emails," *Wall Street Journal*, October 12, 2016, https://www.wsj.com/articles/top-russian-officials-shift-away-from-denying-dnc-hack-1476295233; THR Staff, "Donald Trump Caught on Hot Mic in 2005 Talking About Women."

187 Philip Ewing, "FACT CHECK: Why Didn't Obama Stop Russia's Election Interference In 2016?," National Public Radio, February 21, 2018, https://www.npr.org/2018/02/21/587614043/fact-check-why-didnt-obama-stop-russia-s-election-interference-in-2016.

Page 1378 of 3957

response represented the result that the Russians would have desired. The U.S. government's actions in the form of the FBI/DHS joint report detailing Russian activities and the Treasury Department's economic sanctions did not come until well after the elections had already been decided. The U.S. Intelligence Community assessed that Putin and Russia perceived their ability to shape the American discourse and influence the outcome of the 2016 U.S. Elections to be at least a "qualified success" and that there would be little negative impact to continuing their online operations.[188]

Evaluating the Russian and American efforts using the Kartapolov Framework for this period revealed that Russia was the ultimate winner of the 2016 U.S. elections. The IRA's social media campaign had fulfilled the Kartapolov Framework's core tenets of spreading discontent in the population, exerting political pressure, and confusing political leadership.[189] The American efforts ranged from non-existent, in the case of the social media companies, to ineffective, in the case of the U.S. government.

2. What Happened During the 2018 U.S. Midterm Elections?

After the 2016 U.S. Elections, the Internet Research Agency's online operations continued unabated through the 2018 U.S. Elections.[190] Analyzing the IRA's activities and the countermeasures taken by the private sector companies and the U.S. government revealed how their tactics have evolved. The effectiveness of the Russian and American measures was evaluated using the Kartapolov Framework.

a. The IRA's Social Media Activities

Despite being outed by the media and the U.S. government in late 2016, the IRA appeared to operate without interruption at almost the same levels in 2017 and 2018. This success indicated that the IRA continued to be a well-financed organization and a

188 Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions*, 5.

189 Wilhelm, "A Russian Military Framework," 35.

190 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3.

Page 1379 of 3957

seemingly worthwhile investment for Yevgeniy Prigozhin, Putin's close ally.[191] The IRA's financial strength is shown in Table 3. Given the power structure in Russia, Putin likely knew of and approved of these activities.[192] From his perspective, Putin had won the battle of 2016 and wanted to continue the social media campaign as part of the ideological struggle between Russia and the United States.[193]

Table 3. IRA Spending Plan for 2017 and 2018.[194]

Year	Budget
2017	$12,000,000
2018	$10,000,000 (January through June)

Oxford researcher Philip Howard observed the IRA taking advantage of prominent events by timing its online advertising purchases to coincide with events such as the announcement of the Trump tax plan and U.S. military strikes in Afghanistan and Syria.[195] This development may suggest the IRA had honed its skills to cater to the users it engaged. A second reason could be that the IRA shifted much of its social media activities from Facebook to Instagram. Because Instagram is more image-focused, it could be more conducive to the meme operations which the IRA appeared to favor. In addition, Instagram recognized the importance of meme campaigns and hired a manager focused solely on the

191 Peter Laurence, "Powerful 'Putin's Chef' Cooks up Murky Deals," *BBC News*, November 4, 2019, Online edition, sec. Europe, https://www.bbc.com/news/world-europe-50264747.

192 *Report on Russian Active Measures*, 1.

193 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 99.

194 Adapted from DiResta et al., *The Tactics & Tropes of the Internet Research Agency*; Department of Justice, "Russian National Charged with Interfering in U.S. Political System," United States Attorney's Office Eastern District of Virginia, October 19, 2018, https://www.justice.gov/usao-edva/pr/russian-national-charged-interfering-us-political-system.

195 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3.

Page 1380 of 3957

meme community.[196] Lastly, DiResta stated that groups of low-paid workers, known as click farms, could have been used by the IRA to fraudulently make their Instagram accounts more prominent than they otherwise would have been through organic user engagement.[197]

An analysis of the IRA's Twitter activities from 2014 to 2018 uncovered the sophistication used to target distinct online communities. Specifically, the IRA targeted people from different demographic groups based on their political issues of interest[198] Approximately half of all the tweets from the IRA-controlled accounts happened in 2017.[199] This targeted approach indicated a certain mastery of the platform and seemed to be focused on fomenting dissension among the different groups identified by the IRA.

The IRA continued using online advertising through 2017 before social media companies adjusted their ad purchasing policies, effectively shutting them out.[200] Thus, at least through 2017, the IRA's tactics appeared to be relatively unchanged. Ostensibly, the IRA's continued social media activities on these platforms were meant to set the stage for influencing voter opinions and turnout ahead of the 2018 U.S. Midterm Elections and beyond.

b. Private Sector Countermeasures

Before the 2018 U.S. Midterm Elections, Facebook, Google, and Twitter announced they had taken substantive actions and policy changes to address malign foreign influence and election integrity issues on their platforms.[201] These actions seemed to be

---

196 Heather Leighton, "For Instagram's 10th Birthday, Experts Predict The Future Of Meme Culture," *Forbes*, October 7, 2020, https://www.forbes.com/sites/heatherleighton/2020/10/07/for-instagrams-10th-birthday-experts-predict-the-future-of-meme-culture/.

197 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 8.

198 Freelon and Lokot, "Russian Disinformation Campaigns on Twitter Target Political Communities across the Spectrum. Collaboration between Opposed Political Groups Might Be the Most Effective Way to Counter It.," 3.

199 Freelon and Lokot, 3.

200 Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security"; Twitter, "Elections Integrity."

201 Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security"; Twitter, "Elections Integrity."

Page 1381 of 3957

focused on security and transparency measures. Facebook and Twitter appeared to be the most detailed in sharing their changes and the most public about account takedowns. A possible reason could be that Facebook and Twitter faced more Congressional scrutiny than Google as their senior executives testified before Congress on three separate occasions before the midterm elections.[202] In one of the hearings, Google was also in attendance but appeared more circumspect about account takedown notifications because it did not observe as many IRA-controlled accounts on YouTube.[203] In fact, Google only announced the takedown of one IRA-controlled YouTube account ahead of the 2018 midterm elections.[204]

Facebook stated it took a series of measures to protect its platform: (1) "better collaboration with governmental, non-governmental, and technology companies to identify and disrupt new threats; (2) hiring fact-checking organizations to review content and; (3) improved technological methods for detecting fake accounts."[205] Facebook also changed its advertising purchasing policies to make the buyers transparent and maintains a library of purchased political advertisements. Most notably, Facebook began to publicize its detection and takedowns of fake accounts and pages. In 2018, Facebook announced three takedowns totaling 597 Facebook pages, 287 Facebook accounts, and 99 Instagram accounts.[206] Thus, whether bowing to political pressure or genuinely wanting to reform, Facebook appeared to take tangible actions to combat foreign influence campaigns.

Google and Twitter also took countermeasures ahead of the 2018 U.S. midterm elections. For example, Google announced improved cybersecurity measures to protect

---

[202] Kang, Fandos, and Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill"; Tony Romm, "5 Things We Learned When Facebook, Google, and Twitter Testified to Congress About Russia's Election Meddling," Recode Daily, October 31, 2017, https://www.vox.com/2017/10/31/16588032/facebook-google-twitter-congress-russia-election-2016-tech-hearings-franken-cruz-graham; Katy Steinmetz, "Lawmakers Hint at Regulating Social Media During Hearing with Facebook and Twitter Execs," *Time*, September 5, 2018, https://time.com/5387560/senate-intelligence-hearing-facebook-twitter/.

[203] Kang, Fandos, and Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill."

[204] Google Threat Analysis Group, "Google Safety & Security."

[205] Facebook, "Facebook - Preventing Election Interference."

[206] Facebook.

Page 1382 of 3957

political campaigns and their platforms.[207] During the same year, Twitter indicated its efforts included improving its algorithms to detect and takedown social media bots, establishing an internal cross-functional team to handle foreign influence threats, modifying its advertising policies to promote buyer transparency, updating its terms of service to ban all inauthentic behavior, and enhancing the security configuration settings for the application programming interface.[208] In addition, Twitter highlighted its intelligence sharing with Jigsaw, Google, other social media companies, and law enforcement agencies.[209] In October 2018, Twitter released an archive of foreign-influence-related account information so "members of the public, governments, and researchers can investigate, learn, and build media literacy capacities for the future."[210] In 2018, Twitter announced the takedown of 3,613 IRA-associated accounts.

On the one hand, Google's response to the Russian influence campaigns appeared to be subdued, likely because YouTube had not played a significant role in the IRA's playbook for 2016. For example, Howard noted that Google only provided 228 YouTube 2016 election-related videos to the Senate Intelligence Committee, and each video was viewed about 1,500 times or less.[211] On the other hand, Twitter's response was similar to Facebook's and made substantive efforts to combat malign foreign influence on its platform. As a result, the number of accounts taken down by Facebook and Twitter in 2018 was roughly commensurate with the number of accounts discovered after the 2016 U.S. elections. The reason for this disparity in the number of IRA accounts on each platform is indeterminate.

---

[207] Google Threat Analysis Group, "Google Safety & Security."

[208] Carlos Monje Jr., "2018 U.S. Midterm Elections Review," *Twitter Company* (blog), January 31, 2019, https://blog.twitter.com/en_us/topics/company/2019/18_midterm_review.html.

[209] Twitter, "Elections Integrity."

[210] Twitter, "Retrospective Review Twitter, Inc. and the 2018 Midterm Elections in the United States," Twitter, February 4, 2019, https://blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf.

[211] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 7, 11.

c. U.S. Government Countermeasures

Before the 2018 U.S. midterm elections, the U.S. government took a series of public actions to address Russia's interference in the 2016 U.S. elections and put countermeasures in place to ensure better protection in subsequent elections. These actions comprised both transparency and security measures. Transparency-focused efforts aimed to inform the American electorate about what happened in 2016 and was still occurring. Jennifer Hochschild, a Harvard College professor, believed "democracies thrive best…if citizens have a broad education and some level of political knowledge."[212] Americans should have access to information that is free of corrupt foreign influence to inform their voting. The security-focused actions were intended to deter and punish Russian interference in the U.S. electoral process or safeguard their intended targets. These actions took the form of Congressional hearings, an FBI initiative, multiple indictments, economic sanctions, and other operations. Unlike in the lead-up to the 2016 U.S. elections, the U.S. government was very active and public in enacting countermeasures before the 2018 U.S. midterm elections. These actions are described below in chronological order.

On August 31, 2017, the State Department announced the closures of the Russian Consulate in San Francisco and annexes in New York City and Washington, D.C.[213] These closures were taken in response to Russia reducing the size of the American workforce at the U.S. Embassy in Moscow, which was perceived as a retaliatory measure for the United States sanctioning multiple Russians in December 2016 for their interference in U.S. Elections.[214]

On October 31, 2017, the Senate Judiciary Committee held a hearing with senior executives from Facebook, Google, and Twitter to discuss the extent of the Russian disinformation campaigns on their respective platforms.[215] This public hearing was one

---

[212] Jennifer Hochschild, "If Democracies Need Informed Voters, How Can They Thrive While Expanding Enfranchisement?," *Election Law Journal: Rules, Politics, and Policy* 9, no. 2 (2010): 111–23.

[213] Department of State, "Senior Administration Official on Russia," U.S. Department of State, August 31, 2017, https://2017-2021.state.gov/senior-administration-official-on-russia/.

[214] Rennack, *U.S. Sanctions on Russia*.

[215] Romm, "5 Things We Learned When Facebook, Google, and Twitter Testified to Congress About Russia's Election Meddling."

Page 1384 of 3957

of America's first opportunities to hear about what happened from the U.S. social media companies. It also provided politicians with the occasion to exert pressure on the companies to make constructive changes to their platforms.

In December 2017, Congress reestablished the Global Engagement Center (GEC) as an agency within the State Department responsible for countering foreign state and non-state propaganda and disinformation operations.[216] Previously, the GEC was established under Executive Order 13721 in the Obama administration to counter foreign terrorist propaganda and online recruitment efforts.[217] It would later pivot to focusing on exposing foreign state disinformation campaigns.

On January 29, 2018, the FBI announced its Protected Voices Initiative. FBI Director Christopher Wray said it "provides tools and resources to political campaigns, companies, and individuals to protect against online foreign influence operations and cybersecurity threats."[218] Under the auspices of the initiative, the FBI provided cybersecurity briefings to, and stayed engaged with, the national-level political organizations. This security-based countermeasure was focused on protecting one of the primary targets for Russian information operations.

On February 16, 2018, the Special Counsel's Office indicted Yevgeniy Prigozhin and 12 employees of the IRA with eight criminal counts for their efforts to interfere in the 2016 U.S. Elections.[219] The unsealed indictment affidavit offered the first opportunity for the American public to learn about the extent of the scope and scale of the Russian influence operation. The unsealed indictment affidavit described in evidence-based detail what the IRA had propagated on social media against the American public. The accompanying arrest warrants showed the U.S. government's intention to bring these Russians to face justice at some point.

---

216 Matthew Weed, *Global Engagement Center: Background and Issues*, CRS Report No. IN10744 (Washington, DC: Congressional Research Service, 2017), 2, https://fas.org/sgp/crs/row/IN10744.pdf.

217 Weed, 2.

218 Federal Bureau of Investigation, "Protected Voices."

219 U.S. vs. Internet Research Agency LLC.

On March 28, 2018, the Department of Treasury levied sanctions against 16 Russian nationals for election interference-related activities. These included some of the individuals mentioned above whom the Special Counsel's Office previously indicted. In addition, on June 11, 2018, another eight Russian nationals were sanctioned for associated activities.[220] These were another set of measures likely designed to inflict punishment on the Russian actors and act as a deterrent for future activities targeting U.S. elections.

On April 10–11, 2018, the Senate Commerce Committee and Senate Judiciary Committee held hearings on consecutive days with Mark Zuckerberg to discuss Russia's influence campaigns on Facebook and its countermeasures to combat them.[221] This hearing provided the American public with the opportunity to listen to one of the primary architects of the current social media landscape in the United States. The Senate committees also used this as an opportunity to hold Facebook accountable for its actions and exert pressure for positive change.

On July 17, 2018, the House Judiciary Committee held a hearing with senior executives from Facebook, Google, and Twitter so they could provide updates on their companies' efforts for content filtering to stop foreign influence campaigns on their platforms.[222] On September 5, 2018, the Senate Intelligence Committee held a hearing with senior executives from Facebook and Twitter to discuss their companies' efforts to stop foreign influence campaigns and illegal transactions on their platforms.[223] Both of these hearings were additional occasions for Americans to learn about social media companies' progress in safeguarding the upcoming election.

---

220 Rennack, *U.S. Sanctions on Russia*.

221 Mike Snider, "What's at Stake for Facebook's Mark Zuckerberg as He Testifies for Day 2," *USA Today*, April 10, 2018, https://www.usatoday.com/story/tech/news/2018/04/10/whats-stake-facebooks-mark-zuckerberg-he-testifies-before-congress/503017002/.

222 *Facebook, Google, and Twitter: Examining the Content Filtering Practices of Social Media Giants, House of Representatives*, House of Representatives, 115th Cong., 1st sess., July 17, 2018, 2, https://www.hsdl.org/?view&did=821944.

223 Steinmetz, "Lawmakers Hint at Regulating Social Media During Hearing with Facebook and Twitter Execs."

Page 1386 of 3957

On October 19, 2018, the IRA's chief accountant, Elena Alekseevna Khusyaynova, was indicted by the U.S. Attorney's Office for the Eastern District of Virginia because of her role in the conspiracy to interfere with the U.S. political system, to include the 2016 and 2018 U.S. elections.[224] Khusyaynova's unsealed indictment affidavit revealed the extent of the IRA's financial transactions as the group waged its influence campaign against the United States.[225] Moreover, as she is a regular Russian citizen without the privileges typical to Russian oligarchs or diplomats, her indictment may deter other Russians from working for the IRA or similar types of companies.

The Washington Post reported that U.S. Cyber Command conducted an offensive cyber operation on November 2, 2018, against the St. Petersburg-based IRA office, a day before the U.S. Midterm Elections.[226] This operation was believed to have knocked out the IRA's computer networks for days. If true, this operation showed that the U.S. government was willing to reveal and deploy its technical capabilities to safeguard the integrity of the electoral process.

On November 16, 2018, Congress enacted the Cybersecurity and Infrastructure Security Agency Act of 2018. This legislation created the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security.[227] In January 2017, DHS designated the election system infrastructure as the 17th critical infrastructure sector. CISA is the U.S. government agency charged with helping state and local governments secure America's election systems.[228] Both security-focused actions showed that the U.S.

---

224 Department of Justice, "Russian National Charged with Interfering in U.S. Political System."

225 Department of Justice.

226 Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

227 "Cybersecurity and Infrastructure Security Agency Act of 2018," Pub. L. No. 115–278, Public Law 20 (2018), https://www.hsdl.org/?view&did=829787.

228 Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Security," Cybersecurity and Infrastructure Security Agency, accessed June 3, 2020, https://www.cisa.gov/election-security.

Page 1387 of 3957

government perceives elections are vital to national security and requires consolidating a host of protective cyber functions into one federal agency.

In contrast to the 2016 U.S. elections, the executive and legislative branches of the U.S. government were active ahead of the 2018 elections as it took a series of security measures to shore up vulnerabilities in the different facets of the democratic process, such as providing cybersecurity briefings for political organizations, and enhance transparency about governmental actions to inform the American public, through the many Congressional hearings, law enforcement actions, and economic sanctions.

d. Using the Kartapolov Framework to Evaluate Russian and American Measures in 2018

For the 2018 U.S. elections, the Kartapolov Framework was used to evaluate the effectiveness of the Russian actions, primarily through the efforts of the Internet Research Agency. It was also used to determine the efficacy of the American efforts, both private sector and governmental, to counter each element of the framework. As a reminder, the relevant elements of the framework for this evaluation are: (1) spreading discontent in the population; (2) exerting political pressure; and (3) confusing the political leadership.[229]

After the 2016 U.S. elections, multiple researchers determined that the Internet Research Agency continued at the same cadence and volume of activity as before, seemingly undeterred by being outed in the news media and through government communications.[230] The New Knowledge and Oxford University researchers noted that the Internet Research Agency used meticulous precision to identify different demographic groups by race and political affinities to amplify dissension with its online messaging.[231] Another purpose of the IRA's messaging was to promote right-wing voter turnout and

---

[229] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 36.

[230] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*; Freelon and Lokot, "Russian Disinformation Campaigns on Twitter Target Political Communities across the Spectrum. Collaboration between Opposed Political Groups Might Be the Most Effective Way to Counter It."; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*.

[231] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 8–9; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 18.

Page 1388 of 3957

suppress left-wing and Black voters.[232] The IRA's actions were trying to fulfill the first element of the Kartapolov Framework by trying to spread discontent in the American population. A review of the U.S. Census Bureau's analysis of the 2018 elections voter turnout revealed a mixed outcome to what the IRA would have desired. The overall voter turnout was the highest in 40 years, with 53.4 percent of eligible voters going to the polls in 2018. This turnout contrasts to the 41.9 percent who came out to the polls in 2014, which was the lowest midterm election turnout in 40 years.[233] Table 4 summarizes the increase in both Black and White voter turnout for the midterm elections. While the IRA promoted right-wing voter turnout, which are typically White voters, its efforts to suppress Black voter turnout failed.

Table 4. Voter Turnout by Demographic in Midterm Elections.[234]

Election Year	Black Voter Turnout	White Voter Turnout
2014	40.6%	45.8%
2018	51.4%	57.5%
Change	**+10.8%**	**+11.7%**

The Internet Research Agency's ongoing activities must have exerted some political pressure on the private sector and the U.S. government because of the assortment and frequency of public actions taken by both entities in the run-up 2018 U.S. elections. Thus, the IRA fulfilled the second element of the framework by applying political pressure to the American social media companies and government, but the actions taken by both entities may have blunted the effectiveness of its influence campaigns. However, it does

232 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 19.

233 Jordan Misra, "Voter Turnout Rates among All Voting Age and Major Racial and Ethnic Groups Were Higher Than in 2014," Behind the 2018 U.S. Midterm Election Turnout, April 23, 2019, https://www.census.gov/library/stories/2019/04/behind-2018-united-states-midterm-election-turnout.html.

234 Adapted from Misra.

not appear that the IRA's campaigns confused the political leadership in the United States because the different governmental countermeasures listed in the previous section seemed frequent, deliberate, and proportional.

Application of the Kartapolov Framework appeared to be more favorable to the social media companies' countermeasures during the 2018 election cycle. The framework's first element, spreading discontent in the population, was countered by the social media companies' account takedown operations. As mentioned before, Facebook and Twitter identified and shut down accounts in 2018 at about the same levels as were identified in 2016. The difference from 2016 was that the social media companies were able to disrupt the IRA's activities before the 2018 elections. The framework's second element, exerting political pressure, seemed to make the social media companies act more vigorously in policing their platforms and forthcoming in announcing any actions they took. The third element, confusing the political leadership, will be discussed in the next section when reviewing the efficacy of U.S. government countermeasures. Broadly speaking, the social media companies appeared to be better equipped and decisive in thwarting the IRA's information operations during this election cycle.

Overlaying the Kartapolov Framework's elements on the U.S. government's actions revealed a different outcome than in 2016. For the first element, spreading discontent in the population, the U.S. government showed very public attempts to educate the American public and hold Russian wrongdoing accountable. Through the Justice Department and the Treasury Department, the executive branch made public announcements of indictments and economic sanctions against Russians for their roles in election interference, respectively. In addition, the legislative branch held a series of public hearings to learn about the progress the social media companies were making to counter malign foreign influence and inform the American public.

For the second element, exerting political pressure, the U.S. government was obliged to prevent a repeat of the 2016 interference by Russia. Although difficult to determine whether the U.S. government felt political pressure from the IRA's influence campaign, it displayed a broad spectrum of countermeasures, which were listed in the prior section. Finally, for the third element, confusing the political leadership, both the executive

and legislative branches of the U.S. government appeared to be informed about the threat from Russian influence operations and took appropriate countermeasures to neutralize them.

C. CONCLUSIONS FROM THE 2016 AND 2018 ELECTIONS

In summary, a review of the recent history of Russia's actions to interfere in the U.S. election and America's actions to counter these actions revealed three conclusions. First, the Internet Research Agency was virtually unfettered in its social media campaign to sow division and confusion in the 2016 U.S. elections. Second, the U.S. government and social media companies' countermeasures against the IRA ahead of the 2018 U.S. midterm elections appeared to be generally effective. Third, the Internet Research Agency appeared to be undeterred by the American efforts and made only slight modifications in its tactics from 2016 to 2018.

Researchers have determined that Russian influence campaigns, especially those conducted ahead of the 2016 U.S. elections, can be effective for eliciting partisan responses.[235] Governmental reports, research papers, and the social media companies themselves have acknowledged that the social media companies were unaware of the Russian disinformation campaigns taking place on their platforms and therefore took no active role in countering them. Congressional report findings criticized the executive branch of the government for a tepid and ineffective response to the Russian interference activities. Analysis of voter turnout revealed a relatively high overall high voter turnout but low Black voter turnout in the 2016 elections. This combination of factors may have led to Vladimir Putin achieving his desired goals of eroding American faith in its democratic process and the election of Donald Trump.[236] Ambassador Michael McFaul noted that even if the impact of the Russian influence campaign was minimal, the margin

---

[235] Todd C. Helmus et al., *Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions* (Santa Monica, CA: RAND Corporation, 2020), 51, https://www.rand.org/pubs/research_reports/RRA704-3.html.

[236] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions*, 7.

Page 1391 of 3957

of victory for Trump was about 78,000 votes across three states that tipped the electoral college.[237]

For the 2018 U.S. midterm elections, the combined countermeasures of the private sector and the U.S. government appeared to mitigate the effectiveness of the IRA's influence operations. On December 18, 2018, Dan Coates, Director of National Intelligence, released a press statement in which he said the "Intelligence Community does not have intelligence reporting that indicates any compromise of our nation's election infrastructure that would have prevented voting, changed vote counts or disrupted the ability to tally votes."[238] The ultimate proof was the record turnout of voters across all demographic groups, including Black voters.[239]

Director Coates stated that Russia continued to conduct influence operations after the 2016 elections ahead of the 2018 elections.[240] During this period, the IRA's only shift in tactics appeared to be jettisoning its use of online political advertisements, which was probably the result of the social media companies changing their advertising policies to make it more difficult for foreign entities to purchase advertisements.[241] However, the regular cadence of account shutdown announcements from the social media companies, reports by research firms, and U.S. government reports and statements indicated the Russians would continue to be active ahead of the 2020 U.S. elections. The uncertainty was whether the social media companies and the U.S. government would be up to the task of countering the Russian information operations.

---

237 McFaul, *Securing American Elections*, 14.

238 Office of the Director of National Intelligence, "DNI Coats Statement on the IC's Response to EO 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a U.S. Election," Office of the Director of National Intelligence, December 21, 2018, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2018/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election.

239 Misra, "Voter Turnout Rates among All Voting Age and Major Racial and Ethnic Groups Were Higher Than in 2014."

240 Office of the Director of National Intelligence, "DNI Coats Statement on the IC's Response to EO 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a U.S. Election."

241 Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security"; Twitter, "Elections Integrity."

Page 1392 of 3957

III. THE 2020 ELECTIONS – RUSSIAN GAMBIT AND AMERICAN COUNTERPLAY

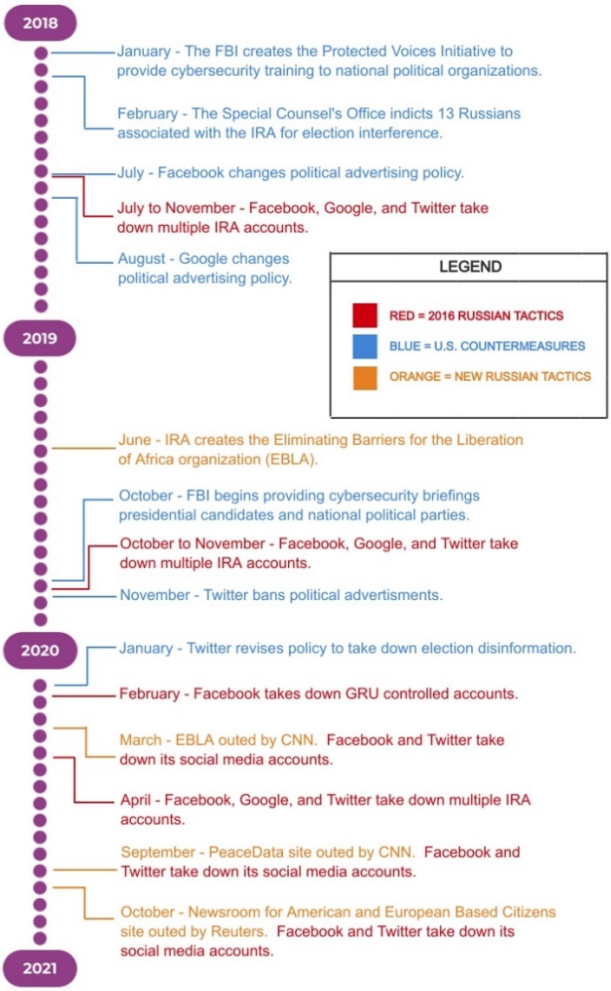
> Foreign nations continue to use influence measures in social and traditional media to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord, and undermine confidence in our democratic process.
>
> — William Evanina, July 24, 2020

The elections of 2016 and 2018 put the major social media companies and the U.S. government on high alert about Russian interference. As a result, both entities were more aggressive in their efforts to thwart the Russians ahead of the 2020 elections. The social media companies partnered with the news media and research organizations to detect and disrupt these Russian disinformation operations. The U.S. government's endeavors included law enforcement actions, threat briefings, and information sharing to the private sector. The cumulative effect of American countermeasures compelled the Russians to evolve their tactics and methods to evade detection continually. Ultimately, the American actions appeared effective in mitigating the Russian online tactics because voters were undeterred and turned out in record numbers for the election.

This chapter reviews the Russian disinformation campaign targeting the 2020 U.S. elections, the countermeasures taken by the social media companies and the U.S. government. It then uses the Kartapolov Framework to evaluate the efficacy of those countermeasures, informing recommendations for counteracting future Russian disinformation campaigns in the next chapter. Finally, figure 5 provides some key highlights of the Russian and American actions after the 2018 midterms to the 2020 elections.

Page 1393 of 3957

Figure 5. Highlights of Russian and American Actions from 2018 to 2020.[242]



[242]Adapted from Federal Bureau of Investigation, "Protected Voices"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive," *Twitter Information Operations* (blog), October 8, 2020, https://blog.twitter.com/en_us/topics/company/2020/disclosing-removed-networks-to-our-archive-of-state-linked-information.html; Facebook, "Facebook - Preventing Election Interference"; Facebook, "October 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), October 27, 2020, https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-mexico-iran-myanmar/; Federal Bureau of Investigation, "Combating Foreign Influence," What We Investigate, accessed October 18, 2020, https://www.fbi.gov/investigate/counterintelligence/foreign-influence; Lauren Feiner and Megan Graham, "Twitter Unveils Final Details for Political Ad Ban, but It's Still Looking Murky," CNBC, November 15, 2019, https://www.cnbc.com/2019/11/15/twitter-unveils-new-political-ad-policy.html; Google Threat Analysis Group, "TAG Bulletin: Q4 2020," Google: Updates from Threat Analysis Group, November 17, 2020, https://blog.google/threat-analysis-group/tag-bulletin-q4-2020/; Google Threat Analysis Group, "Google Safety & Security"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

Page 1394 of 3957

A. THE IRA AND OTHER PROXIES' SOCIAL MEDIA ACTIVITIES

From 2019 through 2020, the major social media companies reported most of the IRA's activities with a couple of exceptions. On at least a quarterly basis, Facebook, Google, and Twitter made announcements regarding the detection and takedown of fake Russian accounts on their platforms via blogposts. In addition, many of the IRA-related activities involved account takedowns in various geographical locations, not just Russia-based accounts. The exceptions to the major social media companies reporting Russian account takedowns came when other organizations were able to identify and expose the activities of the Internet Research Agency. In one instance, CNN broke a story about the IRA's activities in March 2020.[243] In a second instance, Graphika, a New York-based social media analysis company, issued reports on IRA activities and identified another cluster of Russia-controlled campaigns it dubbed "Secondary Infektion."[244] These account takedowns appeared to be coordinated across different organizations as Facebook and Twitter made their own announcements after the reporting by CNN and Graphika.

Different Russian proxy organizations focused on specific voting groups to affect their attitudes. For example, the Internet Research Agency established a front organization called Eliminating Barriers for the Liberation of Africa (EBLA) with offices in Western Africa.[245] On March 12, 2020, CNN exposed EBLA when it televised a news story with an associated news article about EBLA being a Russian troll farm.[246] Through its investigation, CNN determined the head of EBLA was a Russian-speaking Ghanaian named Seth Wiredu, who called himself "Mr. Amara" and registered the organization in June 2019.[247] CNN assessed he was being funded through Yevgeniy Prigozhin's Project Lakhta. Wiredu managed offices outside Accra, Ghana, and Lagos, Nigeria, with

---

[243] Clarissa Ward et al., "Russian Election Meddling Is Back — Via Ghana and Nigeria — and in Your Feeds," CNN, April 11, 2020, https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html.

[244] Ben Nimmo et al., *Secondary Infektion* (New York: Graphika, 2020), https://secondaryinfektion.org/report/secondary-infektion-at-a-glance/.

[245] Ward et al., "Russian Election Meddling Is Back."

[246] Ward et al.

[247] Ward et al.

employees who portrayed themselves as African Americans and engaged in social media activities.[248] The EBLA employees focused primarily on racial issues such as police brutality, displays of anger towards white people, and black empowerment.[249] Figure 6 provides an example of the types of postings put out by EBLA. In a similar fashion to the IRA's operations in St. Petersburg, the EBLA employees received assignments on different themes, coordinated their postings, and worked on cross-platform campaigns.[250] Before it was outed, the EBLA organization appeared to be laying the groundwork for influencing the behavior of Black voters ahead of the 2020 U.S. elections.

Figure 6. An Image from a Facebook Account Controlled by EBLA.[251]

Although the Russians tried to evolve their tactics to evade detection by the social media companies, the effort failed because the social media companies partnered with other

248 Ward et al.

249 Ward et al.

250 Ward et al.

251 Source: Ward et al.

organizations to detect and expose the Russians. One example highlighted this collaboration. On September 1, 2020, Facebook and Twitter announced that they had identified and taken down social media accounts associated with an English and Arabic language website called "PeaceData," which portrayed itself as a progressive-leaning independent news site.[252] Figure 7 shows two postings from the PeaceData site.

In coordination with Facebook, Graphika issued a report on PeaceData, which provided detailed information about the site itself, an analysis of images on the site, and the site's writers.[253] This development was notable for four reasons. First, the site was an example of the IRA shifting content off the social media platforms to a website which it controlled. Second, Graphika analyzed the profile photos of several PeaceData staff members and determined they were created through generative adversarial networks (GANS), which is a type of artificial intelligence.[254] These photos were the first known instance of the IRA using artificial intelligence to generate phony images of people. Examples of these GANS-generated profile photos appear in Figure 8. Third, Reuters broke a story about the IRA posing as PeaceData staff to hire unwitting freelance journalists, including Americans, to write articles for the site.[255] The Carnegie Endowment for International Peace determined that at least 20 freelance journalists had been duped into writing articles for the PeaceData outlet.[256] This instance is the first identified example of the IRA hiring unwitting individuals to generate content on its behalf. Fourth, Facebook shared information about the PeaceData site and associated social media networks with

252 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive," Social Media, *Twitter Information Operations* (blog), September 1, 2020, https://twitter.com/TwitterSafety/status/1300848632120242181; Facebook, "September 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), September 2020, https://about.fb.com/wp-content/uploads/2020/10/September-2020-CIB-Report.pdf.

253 Nimmo et al., "IRA Again: Unlucky Thirteen."

254 Nimmo et al., 6.

255 Jack Stubbs, "Duped by Russia, Freelancers Ensnared in Disinformation Campaign by Promise of Easy Money," Reuters, September 3, 2020, https://www.reuters.com/article/us-usa-election-facebook-russia-idUSKBN25T35E.

256 Alicia Wanless and Laura Walters, "How Journalists Become an Unwitting Cog in the Influence Machine," Carnegie Endowment for International Peace, October 13, 2020, https://carnegieendowment.org/2020/10/13/how-journalists-become-unwitting-cog-in-influence-machine-pub-82923.

Graphika.[257] This collaboration revealed Facebook joining forces with a non-social media company third party to analyze its findings.

Figure 7. Postings from the PeaceData Site.[258]

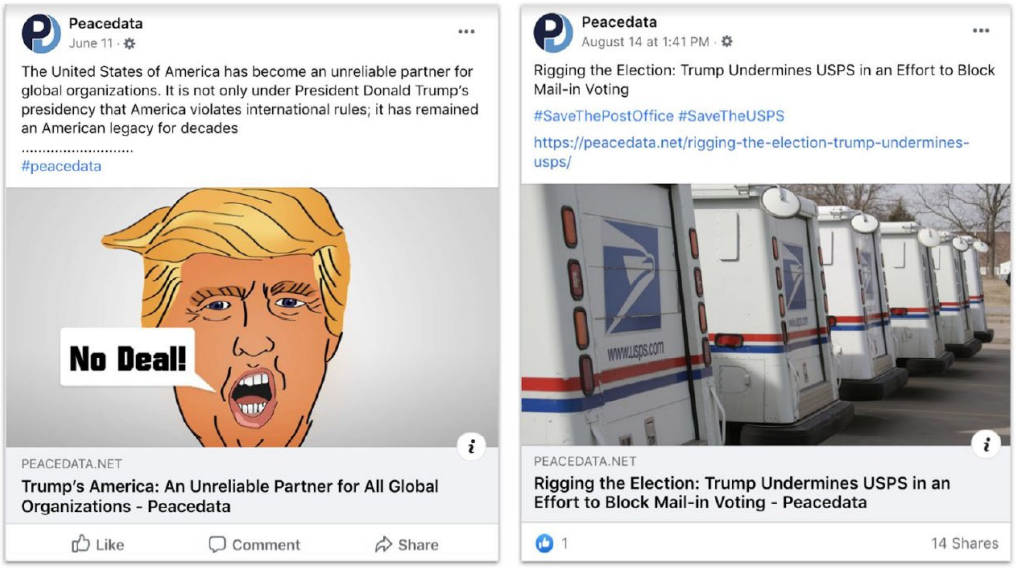
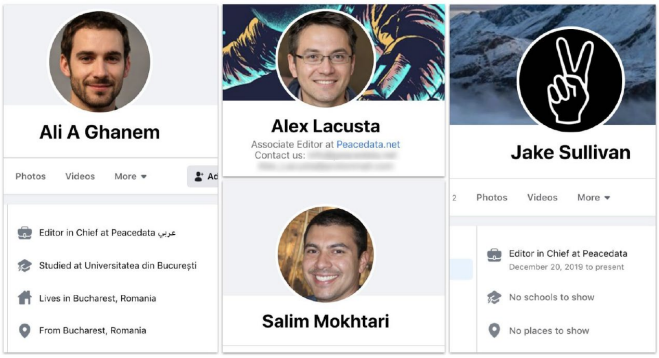


Figure 8. Photos of PeaceData Staff Created by Artificial Intelligence.[259]



257 Nimmo et al., "IRA Again: Unlucky Thirteen," 1.

258 Source: Nimmo et al., 20.

259 Source: Nimmo et al., 5.

Page 1398 of 3957

The Russians continued to demonstrate different tactics such as using alternative communication platforms, artificial intelligence to generate false personas, and unwitting co-optees to avoid detection by the social media companies and the U.S. government. Not only did the Russians use the PeaceData site to appeal to progressives, but they also created another site called the Newsroom for American and European Based Citizens (NAEBC) to appeal to conservatives.[260] On October 1, 2020, Reuters published an article that exposed NAEBC as another news outlet run by the IRA, which appeared to be the ideological counterpart of the PeaceData outlet.[261] Figure 9 shows an example of a posting on NAEBC. Figure 10 shows an example of cross-posting of NAEBC content on Gab.

The NAEBC site was noteworthy for three reasons. First, in addition to the mainstream social media platforms of Facebook, Twitter, and LinkedIn, the IRA used two right-wing social media platforms, Gab and Parler, to disseminate content from NAEBC.[262] Second, Figure 11 shows that the IRA continued using GANS-generated staff profile photos on NAEBC to convey a sense of authenticity.[263] Lastly, Graphika determined that the IRA used various social media accounts to engage with real users and convince them to post on the NAEBC site, which met with some success.[264] However, Graphika assessed that both the PeaceData and NAEBC outlets had limited influence because they were created around June 2020 and taken down by September 2020 before either could generate much viewership.[265] Furthermore, Graphika opined that the purpose for both the websites was two-fold. First, the sites wanted to influence voter turnout through the type of content on each site. For example, on the PeaceData site, Graphika believed articles denigrating Joe Biden compared to other Democratic candidates would

---

[260] Stubbs, "Exclusive."

[261] Graphika Team, *Step Into My Parler; Suspected Russian Operation Targeted Far-Right American Users on Platforms Including Gab and Parler, Resembled Recent IRA-Linked Operation That Targeted Progressives* (New York: Graphika, 2020), 1, https://graphika.com/reports/step-into-my-parler/.

[262] Graphika Team, 16.

[263] Graphika Team, 20.

[264] Graphika Team, 23–26.

[265] Graphika Team, 26.

Page 1399 of 3957

suppress Democratic voter turnout.[266] Second, the content on both PeaceData and NAEBC was meant to inflame existing discord within their viewership.[267]

Figure 9. Posting from the NAEBC Site.[268]

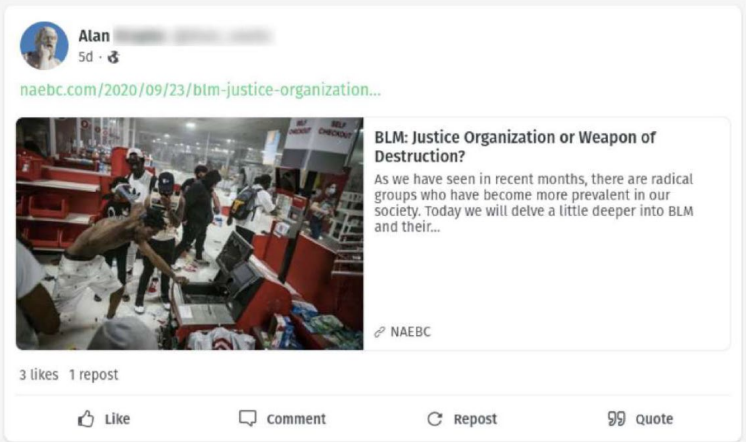
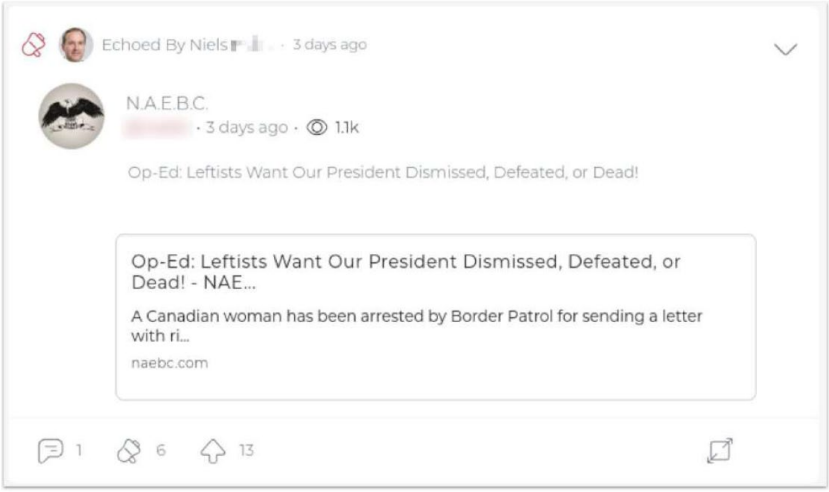


Figure 10. NAEBC Cross-platform Posting on Parler.[269]



266 Graphika Team, 34.

267 Graphika Team, 34.

268 Source: Graphika Team, 8.

269 Source: Graphika Team, 9.

Page 1400 of 3957

Figure 11. GANS-generated Profile Photos for NAEBC Staff.[270]

The Russians targeted the far-right channels as well as the mainstream ones to reach different target audiences. In addition to its work analyzing the aforementioned IRA activities, Graphika conducted an independent investigation into another Russian information operation dubbed "Secondary Infektion."[271] Graphika determined this group has been active from 2014 to at least the beginning of 2020 and characterized the online campaigns as focusing on misinformation about foreign policy and diplomacy-related matters.[272] Although the content appeared in multiple languages, Graphika deduced the campaigns focused on targeting viewers in Europe and North America.[273] Its analysis of the top themes in the content revealed that the articles primarily concentrated on denigrating Ukraine, the United States, NATO, and sowing discord in the rest of Europe.[274] Figure 12 shows the breakdown of articles by quantity and topic. Thus, the Russians had expanded far beyond using the Internet Research Agency as a proxy for its disinformation campaigns.

[270] Source: Graphika Team, 20.

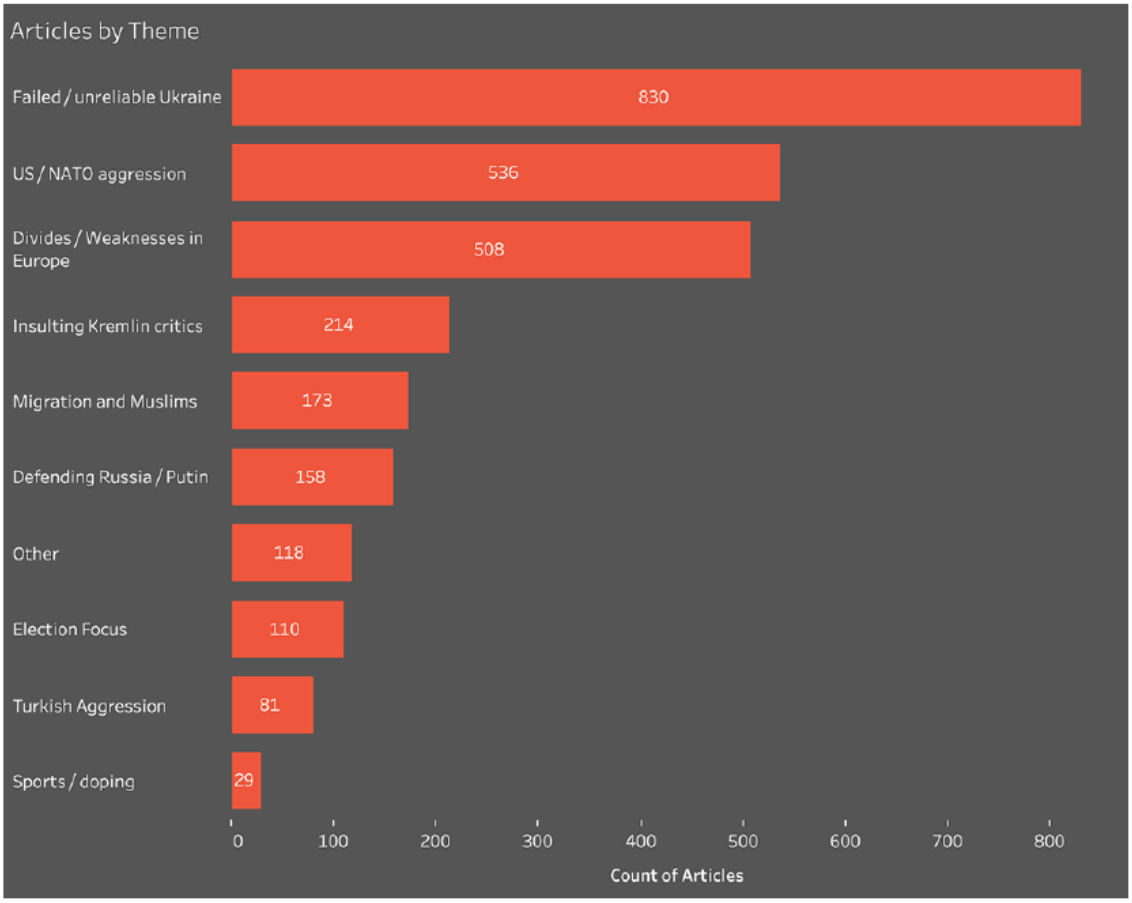
[271] Nimmo et al., *Secondary Infektion*.

[272] Nimmo et al., 4.

[273] Nimmo et al., 11.

[274] Nimmo et al., 14.

Figure 12. Breakdown of Secondary Infektion Articles by Topic.[275]



Secondary Infektion had two features that distinguished it from the other IRA-controlled campaigns. First, the actors behind Secondary Infektion made extensive use of forged postings and documents in an attempt to proliferate disinformation and propagate conflict.[276] Second, Graphika observed that Secondary Infektion used a wide-ranging set of online platforms, especially micro-blogging sites, to disseminate content, not only the mainstream social media platforms.[277] Examples of a forged post and forged document

[275] Source: Nimmo et al., 14.

[276] Nimmo et al., 4.

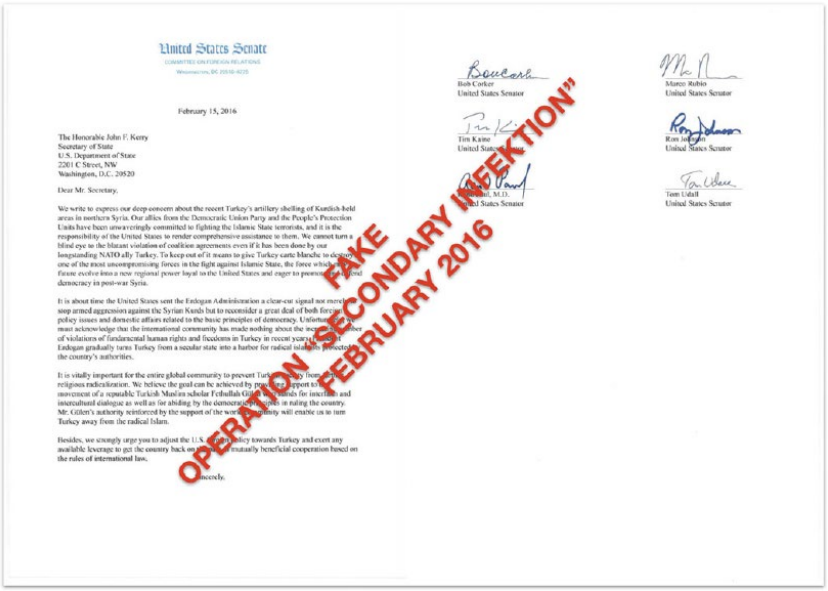
[277] Nimmo et al., 8.

Page 1402 of 3957

are shown in Figures 13 and 14, respectively. The Russians extended their reach across multiple channels and platforms by agilely adapting their tactics.

Figure 13. Secondary Infektion-made Forged Posting from Marco Rubio.[278]

Figure 14. Secondary Infektion-made Forged Letter to John Kerry.[279]



278 Source: Nimmo et al., 5.

279 Source: Nimmo et al., 6.

By being everywhere simultaneously, the Russians effectively reduced the likelihood of being shut down, given the reach of their operations. In discussion with some social media companies, Graphika believed the extensive variety of sites used by Secondary Infektion could be related to operational security.[280] Specifically, this type of behavior would reduce the impact of takedowns by any one company and make coordinated takedowns more difficult across multiple companies.[281] The social media companies told Graphika that the actors behind the Secondary Infektion activities used good security practices because they were consistent and disciplined about using "burner" accounts, which were registered, used to create a series of posts, and then abandoned within the day.[282] Graphika and the social media companies determined that Russian operators conducted Secondary Infektion. Still, they could not determine whether the campaign was associated with the IRA, GRU, or other Russia-based groups.[283] The Secondary Infektion campaigns were another example of the Russians trying to adjust their tactics to avoid detection by the social media companies.

B. PRIVATE SECTOR COUNTERMEASURES

Ahead of the 2020 U.S. elections, the major social media companies, consisting of Facebook, Google, and Twitter, continued their transparency efforts by regularly providing public notifications of foreign influence-related account takedowns. These notifications typically provided summaries of the activities the companies identified, the number of accounts taken down, and how these accounts violated their terms of service. In addition, all three companies published security measures regarding technology improvements and policy changes on their platforms ahead of the elections.[284]

---

280 Nimmo et al., 8.

281 Nimmo et al., 8.

282 Nimmo et al., 8.

283 Nimmo et al., 11.

284 Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security"; Twitter, "Elections Integrity."

Page 1404 of 3957

In 2019, Facebook announced two sets of takedowns. First, on October 21, 2019, it removed 50 Instagram and one Facebook account, which originated from Russia and focused on American users. Then, on October 30, 2019, Facebook removed five Instagram accounts, 35 Facebook accounts, 53 Pages, and seven Groups, which originated from Russia and focused on users in African countries (Cameroon, Côte d'Ivoire, the Democratic Republic of the Congo, Mozambique, Central African Republic, and Madagascar).[285] These actions showed that the IRA's activities persisted and expanded into targeting different countries and that Facebook was actively monitoring its platform and taking efforts to disrupt the IRA.

Social media companies uncovered even deeper links to Russia. In 2020, Facebook announced six sets of takedowns. All of them are summarized in Table 5. In contrast to 2016, when 470 IRA accounts were identified, Facebook identified and shut down 825 accounts in 2020. In one noteworthy takedown, Facebook discovered Facebook accounts, pages, and groups controlled by the GRU, targeting Ukraine and other Eastern European countries, and announced their removal on February 12, 2020.[286] The use of the GRU for disinformation campaigns appeared to be a new tactic by the Russians. As mentioned before, the GRU was responsible for the hack and dump attack of the Democratic National Committee in 2016 but had not previously engaged in social media influence campaigns. After the Internet Research Agency and Secondary Infektion, the GRU would be the third different Russian-controlled entity discovered to be conducting influence campaigns ahead of the 2020 elections. These takedowns confirmed the ongoing social media-focused portion of the Russian influence strategy.

[285] Facebook, "Facebook - Preventing Election Interference."

[286] Facebook.

Page 1405 of 3957

Table 5. Summary of Facebook Takedowns for 2020.[287]

Type	Month					
	February	March	April	August	September	October
Facebook Account	78	49	91	13	229	0
Facebook Page	11	69	46	2	36	2
Facebook Group	29	0	2	0	19	0
Instagram Account	4	85	1	0	37	22
Total	122	203	140	15	321	24
Grand Total	825					

On March 12, 2020, Facebook announced another noteworthy takedown, in which it shut down 85 Instagram accounts, 69 Pages, and 49 Facebook accounts.[288] Its takedown coincided with the CNN story regarding the Eliminating Barriers for the Liberation of Africa organization discussed above. Facebook assessed that individuals from Russia had recruited locals in Ghana and Nigeria to build an online social network and develop an audience; EBLA controlled at least one Instagram account with over 260,000 followers and one Facebook account with over 13,000 followers.[289] The IRA's expansion into West Africa mirrored Yevgeniy Prigozhin's business interests on the continent and suggested the IRA thought its troll-farm model could be successfully exported into other countries.[290] These takedowns demonstrated that Facebook successfully identified Russian disinformation operations despite a shift in their tactics.

[287] Adapted from Facebook, "February 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), March 2020, https://about.fb.com/wp-content/uploads/2020/03/February-2020-CIB-Report.pdf; Facebook, "March 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), April 2, 2020, https://about.fb.com/news/2020/04/march-cib-report/; Facebook, "April 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), May 5, 2020, https://about.fb.com/news/2020/05/april-cib-report/; Facebook, "September 2020 Coordinated Inauthentic Behavior Report"; Facebook, "August 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), September 1, 2020, https://about.fb.com/wp-content/uploads/2020/09/August-2020-CIB-Report.pdf; Facebook, "October 2020 Coordinated Inauthentic Behavior Report."

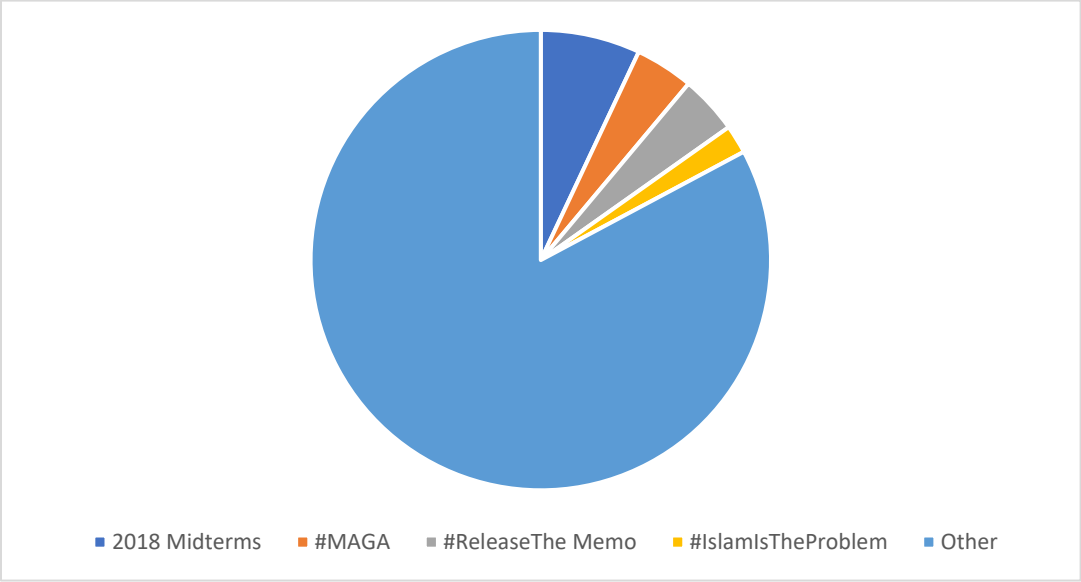
[288] Facebook, "Facebook - Preventing Election Interference."

[289] Facebook.

[290] Grossman, Bush, and DiResta, "Evidence of Russia-Linked Influence Operations in Africa," 2.

In 2019, Twitter announced two takedowns totaling 422 IRA-controlled accounts, which made about 929,000 tweets.[291] Figure 15 demonstrates a categorization of tweets by topic. A review of these tweets revealed a continued focus on the 2018 midterm U.S. elections, with seven percent of all tweets, where Democrats had taken over control of the House of Representatives. The other prominent topics focused on promoting Trump, a right-wing meme that accused the FBI of misusing the Steele dossier to obtain a surveillance order on Trump associate, Carter Page, and Islamophobic rhetoric. The themes promoted by the IRA on Twitter showed its continued acuity in determining the hot-button issues that would agitate right-wing voters.

Figure 15. Breakdown of Twitter Tweets by Topic for 2019.[292]



On November 11, 2019, Twitter announced a ban on virtually all political advertisements.[293] It made a few minor exceptions for issue-based ads and news

[291] Twitter, "Elections Integrity."

[292] Adapted from Twitter.

[293] Feiner and Graham, "Twitter Unveils Final Details for Political Ad Ban, but It's Still Looking Murky."

organizations already exempted from its policy. Twitter "defines political advertising as referencing a candidate, political party, elected or appointed government official, election, referendum, ballot measure, legislation, regulation, directive or judicial outcome."[294] Although Twitter was the first of the major social media companies to ban political advertisements, critics in news media perceived it as an expedient move meant to earn goodwill with the public while only costing less than one percent of its quarterly revenue.[295]

Expanding beyond earlier takedowns, the major social media companies coordinated their publicity for more significant impact and established more direct links to Russia. In 2020, Twitter announced four sets of takedowns, as summarized in Table 6. For 2020, a total of 1,233 accounts were taken down, versus the 3,814 accounts identified as being controlled by the IRA in 2016. One noteworthy takedown occurred on March 12, 2020, when Twitter announced the shutdown of 71 accounts operated by the Eliminating Barriers for the Liberation of Africa organization in Ghana and Nigeria.[296] Twitter attributed them to Russian-sponsored activities, which CNN characterized as an attempt "to sow discord by engaging in conversations about social issues, like race and civil rights."[297] The synchronization of announcements by Facebook and Twitter with the CNN breaking story suggests some level of coordination between the three companies.

Another significant Twitter takedown occurred in June 2020, with the shutdown of 1152 accounts, which Twitter and the Stanford Internet Observatory attributed a campaign dubbed the "Current Policy" to the IRA because of the anti-Western and pro-Putin content it disseminated.[298] Stanford's analysis determined the Current Policy accounts posted more than 3.4 million tweets since 2013, with some focused on portraying actual Russian

---

294 Feiner and Graham.

295 Michael Nuñez, "The Surprising Truth about Twitter's Political Ad Ban," *Forbes*, November 1, 2019, https://www.forbes.com/sites/mnunez/2019/11/01/the-surprising-truth-about-twitters-political-ad-ban/.

296 Ward et al., "Russian Election Meddling Is Back."

297 Ward et al.

298 Stanford Internet Observatory, "Analysis of June 2020 Twitter Takedowns Linked to China, Russia, and Turkey."

Page 1408 of 3957

government agencies and others working to boost specific Russian politicians or federal initiatives.[299] These actions revealed coordination among the social media companies, news media, and a research organization to thwart Russian disinformation operations.

Table 6. Summary of Twitter Takedowns for 2020.[300]

Type	Month			
	March	June	September	October
Account	71	1152	5	5
Grand Total	1,233			

At the beginning of 2020, Twitter announced an enhancement of its safety policies, developing better tools for detecting abusive behavior, and aggressively taking actions against violations of the terms of service.[301] Twitter also highlighted its collaboration with political parties, researchers, and election officials. In addition, a Twitter spokesperson stressed the importance of staying in contact with state election officials and law enforcement.[302]

On November 26, 2019, Google announced it had shut down 15 YouTube channels and associated Google accounts. These IRA-controlled accounts used English, French, and Arabic language content to target users in South Africa, Madagascar, Sudan, and the Central African Republic. Google said these accounts were associated with the account

299 Stanford Internet Observatory.

300 Adapted from Ward et al., "Russian Election Meddling Is Back"; @TwitterSafety, "June 2020: Disclosing Networks of State-Linked Information Operations We've Removed," *Twitter Information Operations* (blog), June 12, 2020, https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.html; @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

301 Twitter, "Elections Integrity."

302 Twitter.

Page 1409 of 3957

takedowns Facebook had announced on October 30, 2019.[303] This statement confirmed joint action facilitated by information sharing between the two companies.

On March 3, 2020, Google announced it had developed policies prohibiting deceptive practices such as voter suppression and misrepresentation in all its products, including Google Ads, YouTube, and the Google Play Store.[304] The company also mentioned working closely with other technology companies and the FBI regarding referrals and leads.[305] This announcement by Google showed an effort to be more transparent, coordinate with other social media companies, and acknowledge some engagement with the FBI.

In April 2020, Google's Threat Analyst Group began to blog about account takedowns every quarter. Table 7 provides a summary of the number and types of accounts taken down by Google. For 2020, Google took down a total of 129 accounts, which is lower in number than in 2016, when it identified and submitted 228 YouTube videos and 655 AdWord advertisements to the Senate Intelligence Committee for review.[306]

Table 7. Summary of Google Takedowns for 2020.[307]

Type	Month				
	April	May	June	October	November
YouTube Channel	22	47	17	28	10
Blog	3	0	0	1	0
AdSense Account	0	1	0	0	0
Total	25	48	17	29	10
Grand Total	**129**				

303 Google Threat Analysis Group, "Google Safety & Security."

304 Google Threat Analysis Group.

305 Google Threat Analysis Group.

306 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 7.

307 Adapted from Google Threat Analysis Group, "TAG Bulletin: Q2 2020," *Google: Updates from Threat Analysis Group* (blog), August 5, 2020, https://blog.google/threat-analysis-group/tag-bulletin-q2-2020/; Google Threat Analysis Group, "TAG Bulletin," November 17, 2020.

C. U.S. GOVERNMENT COUNTERMEASURES

Ahead of the 2020 U.S. elections, the U.S. government appeared publicly focused on transparency efforts, such as public statements and a hearing, and modifying the policies regarding interactions with political campaigns. The U.S. government also took security steps, such as information sharing with relevant stakeholders, including social media companies and political campaigns. The major social media companies mentioned working with the U.S. government to some extent. Some news reporting corroborated this engagement between the private sector companies and the U.S. government.

Only one public Congressional hearing took place before the U.S. elections on November 3, 2020. On September 18, 2019, the Senate Commerce Committee held a hearing with senior executives from Facebook, Google, and Twitter to discuss their companies' efforts to remove extremist content and disinformation from their platforms.[308] This hearing was the only opportunity in 2019 for the American public through Congressional testimony and for Congress to publicly hold the companies accountable for the actions they previously pledged to protect the elections.

On May 15, 2020, to address foreign interference threats more directly, William Evanina, Director of the National Counterintelligence and Security Center (NCSC), was tasked with leading all the U.S. government threat intelligence briefings to the relevant national political committees and presidential campaign committees.[309] The ODNI likely changed the briefers from a rotating cadre of analysts from the FBI and DHS to streamline the process for the recipients and let the political campaigns and all Americans know the entire U.S. Intelligence Community backs these threat briefings.[310]

Before the 2020 U.S. elections, the FBI took some public actions related to election security. On October 23, 2019, FBI Director Wray announced an expansion of the

---

[308] U.S. Congress. Senate, September 18, 2019.

[309] Office of the Director of National Intelligence, "Director of National Intelligence Announces Changes to Election Security Briefings," Office of the Director of National Intelligence, May 15, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2118-director-of-national-intelligence-announces-changes-to-election-security-briefings.

[310] Office of the Director of National Intelligence.

Page 1411 of 3957

Protected Voices Initiative.[311] New cybersecurity training videos and reference materials were added to the website. Furthermore, the FBI indicated it would provide cybersecurity training to all of the presidential campaigns ahead of the primary election season.[312] This training supplemented the FBI's ongoing engagement with the national-level political committees. This security-related action continued the FBI's efforts to help the various political campaigns safeguard their computer networks and electronic devices.

On January 16, 2020, the FBI stated it was modifying its notification policy regarding computer intrusions to election infrastructure. Previously, the FBI would notify local election officials whose organizations typically owned and maintained the election systems and equipment. The local officials would be responsible for informing the state-level officials. With this policy change, the FBI would simultaneously notify the designated chief state-level election official as well as the local officials impacted by a cyber-attack. According to the FBI press release, "this new policy will result in increased collaboration between all levels of government for the integrity and security of U.S. elections."[313] Thus, the FBI appeared to publicly state affirmative actions it was taking to safeguard the elections. Previously, the FBI had been typically reluctant to disclose election-related actions to the public.

Despite not making public announcements about its involvement with the private sector, the U.S. government appeared to be more engaged with social media companies ahead of the 2020 U.S. elections than in 2016. On September 4, 2019, Facebook hosted an election security meeting with the FBI, DHS, and ODNI.[314] The other companies

311 "Protecting Every Voice: FBI Expands Suite of Resources on Election Security," *Homeland Security Today* (blog), October 23, 2019, https://www.hstoday.us/subject-matter-areas/infrastructure-security/protecting-every-voice-fbi-expands-suite-of-resources-on-election-security/.

312 "Protecting Every Voice."

313 Federal Bureau of Investigation, "FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure," FBI Press Releases, January 16, 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-policy-for-notifying-state-and-local-election-officials-of-cyber-intrusions-affecting-election-infrastructure.

314 Kurt Wagner, "Facebook Meets With FBI to Discuss 2020 Election Security," Bloomberg, September 4, 2019, https://www.bloomberg.com/news/articles/2019-09-04/facebook-meets-with-fbi-to-discuss-2020-election-security.

Page 1412 of 3957

attending the meeting included Google, Microsoft, and Twitter.[315] The group discussed plans for better coordination and information sharing.[316] This meeting was the first indication of private sector companies meeting with the U.S. government to safeguard the 2020 U.S. elections. In August 2020, the New York Times broke a story revealing that the private sector companies working with the U.S. government had expanded to include the Wikimedia Foundation, Verizon Media, Reddit, Pinterest, and LinkedIn.[317] A spokesperson for the private sector companies stated that they regularly met with the U.S. government agencies responsible for election security to discuss threat trends and worked closely with each represented company to protect their platforms.[318]

Public statements from some social media companies revealed that the U.S. government, particularly the FBI, had provided them with tipper information to detect Russian influence operations on their platforms. In August 2020, Facebook announced that it had taken down two pages and 13 Facebook accounts, which the IRA was controlling, and mentioned finding the cluster due to off-platform activities identified by the FBI.[319] In September 2020, Facebook and Twitter announced the takedown of PeaceData-associated accounts being controlled by the IRA.[320] Facebook stated that it had been able to identify the accounts based on off-platform information provided by the FBI.[321] Twitter went further in its statement when it expressly thanked the FBI's Foreign Influence Task Force for its "close collaboration and continued support of our work to protect the public conversation at this critical time."[322] In October 2020, Facebook identified and shut down

---

315 Wagner.

316 Wagner.

317 Mike Isaac and Kate Conger, "Google, Facebook and Others Broaden Group to Secure U.S. Election," *New York Times*, August 12, 2020, https://www.nytimes.com/2020/08/12/technology/google-facebook-coalition-us-election.html.

318 Isaac and Conger.

319 Facebook, "August 2020 Coordinated Inauthentic Behavior Report."

320 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; Facebook, "September 2020 Coordinated Inauthentic Behavior Report."

321 Facebook, "September 2020 Coordinated Inauthentic Behavior Report."

322 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

Page 1413 of 3957

a network of IRA-controlled Facebook and Instagram operated out of Mexico and Venezuela.[323] Once again, Facebook mentioned its ability to identify these accounts based on information provided by the FBI.[324] Also, in October 2020, Google noted it had shut down one blog and 26 YouTube channels being operated by the IRA.[325] In addition, Google's Threat Analysis Group mentioned it had received leads provided by the FBI to support its internal investigation.[326] In total, the FBI appears to have shared information with Facebook, Google, and Twitter on at least four occasions, which led to the detection and takedown of multiple IRA-controlled accounts on their respective platforms. This sharing contrasted with 2016 when it seemed that the U.S. government had not shared any threat information with the social media companies ahead of the 2016 U.S. elections.

Besides the FBI and DHS, other U.S. government agencies were also publicly involved in election security. For example, in August 2020, the NSA, jointly with the FBI, issued a cybersecurity advisory exposing complex malware dubbed "Drovorub," created by Russian Military Intelligence.[327] This advisory was the first of its kind and would allow private and public sector organizations to safeguard themselves ahead of the election. Also, in August 2020, the State Department's Global Engagement Center issued an extensive report revealing the disinformation tactics employed by the Russian government and associated organizations, such as the IRA.[328] The State Department believed this report would help news media, private and public sector organizations, and other governments detect and analyze Russian influence operations to build up a collective resilience.[329]

---

[323] Facebook, "October 2020 Coordinated Inauthentic Behavior Report."

[324] Facebook.

[325] Google Threat Analysis Group, "TAG Bulletin," November 17, 2020.

[326] Google Threat Analysis Group.

[327] National Security Agency and Federal Bureau of Investigation, *Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*, Rev 1.0 (Washington, DC: National Security Agency & Federal Bureau of Investigation, 2020), https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF.

[328] Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem*.

[329] Global Engagement Center, 2.

Page 1414 of 3957

During the elections, the U.S. government had little to do with the actual administration of political campaigns or elections. Instead, the U.S. government was responsible for providing funding to states for equipment upgrades, conducting enforcement actions to ensure fair elections, and keeping the American public apprised of any significant developments.[330] On November 4, 2020, after the election polls had closed across the United States, Christopher Krebs, Director of the Cybersecurity and Infrastructure Security Agency, issued a statement that the U.S. government had seen no evidence of Russian or other foreign adversaries changing ballots or preventing Americans from voting. In December 2020, Krebs reaffirmed his belief about the integrity of the 2020 U.S. Elections during a hearing before the Senate Committee on Homeland Security and Governmental Affairs in December 2020.[331] Senior election executives representing America's election infrastructure sector made a statement that echoed Krebs' claim of a safe and fair election.[332]

In March 2021, the Office of the Director of National Intelligence issued the Intelligence Community's report assessing foreign threats to the 2020 U.S. elections.[333] Similar to what NCSC Director Evanina said in his August 2020 statement, the ODNI assessment emphasized the ongoing and concerted Russian disinformation campaign, which was designed to promote the reelection of President Trump, denigrate Joe Biden and the Democratic Party, erode trust in the election process, and inflame political and social tensions within the United States.[334] The ODNI discussed the efforts of the Internet

---

330 R. Sam Garrett, *Federal Role in U.S. Campaigns and Elections: An Overview*, CRS Report No. R45302 (Washington, DC: Congressional Research Service, 2018), 27, https://fas.org/sgp/crs/misc/R45302.pdf.

331 *Examining Irregularities in the 2020 Election: Hearing before the Committee on Homeland Security and Governmental Affairs*, Senate, 116th Cong., 2nd Session, December 16, 2020, 2, https://www.hsgac.senate.gov/imo/media/doc/Testimony-Krebs-2020-12-16.pdf.

332 Elections Infrastructure Government Coordinating Council and Election Infrastructure Sector Coordinating Executive Committee, "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees," November 12, 2020, https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

333 Office of the Director of National Intelligence, "Intelligence Community Assessment on Foreign Threats to the 2020 U.S. Federal Elections."

334 Office of the Director of National Intelligence.

Research Agency and highlighted the "short-lived troll farms" based in Mexico and Western Africa, which were initiated to avoid the ongoing account takedown efforts by the social media companies with help from the U.S. government.[335] The ODNI concluded that greater awareness by the news media and the American public, coupled with the actions taken by the social media companies and the U.S. government, likely countered the Russian efforts to some degree.[336]

D. USING THE KARTAPOLOV FRAMEWORK TO EVALUATE RUSSIAN AND AMERICAN MEASURES IN 2020

As previously used for appraising IRA information operations during the elections in 2016 and 2018, the relevant components of the Kartapolov Framework were used to evaluate the Russian and American efforts to determine their effectiveness for the 2020 U.S. Elections. To reiterate, these components are: (1) spreading discontent in the population, (2) exerting political pressure, and (3) confusing the political leadership.[337] The impact of the Russian campaigns on American political leadership will be gauged in the section evaluating the countermeasures taken by the U.S. government.

1. The IRA and Other Proxies – Impact and Evolution

The Internet Research Agency evolved its tactics ahead of the 2020 U.S. elections but was unsuccessful in achieving its ultimate desired outcome of a Trump reelection. The IRA's tactical developments were two-fold: (1) moving troll farm operations to locations outside of Russia, namely West Africa and Mexico, and (2) moving content from the social media platforms to websites the IRA controlled. For the first component of the Kartapolov Framework, a review of all four of the IRA's campaigns for 2020 showed they were focused on inflaming dissension in the populace. CNN evaluated the social media content disseminated by Eliminating Barriers for the Liberation of Africa and noted it was primarily focused on racial issues such as Black empowerment and used language meant

335 Office of the Director of National Intelligence, 3.

336 Office of the Director of National Intelligence, 6.

337 Wilhelm, "A Russian Military Framework," 35.

to inflame divisions between American racial groups.[338] For the PeaceData outlet, Graphika's analysis determined the actors behind it were targeting progressive groups in the United States, especially those who identified with democratic socialism.[339] The Newsroom for American and European Based Citizens site appeared to be the counterweight to PeaceData. It targeted viewers with a far-right ideology because it covered topics such as racist tropes about black people and criticism of the Black Lives Matter movement.[340] Lastly, the Secondary Infektion campaign's focus on diplomacy and foreign policy appeared to be tailored to denigrate the United States and its European allies while also trying to foment conflict between the allied countries.[341] Although the Russian actions likely inflamed already existing dissension in the United States, it did not appear to deter voter turnout at all. The effectiveness of the Russian messaging was probably blunted by the account takedowns by the major social media companies and being outed by the news media before it could develop traction with the targeted audiences.

For the second component of the Kartapolov Framework, exerting political pressure, the Russian campaigns appeared to have mixed results. On the one hand, from interviews conducted with the social media companies, CNN determined that the IRA-controlled organization, Eliminating Barriers for the Liberation of Africa, had successfully gathered many followers for its social media accounts since its inception in June 2019.[342] Facebook reported to CNN that the EBLA-controlled accounts had about 267,000 users following EBLA-controlled Facebook or Instagram accounts.[343] Twitter reported that EBLA-controlled accounts had about 68,000 followers before being shut down.[344] Although the number of followers does not directly correlate to the amount of political

338 Ward et al., "Russian Election Meddling Is Back."

339 Nimmo et al., "IRA Again: Unlucky Thirteen," 24–25.

340 Graphika Team, *Step Into My Parler*, 8.

341 Nimmo et al., *Secondary Infektion*, 13.

342 Ward et al., "Russian Election Meddling Is Back."

343 Ward et al.

344 Ward et al.

pressure, it indicates that EBLA's content resonated enough with social media users to convince them to follow the EBLA-controlled accounts.

On the other hand, the other Russian campaigns appeared to be less effective in creating political pressure. Since its inception in February 2020, the PeaceData site averaged about ten posts per day on the English-language page and 20 posts per day on the Arabic-language page.[345] Twitter noted that the PeaceData-associated Twitter accounts were "low quality and spammy," and assessed they did not garner much attention from other Twitter users.[346] Facebook also took down a few PeaceData-associated Facebook and Instagram accounts but did not characterize how other users engaged with these accounts.[347] The Newsroom for American and European Based Citizens outlet started in June 2020 but did not appear to attract much of a social media following. Graphika discovered that only about 14,000 users on Parler and 3,000 users on Gab followed the NAEBC site.[348] The Secondary Infektion campaign appeared to be prolific during its existence. Still, Graphika noted that the vast majority of the content produced did not garner much, if any, engagement with other users.[349] Graphika opined that the operators behind Secondary Infektion were motivated more by hitting production metrics than content engagement or virality.[350] The ability of the Russian influence campaigns to generate political pressure may have been dampened by the social media company account takedowns and exposure by media outlets and Graphika, which will be discussed in more detail in the next section.

For the third component of the Kartapolov Framework, namely confusing the political leadership, the impact of the Internet Research Agency and other Russian proxies'

---

345 Nimmo et al., "IRA Again: Unlucky Thirteen," 5.

346 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

347 Facebook, "September 2020 Coordinated Inauthentic Behavior Report."

348 Graphika Team, *Step Into My Parler*, 2.

349 Nimmo et al., *Secondary Infektion*, 8.

350 Nimmo et al., 8.

Page 1418 of 3957

actions will be discussed in the section evaluating the impact of the U.S. government's actions.

2. The Private Sector Companies' Impact and Adaptations

The effectiveness of the private sector countermeasures used against the Russian influence operations targeting the 2020 U.S. election was evaluated using the Kartapolov Framework. To combat the first component, spreading discontent in the American public, the private sector responded to take security-focused actions. Specifically, the companies enhanced their detection systems to identify and disrupt Russian influence activities before gaining much traction with their users. As a result, each of the prominent social media companies had somewhat different results from 2016 to 2020, shown in table 8.

Table 8. Social Media Account Takedowns between 2016 and 2020.[351]

Company	Number of Accounts Taken Down		
	2016	2020	Difference
Facebook	470	825	+355
Google	883	129	-754
Twitter	1,233	3,814	+2,581

While Facebook and Twitter saw an increase in IRA-controlled accounts on their platforms, Google saw a decrease in accounts taken down. A partial explanation for this phenomenon could be that Instagram, a wholly-owned Facebook subsidiary, was the most

[351] Adapted from @TwitterSafety, "June 2020: Disclosing Networks of State-Linked Information Operations We've Removed"; @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; Facebook, "February 2020 Coordinated Inauthentic Behavior Report"; Facebook, "March 2020 Coordinated Inauthentic Behavior Report"; Facebook, "April 2020 Coordinated Inauthentic Behavior Report"; Facebook, "September 2020 Coordinated Inauthentic Behavior Report"; Facebook, "August 2020 Coordinated Inauthentic Behavior Report"; Facebook, "October 2020 Coordinated Inauthentic Behavior Report"; Google Threat Analysis Group, "TAG Bulletin," August 5, 2020; Google Threat Analysis Group, "TAG Bulletin," November 17, 2020; Ward et al., "Russian Election Meddling Is Back."

conducive social media platform for propagating memes, which has become prevalent in popular culture and was also favored by the IRA.[352] Another explanation was that the IRA might have needed to shift resources away from YouTube activities to develop the PeaceData and Newsroom for American and European Based Citizens outlets.

Another method for stopping the spread of discontent in the population was for the private sector companies to share data from foreign influence-related account takedowns with third-party organizations, such as researchers and research institutions. After the 2016 U.S. Elections, each of the companies shared data with the Senate Committee on Intelligence, who in turn shared it with researchers to analyze it.[353] Since that time, each company has shared data to varying degrees with researchers and other organizations. For example, in June 2020, Twitter shared information with Stanford University regarding the detection and takedown of Chinese, Russian, and Turkish influence campaigns on their platform.[354] Twitter shared the data with Stanford as an objective third party to analyze and publish the results in service of increased transparency.[355] In September 2020, Graphika revealed Facebook had given it data regarding the PeaceData outlet.[356] In October 2020, Graphika received information from Facebook and Twitter regarding the Newsroom for American and European Based Citizens outlet.[357] These examples illustrated the social media sharing information with third parties to presumably publicize objective analysis regarding IRA disinformation and tactics to the public.

All of the major social media companies took visible measures to counter political pressure, the second component of the Kartapolov Framework, which the IRA exerted through its online influence activities on the different social media platforms. These transparency-focused actions included the increased cadence of each company's public

352 Leighton, "For Instagram's 10th Birthday, Experts Predict The Future Of Meme Culture"; Alina Polyakova, "The Kremlin's Plot against Democracy," *Foreign Affairs*, October 2020.

353 *Russian Active Measures Campaigns: Volume 1*.

354 Stanford Internet Observatory, "Analysis of June 2020 Twitter Takedowns Linked to China, Russia, and Turkey."

355 Stanford Internet Observatory.

356 Nimmo et al., "IRA Again: Unlucky Thirteen."

357 Graphika Team, *Step Into My Parler*.

notifications to the general public regarding account takedowns. A secondary transparency-focused action was each company's effort to enact and improve its advertising purchasing policies. For Facebook and Google, these improvements appeared to make it more difficult for foreign actors to purchase political advertisements.[358] Twitter went the furthest of the three social media companies by banning political ads entirely in its November 2019 announcement.[359] The third type of transparency-focused action was the attempt by companies to improve the labeling of content. Again, Twitter appeared to be the most aggressive of the three social media companies. In May 2020, Twitter announced that labeling would be applied to all content disputed, misleading, or synthetically generated.[360] In June 2020, Facebook made a similar announcement and modified its policies to improve transparency for political content and advertisements.[361] Thus, the private sector companies' collective security and transparency-related actions seemed to diminish the impact of the Russian influence operations by preventing them from gaining much traction on the social media platforms.

3. The U.S. Government's Impact – Transparency and Private Sector Partnerships

Examining the U.S. government's actions to protect the 2020 U.S. Elections through the Kartapolov Framework revealed a more robust response than in 2016. For the first element of the framework, spreading discontent across the populace, the U.S. government took a range of security and transparency-related actions to impede Russian influence operations. Likely the most significant action was the FBI's reported information sharing with the social media companies on at least four occasions, which led to the

358 Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security."

359 Twitter, "Elections Integrity."

360 Yoel Roth and Nick Pickles, "Updating Our Approach to Misleading Information," *Only on Twitter* (blog), May 11, 2020, https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.html.

361 Facebook, "Facebook - Preventing Election Interference."

Page 1421 of 3957

companies identifying and taking down multiple clusters of IRA-controlled accounts.[362] In addition, the U.S. government meeting with the private sector companies on at least two separate occasions to share information on threat trends may have added context and atmospherics to enhance the companies' detection methods.[363] Finally, the report issued by the State Department's Global Engagement Center in August 2020 may be regarded as a U.S. government transparency effort to expose Russian disinformation tactics to the American public and blunt the impact of these tactics.[364] In general, the U.S. government appeared more actively engaged with the social media companies ahead of the 2020 elections.

For the second element of the Kartapolov Framework, exerting political pressure, the U.S. government took a series of measures, which may have diffused the pressure that Russia was trying to apply through its information operations. The FBI's Protected Voice Initiative, which provided cybersecurity training to the national level political parties and presidential campaigns, was coupled with the classified threat briefings to the same organizations provided by National Counterintelligence and Security Center's Director William Evanina.[365] Furthermore, the FBI modified its victim notification process by including designated state-level election officials when notifying local or county-level election officials of cybersecurity issues.[366] Finally, the highly detailed joint NSA/FBI cybersecurity advisory regarding the Drovorub malware exposed one of the Russian

362 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; Facebook, "September 2020 Coordinated Inauthentic Behavior Report"; Facebook, "October 2020 Coordinated Inauthentic Behavior Report"; Google Threat Analysis Group, "TAG Bulletin," November 17, 2020; Graphika Team, *Step Into My Parler*.

363 Isaac and Conger, "Google, Facebook and Others Broaden Group to Secure U.S. Election"; Wagner, "Facebook Meets With FBI to Discuss 2020 Election Security."

364 Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem*, 3.

365 Federal Bureau of Investigation, "Combating Foreign Influence"; Office of the Director of National Intelligence, "Director of National Intelligence Announces Changes to Election Security Briefings."

366 Federal Bureau of Investigation, "FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure — FBI," FBI Press Releases, January 16, 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-policy-for-notifying-state-and-local-election-officials-of-cyber-intrusions-affecting-election-infrastructure.

Page 1422 of 3957

military's most potent cyber weapons, providing organizations with time to protect themselves ahead of the elections.[367] This combination of actions by the U.S. government probably ensured no significant data breaches at any national-level political parties or campaigns during the 2020 U.S Elections.

For the third element of the Kartapolov Framework, confusing the political leadership, the U.S. government, both the executive and legislative branches, appeared to be focused and decisive in its endeavors to safeguard the 2020 U.S. Elections. In September 2019, the Republican-chaired Senate Commerce Committee called a hearing with senior executives from Facebook, Google, and Twitter to learn about their progress in removing disinformation and violent content from their platforms.[368] The following year, public statements made by NCSC Director William Evanina in July 2020 and August 2020 gave a clear indication that the U.S. Intelligence Community was aware of Russian activities targeting the elections and decided to inform the American public.[369] In a similar vein, on the day after the elections closed, Christopher Krebs, Director of the Cybersecurity and Infrastructure Security Agency, stated that the U.S. government had "no evidence any foreign adversary was capable of preventing Americans from voting or changing vote tallies."[370] In October 2020, the Department of Justice indicted six officers in the Russian Military Intelligence Unit 74455, responsible for hacking attacks in Georgia and Ukraine,

---

[367] Dan Goodin, "NSA and FBI Warn That New Linux Malware Threatens National Security," *Ars Technica*, August 13, 2020, https://arstechnica.com/information-technology/2020/08/nsa-and-fbi-warn-that-new-linux-malware-threatens-national-security/.

[368] September 18, 2019.

[369] William Evanina, "Statement by NCSC Director William Evanina: 100 Days Until Election 2020," Office of the Director of National Intelligence, July 24, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020; William Evanina, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," Office of the Director of National Intelligence, August 7, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

[370] Christopher Krebs, "Statement from CISA Director Krebs Following Final Day of Voting," Cybersecurity and Infrastructure Security Agency, November 4, 2020, https://www.cisa.gov/news/2020/11/04/statement-cisa-director-krebs-following-final-day-voting.

Page 1423 of 3957

and the Winter Olympics in South Korea.[371] Some of these GRU officers had been previously indicted for hacking the Democratic National Committee in 2016.[372] Interestingly, the Department of Justice highlighted the assistance of the threat intelligence teams from Google and Cisco for this indictment.[373] Additionally, the report on Russian disinformation tactics issued by the State Department and the joint cybersecurity advisory issued by the NSA and FBI rounded out the U.S. government's multi-agency approach to exposing malign Russian activities through different avenues.

E. VOTER TURNOUT IN THE 2020 ELECTIONS

The two most important indicators of a secure and successful election were high voter turnout and no evidence of systemic voter fraud. The Pew Research Center determined that 2020 had the highest voter turnout since 1960, with approximately 158 million Americans casting ballots.[374] Table 9 shows a comparison in voter turnout between 2016 and 2020, both of which were presidential election years. In addition, multiple news organizations and think tanks on both sides of the aisle reported that the 2020 U.S. elections were free of any systemic voter fraud, impacting the results.[375]

---

[371] Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," Department of Justice, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[372] Department of Justice.

[373] Department of Justice.

[374] Drew DeSilver, "Turnout Soared in 2020 as Nearly Two-Thirds of Eligible U.S. Voters Cast Ballots for President," *Pew Research Center Fact Tank* (blog), January 28, 2021, https://www.pewresearch.org/fact-tank/2021/01/28/turnout-soared-in-2020-as-nearly-two-thirds-of-eligible-u-s-voters-cast-ballots-for-president/.

[375] Brennan Center for Justice, "It's Official: The Election Was Secure | Brennan Center for Justice," *Brennan Center for Justice* (blog), December 11, 2020, https://www.brennancenter.org/our-work/research-reports/its-official-election-was-secure; Nick Corasaniti, Reid J. Epstein, and Jim Rutenberg, "The Times Called Officials in Every State: No Evidence of Voter Fraud," *New York Times*, November 11, 2020, https://www.nytimes.com/2020/11/10/us/politics/voting-fraud.html; Justin Grimmer, Haritz Garro, and Andrew Eggers, "No Evidence For Voter Fraud: A Guide To Statistical Claims About The 2020 Election," Text (Palo Alto, CA: Hoover Institution, February 3, 2021), https://www.hoover.org/research/no-evidence-voter-fraud-guide-statistical-claims-about-2020-election; Reality Check Team, "US Election 2020: Fact-Checking Trump Team's Main Fraud Claims," BBC News, November 23, 2020, https://www.bbc.com/news/election-us-2020-55016029.

Page 1424 of 3957

Table 9. Comparison of Overall Voter Turnout for Presidential Elections.[376]

Election Year	Number of Voters Turning Out	Percentage of Voter Turnout
2016	137,500,000	61.4%
2020	158,000,000	66.2%
Change	**+20,500,000**	**+4.8%**

It is still unclear whether the IRA's operations contributed to the record number of Americans to vote or suppress turnout among Black voters in 2016. The U.S. Census Bureau will not have an analysis of voter demographics for the 2020 elections until late in 2021. Despite the lack of demographic data for 2020, the Russian attempts to depress voter turnout were unsuccessful as Americans turned out in record numbers.

F. CONCLUSIONS FROM THE 2020 U.S. ELECTIONS

Reflecting on the 2020 elections, three main themes emerged. First, the Russians continued their efforts to target the U.S. elections while shifting tactics to avoid detection. Second, the social media companies, along with news media and research organizations, were able to identify and disrupt the evolving Russian disinformation campaigns. Third, the U.S. government was a more active player in securing the elections, primarily through its information sharing with the social media companies, political organizations, and the American public.

Despite the best efforts of the Russians, social media companies, news media, and research organizations were able to detect, expose, and disrupt the activities of the Internet Research Agency and their other online groups, namely Secondary Infektion and the GRU. Although America's private sector may have been caught unaware during the 2016 elections, it was on heightened alert ahead of 2020, with the noteworthy efforts of CNN,

[376] Adapted from DeSilver, "Turnout Soared in 2020 as Nearly Two-Thirds of Eligible U.S. Voters Cast Ballots for President"; Krogstad and Lopez, "Black Voter Turnout Fell in 2016."

Reuters, and Graphika exposing Russian disinformation activities and paving the way for the social media companies to shut down their social media accounts.

The U.S. government's response to the Russian influence campaign appeared more robust before the 2020 elections than in the 2016 or 2018 elections. These efforts comprised a series of transparency and security-related measures. The most important actions taken by the U.S. government may have been the information sharing with the social media companies to expose Russia's different operations and shut down its accounts. In addition, the U.S. government's information-sharing may have helped the social media companies secure their platforms by identifying malign Russian influence activities. At first glance, the U.S. government's other responses, such as economic sanctions and indictments, may not seem impactful because the United States does not have an extradition treaty with Russia. As a result, the sanctioned or indicted individuals may never be brought to justice in the U.S. court system. However, a critical role of sanctions and indictments is to provide transparency, i.e., factual narratives of the crimes perpetrated by Russia that informs the American public.

It took the collaborative efforts of the private sector, in the form of social media companies, researcher organizations, and news media, and the public sector, in the form of the executive and legislative branches of the U.S. government, to turn back the Putin-sanctioned disinformation operations which were targeting the 2020 U.S. elections. These collective actions were viewed through the lens of the Kartapolov Framework to determine their effectiveness in countering Russian influence operations. The next chapter will identify and examine the most effective countermeasures and provide recommendations for safeguarding future elections.

Page 1426 of 3957

IV. CONCLUSIONS AND RECOMMENDATIONS TO COUNTER RUSSIA IN THE FUTURE

> The problem of foreign actors trying to influence the American electorate is not going away and, given the current partisan divides in this country, may find fertile ground in which to grow in the future.
>
> — Mark Warner, March 16, 2021

Senator Warner, Chair of the Senate Intelligence Committee, made the above statement after the Office of the Director of National Intelligence released its report appraising foreign threats to the 2020 U.S. elections. This report, backed by the entire U.S. Intelligence Community, assessed that Russia was actively trying to influence the elections through information operations.[377] Furthermore, the report forecasts Russia will continue to interfere in future U.S. elections to degrade the United States' global credibility and weaken its influence overseas.[378] In anticipation of the continued Russian influence threat, this chapter provides a final summation of the American efforts to protect the 2020 elections and concludes which efforts were the most effective. Based on these conclusions, recommendations have been proposed to protect future U.S. elections. These recommendations are derived, in part, from proposals by subject matter experts in a variety of fields.

A. CONCLUSIONS – THERE IS NO END GAME

The major social media companies and the U.S. government's efforts to protect the 2020 U.S. elections against Russian malign influence campaigns appeared to be generally successful. Using the Kartapolov Framework in this thesis provided a systematic method to analyze the effectiveness of the American countermeasures qualitatively. As a reminder, the framework is a mental model devised by Thomas Wilhelm, a U.S. Army researcher, to understand better the Russian military's perspective in conducting information operations

[377] Office of the Director of National Intelligence, "Intelligence Community Assessment on Foreign Threats to the 2020 U.S. Federal Elections," 2.

[378] Office of the Director of National Intelligence, 5.

Page 1427 of 3957

to further its objectives.[379] The most effective measure taken by the major social media companies was the rapid detection and takedown of fake accounts and content generated by the Internet Research Agency and other Russian proxies. The social media companies' other efficacious efforts included publicizing these account takedowns, which promoted transparency to the American public, and partnering with other organizations, such as news media and researchers, to expose Russian influence activities which were not on the social media platforms. The most effective measure taken by the U.S. government was likely its information-sharing efforts with the social media companies to help them identify previously unknown Russian influence activities on their platforms. The U.S. government's other effective efforts included its initiative to inculcate good cybersecurity practices among the national-level political parties and campaigns and regular public messaging about malign influence activities to the American populace.

The Internet Research Agency resembled a professional marketing firm that employed both technology and psychology to maximum effect.[380] It took advantage of easy-to-use social media platforms to reach millions of U.S. citizens.[381] The IRA recognized the existing dissension among different sectors of the American population and exploited it to drive people further into tribalism.[382] Over the past several years, the IRA honed its skills and precisely identified specific in-groups it wanted to influence. On the right side of the political spectrum, the IRA focused on issues such as illegal immigration, gun rights, religious freedom, anti-abortion, and the general fear of change.[383] Although challenging, if not impossible to quantify, the IRA's influence activities may have reinforced these people's in-group beliefs, which could have potentially activated them to vote for Trump. On the left side of the political spectrum, the IRA appeared to play on the fears and frustrations of the more racially and ideologically diverse group to suppress voter

379 Wilhelm, "A Russian Military Framework," 33.

380 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

381 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 39.

382 *Report on Russian Active Measures*, 4.

383 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 99.

Page 1428 of 3957

turnout.[384] The IRA's main shift in tactics from 2016 to 2020 was its creation of fake news outlets appealing to far-right conservatives, in the form of the Newsroom for American and European Based Citizens, and ultraliberals, in the form of the PeaceData site.[385] Ostensibly, the IRA's rationale for this shift was to control its own content and avoid the aggressive disruption tactics of the major social media companies. The IRA's other significant shift was to use indigenous workers in other countries to mask its true identity, explicitly creating the front organization known as Eliminating Barriers for the Liberation of Africa.[386]

The Internet Research Agency's role in influencing the 2016 and 2020 U.S. Presidential Elections may have been marginal but still impactful. That being said, the IRA's influence in 2020 was significantly diminished compared to its efforts in 2016. The primary reason was that the IRA's activities were unnoticed and unconstrained in 2016 but were quickly detected and disrupted in 2020 by the major social media companies and the U.S. government. One of the IRA's primary goals was to suppress Black voter turnout.[387] An illustrative statistic was the decline of Black voter turnout in 2016 by seven percent compared to the 2012 elections.[388] In 2020, Black voter turnout rebounded by four percent over the 2016 levels.[389] In addition, other minority groups had significant increases in voter turnout for 2020. Hispanic voter turnout increased by six percent, and Asian voter turnout increased by ten percent.[390] These 2020 turnout results showed the ineffectiveness of the IRA's efforts.

---

384 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3.

385 Graphika Team, *Step Into My Parler*, 2; Nimmo et al., "IRA Again: Unlucky Thirteen," 1.

386 Ward et al., "Russian Election Meddling Is Back."

387 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 18.

388 Krogstad and Lopez, "Black Voter Turnout Fell in 2016."

389 William H. Frey, *Turnout in 2020 Election Spiked among Both Democratic and Republican Voting Groups, New Census Data Shows* (Washington, DC: Brookings, 2021), https://www.brookings.edu/research/turnout-in-2020-spiked-among-both-democratic-and-republican-voting-groups-new-census-data-shows/.

390 Frey.

Page 1429 of 3957

Many factors are at play when trying to measure the effects of Russia's influence operations. First-order effects include real users interacting with inauthentic content, Russian-bot amplification of divisive organic content, and IRA-controlled accounts communicating directly with real users. Second-order effects include changes to the social network itself by the actions mentioned above and contemporaneous sociopolitical events influencing discussions. Due to how the U.S. Electoral College process awards presidential electoral votes, the U.S. Presidency was decided by about 78,000 votes combined across Michigan, Pennsylvania, and Wisconsin for 2016.[391] In 2020, Biden won the presidency by about 45,000 votes combined across Arizona, Georgia, and Wisconsin.[392] In both presidential elections, voter turnout was near historical highs.[393] In order to protect future elections in the United States, a whole-of-society approach will be needed to counter malign influence from Russia and other adversarial nation-states.

B. RECOMMENDATIONS FOR PROTECTING FUTURE ELECTIONS FROM RUSSIAN INTERFERENCE

Like the Cold War's nuclear arms race, the United States may be in a new information operations race with Russia. Based on the evaluation of the Russian actions and the effectiveness of the American responses, this section makes recommendations for protecting future elections that have been drawn from experts in the U.S. government, non-governmental organizations, and academic institutions. The three types of possible actions are broadly categorized as security, transparency, and resiliency measures.[394] Social media companies and the U.S. government have mainly focused on the first two types of measures: security and transparency. Although these measures proved to be successful for the 2020 elections and are essential to safeguarding our democracy and the public

391 Dante Chinni, "Did Biden Win by a Little or a Lot? The Answer Is ... Yes.," NBC News, December 20, 2020, https://www.nbcnews.com/politics/meet-the-press/did-biden-win-little-or-lot-answer-yes-n1251845.

392 Chinni.

393 Frey, *Turnout in 2020 Election Spiked*; Krogstad and Lopez, "Black Voter Turnout Fell in 2016."

394 Cederberg et al., *National Counter-Information Operations Strategy*; DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*; King and Gallagher, *Cybersecurity Lessons from the Pandemic*; *Report on Russian Active Measures*; *Russian Active Measures Campaigns: Volume 1*.

perception of fair elections, they may not be sufficient for future elections because of the current political rancor in the United States. To that end, resiliency measures will be the third critical component to promote a flourishing American democracy.

1. Security Measures

Security measures serve three purposes: (1) prevention of disinformation or data breaches, (2) deterrence of damaging actions or operations, and (3) punishment of criminal or other harmful actions.[395] These recommendations came from an evaluation of U.S. government and private sector actions taken to counter the efforts of the Internet Research Agency and other Russian actors. The most impactful measures against the evolving threat from Russian information operations were distilled from various U.S. government, non-governmental organizations, and academic literature. The proposed security measures, summarized in Table 10, include enhanced cybersecurity, enhanced disinformation detection, economic sanctions, information sharing, and the establishment of a fusion center. Items highlighted in yellow are existing measures. Items highlighted in green are new proposed measures.

[395] Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; U.S. Congress. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns: Volume 1*, 54.

Page 1431 of 3957

Table 10. Security Measures for Countering Russian Information Operations.

Measure	Description	Responsibility
Enhanced Cybersecurity	Build up cyber expertise and defenses to prevent breaches of election infrastructure and other government infrastructure.[396]	• Government • Private Sector
Enhanced Detection	Use advanced technologies, such as artificial intelligence, to quickly detect and take down disinformation. These technologies can augment other types of content moderation.[397]	• Private Sector
Economic Sanctions	Deter malicious activities and impose costs for actors who seek to interfere in U.S. elections and the democratic process.[398]	• Government
Information Sharing among Government, Social Media Companies, and External Researchers	Share threat intelligence among key stakeholders to detect, identify, and disrupt disinformation campaigns.[399]	• Government • Private Sector • Researchers
National Counter Information Operations Center	Create an interagency fusion center under the Office of the Director of National Intelligence to coordinate strategy, intelligence, and operations regarding disinformation campaigns.[400]	• Government

The first recommendation is for the U.S. government to continue providing cybersecurity training and briefings to relevant stakeholders. The Russians did not cause any significant data breaches of any national-level political organizations or campaigns for

396 Adapted from O'Connor et al., *Cyber-Enabled Foreign Interference*, 6; *Russian Active Measures Campaigns: Volume 1*, 55; *Report on Russian Active Measures*, 121–22.

397 Adapted from Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; Cartwright, Weir, and Frank, "Fighting Disinformation Warfare with Artificial Intelligence," 73.

398 Adapted from Cederberg et al., *National Counter-Information Operations Strategy*, 11; Polyakova, "The Kremlin's Plot against Democracy."

399 Adapted from Cederberg et al., *National Counter-Information Operations Strategy*, 12; Hanlon, *A Long Way to Go*, 10; O'Connor et al., *Cyber-Enabled Foreign Interference*, 6.

400 Adapted from Cederberg et al., *National Counter-Information Operations Strategy*, 12; Terry L. Thompson, "No Silver Bullet: Fighting Russian Disinformation Requires Multiple Actions," *Georgetown Journal of International Affairs* 21 (2020): 182–94, https://doi.org/10.1353/gia.2020.0033.

the 2020 U.S. Elections. Some of this success can be attributed to the cybersecurity training and briefings provided to the political organizations and campaigns by the FBI and DHS.[401] The prevention of data breaches in the future will mean less fodder for the Russians or other adversarial governments to incorporate into disinformation campaigns. These cybersecurity enhancement actions should continue to be used moving forward as technological changes happen rapidly.[402]

The second recommendation calls for advanced technologies, including artificial intelligence, to be developed and deployed on social media and news platforms to enhance the detection, monitoring, and neutralization of covert malign foreign influence activities.[403] These malign activities may take the form of disinformation content, botnet amplifications, or incitement of divisive issues. The neutralization can take the form of traditional account takedowns or marking the accounts and content with labels identifying their origins and providing access to sources of factual information. Advanced technology tools should be developed so platform companies or users may detect disinformation or influence activities and crowdsource the appropriate neutralization methods.[404] The removal of foreign disinformation content can help promote the integrity of American free speech and halt the erosion of trust in the electoral process.[405] Due to the First Amendment (free speech) and Fourth Amendment (privacy) constraints on the U.S. government, advanced detection and removal technologies are best employed by private sector companies.[406]

---

401 Federal Bureau of Investigation, "Combating Foreign Influence"; Federal Bureau of Investigation, "Protected Voices"; Office of the Director of National Intelligence, "Director of National Intelligence Announces Changes to Election Security Briefings."

402 U.S. Congress. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns: Volume 1*, 55–56.

403 Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; Hanlon, *A Long Way to Go*, 2; Marcellino et al., *Foreign Interference in the 2020 Election*.

404 Cartwright, Weir, and Frank, "Fighting Disinformation Warfare with Artificial Intelligence," 73.

405 Suzanne E. Spaulding and Eric Goldstein, *Countering Adversary Threats to Democratic Institutions: An Expert Report* (Washington, DC: Center for Strategic and International Studies, 2018), 4, https://www.csis.org/analysis/countering-adversary-threats-democratic-institutions.

406 Facebook, "The State of Influence Operations 2017–2020," *About Facebook* (blog), May 26, 2021, 5, https://about.fb.com/news/2021/05/influence-operations-threat-report/.

Page 1433 of 3957

The third recommendation is the continued use of economic sanctions by the U.S. government. Continued sanctions by the Department of Treasury against Russian individuals and entities appeared to have had a significant impact on Russia as a security measure. As anecdotal evidence, one of the primary discussion topics at the infamous Trump Tower meeting was supposed to be the previously mentioned Magnitsky Act.[407] This act imposed severe financial sanctions on the close allies of Putin and continues to be a thorn in his side.[408] The sanctions imposed in 2018 may have an add-on effect to the Magnitsky Act.[409] Economic sanctions should continue to be part of a broad range of tools utilized concurrently by the U.S. government for deterrent and punitive effects.[410]

The fourth recommendation is the establishment of formal information-sharing mechanisms. Information sharing among different organizations is occurring, but on an ad hoc basis, as was seen ahead of the 2020 elections when the FBI shared information with the social media companies to help them detect the disinformation campaigns on their platforms.[411] Information sharing among relevant stakeholders in the malign foreign influence space should be formalized and standardized. Appropriate sharing should occur between social media companies, those companies and the U.S. government, and researchers with the U.S. government and social media companies. The Information Sharing and Analysis Center (ISAC) model has proven successful in different sectors for information sharing. One example of this is the Financial Sector ISAC (FS-ISAC).[412] Currently, no Social Media Sector ISAC exists. This gap is likely because of the competitive nature of social media companies. Still, the FS-ISAC has shown that financial

---

407 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 185.

408 Ioffe, "Why Does the Kremlin Care So Much about the Magnitsky Act?"

409 Rennack, *U.S. Sanctions on Russia*.

410 Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; Cederberg et al., *National Counter-Information Operations Strategy*, 12.

411 Facebook, "September 2020 Coordinated Inauthentic Behavior Report"; Facebook, "October 2020 Coordinated Inauthentic Behavior Report"; Google Threat Analysis Group, "TAG Bulletin," November 17, 2020; @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

412 ISAO Standards Organization, "Financial Services ISAC," ISAO Standards Organization, accessed April 21, 2021, https://www.isao.org/information-sharing-group/sector/financial-services-isac/.

Page 1434 of 3957

institutions can set aside rivalries for the common good. The benefit of having an information-sharing organization would be to establish norms and best practices for the private sector, in addition to sharing threat indicators for mutual benefit.

The last recommendation is for the U.S. government to establish a National Counter Information Operations Center as an interagency fusion center and focal point for countering disinformation campaigns.[413] The bipartisan U.S. Cyberspace Solarium Commission pointed out that the 2020 National Defense Authorization Act (NDAA) provided a provision wherein the Office of the Director of National Intelligence could form a "Social Media Data and Threat Analysis Center."[414] This center could be modeled after the National Counterterrorism Center, which also operates under the Office of the Director of National Intelligence. The commission envisioned a center that would allow the relevant U.S. government elements to work alongside social media companies to combat disinformation.[415] In April 2021, the Office of the Director of National Intelligence responded to the new legislation by announcing it was establishing "the Foreign Malign Influence Center "in light of evolving threats and in support of growing policy and congressional requirements."[416] As of the writing of this thesis, no further details have been provided by ODNI, but the announcement appears to be in line with the functionality of the center proposed in the 2020 NDAA.

2. Transparency Measures

Transparency measures are designed to build trust and confidence in organizations by sharing relevant information with the general public.[417] The transparency measures proposed include a public communications strategy, content labeling standards, updated

---

413 Cederberg et al., *National Counter-Information Operations Strategy*, 12; Thompson, "No Silver Bullet."

414 King and Gallagher, *Cybersecurity Lessons from the Pandemic*, 12.

415 King and Gallagher, 12.

416 Martin Matishak, "Intelligence Community Creating Hub to Gird against Foreign Influence," *Politico*, April 26, 2021, https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604.

417 Cederberg et al., *National Counter-Information Operations Strategy*, 12.

Page 1435 of 3957

political advertising and campaign finance laws, and transparency reporting. Table 11 summarizes the proposed transparency measures to combat Russian disinformation campaigns. As with the last table, yellow highlighted items are existing measures, and green highlighted items are new proposed measures.

Table 11. Transparency Measures for Countering Malign Russian Influence.

Measure	Description	Responsibility
Public Communication Strategy	Devise and execute a strategy to counter disinformation in the public sphere, both domestically and overseas, through multiple avenues.[418]	• Government • Private Sector
Content Labeling	Establish and use a standardized method for labeling disinformation and misinformation on websites and social media platforms.[419]	• Private Sector
Transparency Reporting	Provide the public with reports that summarize the quantity and type of disinformation on a company's platform. These reports should include raw data for third parties, such as researchers, to conduct detailed analyses.[420]	• Private Sector • Researchers
Update Political Advertising and Campaign Finance Laws	Strengthen current statutes to improve transparency and prevent foreign entities from purchasing advertisements or donating to political campaigns.[421]	• Government

[418] Adapted from Cederberg et al., 11–12; Marcellino et al., *Foreign Interference in the 2020 Election*; Polyakova, "The Kremlin's Plot against Democracy."

[419] Adapted from Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 2; Hanlon, *A Long Way to Go*, 6; Thompson, "No Silver Bullet."

[420] Adapted from DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1; Hanlon, *A Long Way to Go*, 1; Thompson, "No Silver Bullet."

[421] Adapted from Cederberg et al., *National Counter-Information Operations Strategy*, 12; *Report on Russian Active Measures*, 127.

First, a public communications strategy would be a whole-of-government plan to effectively counter disinformation and propaganda campaigns being waged against the American populace.[422] An effective strategy would involve providing counter-narratives using factual information across various mediums to ensure the public received it, such as through news media and social media outlets.[423] It would also involve exposing false or misleading content and the origins of this information so Americans could understand how they were being targeted.[424]

Second, the private sector companies should also standardize and expand their use of labeling for disinformation, misleading content, and the origins of content.[425] This change would allow users to decide for themselves how to think about and handle the content. As an example, Twitter and Facebook have started labeling misleading tweets and posts by government officials.[426] The Foreign Agent Registration Act (FARA) is the U.S. government's version of what Twitter is doing regarding labeling.[427] FARA mandates that all agents of foreign governments register with the Department of Justice and ensure all of their content in advertising or other messaging is prominently labeled.[428] However, this statute was enacted in 1938 and could use an update to consider current malign influence efforts by Russia and other countries.[429] Congress should provide legislative fixes to enhance the transparency of foreign involvement with U.S. officials or political

---

422 Cederberg et al., *National Counter-Information Operations Strategy*, 11.

423 Cederberg et al., 11.

424 Marcellino et al., *Foreign Interference in the 2020 Election*; Polyakova, "The Kremlin's Plot against Democracy."

425 Hanlon, *A Long Way to Go*, 6.

426 Facebook, "Facebook - Preventing Election Interference"; Twitter, "Elections Integrity."

427 Jessica Brandt and Josh Rudolph, *Spies and Money: Legal Defenses Against Foreign Interference in Political Campaigns* (Washington, DC: Alliance for Security Democracy, German Marshall Fund, 2021), https://securingdemocracy.gmfus.org/spies-and-money-legal-defenses-against-foreign-interference-in-political-campaigns/.

428 Brandt and Rudolph.

429 Carolyn Kenney, Max Bergmann, and James Lamond, *Understanding and Combating Russian and Chinese Influence Operations* (Washington, DC: Center for American Progress, 2019), 8, https://www.hsdl.org/?view&did=822729.

candidates.[430] This addendum includes foreign businesses and consultants who support political campaigns, as well as the disclosure of any financial interests a political candidate may have overseas.

Third, transparency reports are the key mechanism for private sector organizations to share information with the American public.[431] These reports should be expanded to include more nuanced details about foreign influence activities detected and thwarted on social media platforms. All social media companies should also make public their entire archives of malign covert influence content that was taken down.[432] These archives will enable general users, as well as researchers and non-governmental organizations, to analyze the data and provide reports to the American populace. The relationship between the companies and the researchers can help the companies build capacity to analyze malign foreign influence efforts and earn public trust from engaging with independent researchers.

Last, both political advertising and campaign finance laws should be strengthened by closing loopholes to identify the buyers and donors more quickly while also considering the exponential growth of online platforms for advertising and fundraising.[433] Current technology advancements have allowed foreign entities to anonymize or obscure their identities and origins. The House Intelligence Committee noted loopholes in current campaign finance laws that allow foreign entities to provide services to political campaigns.[434] Improved political advertising and campaign finance laws will allow the American public to make informed decisions during the elections.

---

[430] McFaul, *Securing American Elections*, 55.

[431] DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1; Facebook, "Threat Report," 5; Hanlon, *A Long Way to Go*, 1.

[432] DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1; Hanlon, *A Long Way to Go*, 10; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 40.

[433] Cederberg et al., *National Counter-Information Operations Strategy*, 12; "Page 1 - Introduction," n.d., 127.

[434] U.S. Congress. House Permanent Select Committee on Intelligence, *Report on Russian Active Measures*, 127.

3. Resiliency Measures

The last but perhaps most crucial measure for consideration is resiliency. The 2021 Intelligence Community's annual threat assessment named Russia as one of "the most serious intelligence threats to the United States" and warned that the Russian government would continue its efforts to propagate dissension in the American populace.[435] In combating future Russian influence campaigns, the two relevant facets of resiliency are improved media literacy and critical thinking for the American public.[436]

Improved media literacy requires both educational and technological components. One study showed that media literacy education for adolescents had "more to do with promoting an understanding of media content and production, rather than simply forming habits of consumption."[437] The government, news media, and social media companies all need to play a role in helping both children and adults understand media content origination and generation.[438] The solutions include public service announcements that are informed by media literacy experts, education programs for school-aged children, and career development or continuing education programs for adults.[439]

Technological enhancements are also needed to improve media literacy. In our current digital age, Americans are awash with overwhelming amounts of information, much of which is false or misleading. A recent study showed that exposure to inaccurate or misleading information on Facebook might slow down or stop users' knowledge

---

435 Office of the Director of National Intelligence, *2021 Annual Threat Assessment of the U.S. Intelligence Community*, 11.

436 McFaul, *Securing American Elections*, 8.

437 Sebastián Valenzuela, Ingrid Bachmann, and Marcela Aguilar, "Socialized for News Media Use: How Family Communication, Information-Processing Needs, and Gratifications Determine Adolescents' Exposure to News," *Communication Research* 46, no. 8 (2016): 1111, https://doi.org/10.1177/0093650215623833.

438 Spaulding and Goldstein, *Countering Adversary Threats to Democratic Institutions*, 11.

439 Cederberg et al., *National Counter-Information Operations Strategy*, 11; Jon Roozenbeek and Sander van der Linden, "Breaking Harmony Square: A Game That 'Inoculates' against Political Misinformation," *Harvard Kennedy School Misinformation Review* 1, no. 8 (2020): 1–26, https://doi.org/10.37016/mr-2020-47; Spaulding and Goldstein, *Countering Adversary Threats to Democratic Institutions*, 4.

Page 1439 of 3957

acquisition.[440] All of this content, if made by Americans, is considered free speech. A thornier issue is the artificial amplification of American free speech by Russia or other foreign actors through social media botnets.[441] Artificial intelligence and other advanced technologies will be needed to detect and take down the Russian-controlled bots generating or amplifying malicious content while distinguishing it from First Amendment protected American speech.[442]

One of the essential skills needed for each American is critical thinking, i.e., the ability to discern fact from fiction to make informed conclusions and decisions.[443] Although the focus of this thesis was Russian disinformation campaigns, domestic disinformation operations also featured prominently ahead of the 2020 elections.[444] Critical thinking is an important measure that can be used to examine information despite its origin and is already being taught to some degree as a part of different school subjects such as language arts, mathematics, and social studies. A vital part of a good school curriculum should teach students how to be critical and discerning in their digital media consumption as references and sources for their other coursework.[445]

Furthermore, Americans can learn from other democracies targeted by Russian propaganda. Even with the unrelenting assault of Russian information operations, the democracies in former Soviet Bloc countries appear to have relatively informed and resilient electorates because media literacy and critical thinking are indoctrinated into their

---

[440] Sangwon Lee and Michael Xenos, "Social Distraction? Social Media Use and Political Knowledge in Two U.S. Presidential Elections," *Computers in Human Behavior* 90 (January 2019): 22, https://doi.org/10.1016/j.chb.2018.08.006.

[441] Linvill and Warren, "Engaging with Others," 3.

[442] Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; Cartwright, Weir, and Frank, "Fighting Disinformation Warfare with Artificial Intelligence," 1.

[443] Spaulding and Goldstein, *Countering Adversary Threats to Democratic Institutions*, 11.

[444] Scott Jaspar, "Why Foreign Election Interference Fizzled in 2020," *Atlantic Council* (blog), November 23, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/why-foreign-election-interference-fizzled-in-2020/.

[445] Belinha S. de Abreu, *Teaching Media Literacy*, 2nd ed. (Chicago: American Library Association, 2019), 10.

entire education and news media ecosystem.[446] European media platforms do not feature standardized labeling of disinformation or state-sponsored content. Though these Eastern European countries do not have the economic or technological advantages of the United States, they seem to be inoculated from the effects of Russian disinformation operations.[447] Improved media literacy and critical thinking will help Americans discern what they are reading to make better-informed decisions regarding elections and other vital issues.[448]

During his farewell speech after serving a second term in office, George Washington stated, "Against the insidious wiles of foreign influence...the jealousy of a free people ought to be constantly awake, since history and experience prove that foreign influence is one of the most baneful foes of republic government."[449] Those words seem prescient today, well over two hundred years later. Except for an interlude from the end of the Cold War in 1991 to 2014, Russia has waged a campaign of information warfare to tear the fabric of Western democracy through wide-ranging operations on social media platforms targeting Americans.[450] Both the U.S. government and major social media companies were caught flatfooted in 2016 but took a series of security and transparency actions since then to counter the ongoing Russian efforts targeting U.S. elections specifically and American democracy more broadly. Hopefully, incorporating the existing and proposed measures will help repair and strengthen the framework of American democracy for the 21st century.

---

446 John R. Raines, *Countering Russian Disinformation: Europe Dusts Off the Mighty Wurlitzer*, E-Notes (Philadelphia, PA: Foreign Policy Research Institute, 2015), 6, http://www.fpri.org/docs/haines_-_wurlitzer.pdf.

447 Raines, 6.

448 Spaulding and Goldstein, *Countering Adversary Threats to Democratic Institutions*, 12.

449 George Washington, "Washington's Farewell Address," Digital History, 1796, http://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=3&psid=160.

450 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 4; National Museum of American History, "The End of the Cold War," Cold War Timeline, 2000, https://americanhistory.si.edu/subs/history/timeline/end/.

THIS PAGE INTENTIONALLY LEFT BLANK

Page 1442 of 3957

LIST OF REFERENCES

Abrams, Steve. "Beyond Propaganda: Soviet Active Measures in Putin's Russia." *Connections: The Quarterly Journal* 15, no. 1 (2016): 5–31. https://doi.org/10.11610/Connections.15.1.01.

Abreu, Belinha S. de. *Teaching Media Literacy*. 2nd ed. Chicago: American Library Association, 2019.

Alperovitch, Dmitri. "Our Work with the DNC: Setting the Record Straight." *Crowdstrike Blog* (blog), June 5, 2020. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Barbu, Viorel. "The Hybrid War in the East-West Paradigm." In *Strategic Changes in Security and International Relations*, edited by Dorin Corneliu Pleșcan, Ion Puricel, Daniel Ghiba, Lucian Dragoș Popescu, Ioana Enache, and Tudorel Lehaci, XVI, Part 2:101–12. Bucharest, Romania: "Carol I" National Defence University, 2020. https://www.strategii21.ro/A/2020-04.%20STRATEGIC%20CHANGES%20IN%20SECURITY%20AND%20INTERNATIONAL%20RELATIONS/FSA_2020_VOLUMUL%202.pdf#page=102.

Birch, Sarah. "Perceptions of Electoral Fairness and Voter Turnout." *Comparative Political Studies* 43, no. 12 (December 1, 2010): 1601–22. https://doi.org/10.1177/0010414010374021.

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger. *Countering Russian Social Media Influence*. Santa Monica, CA: RAND Corporation, 2018. https://doi.org/10.7249/RR2740.

Brandt, Jessica, and Josh Rudolph. *Spies and Money: Legal Defenses Against Foreign Interference in Political Campaigns*. Washington, DC: Alliance for Security Democracy, German Marshall Fund, 2021. https://securingdemocracy.gmfus.org/spies-and-money-legal-defenses-against-foreign-interference-in-political-campaigns/.

Brennan Center for Justice. "It's Official: The Election Was Secure | Brennan Center for Justice." *Brennan Center for Justice* (blog), December 11, 2020. https://www.brennancenter.org/our-work/research-reports/its-official-election-was-secure.

Buzzetto-More, Nicole A. "Social Media and Prosumerism." *Issues in Informing Science and Information Technology* 10 (July 2013): 67–80.

Page 1443 of 3957

Cartwright, Barry, George Weir, and Richard Frank. "Fighting Disinformation Warfare with Artificial Intelligence: Identifying and Combatting Disinformation Attacks in Cloud-Based Social Media Platforms." In *CLOUD COMPUTING 2019 Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization*, edited by Bob Duncan, Yong Woo Lee, Magnus Westerlund, and Andreas Aßmuth, 73–77. Venice, Italy: IARIA, 2019. https://www.researchgate.net/publication/333024381_CLOUD_COMPUTING_2019_Proceedings_of_the_Tenth_International_Conference_on_Cloud_Computing_GRIDs_and_Virtualization.

Cederberg, Gabriel, Jordan D'Amato, Corinna Fehst, Simon Jones, Kunal Kothari, Aleksandra Milcheva, and Irene Solaiman. *National Counter-Information Operations Strategy*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019. https://www.belfercenter.org/publication/national-counter-information-operations-strategy.

Chekinov, S.G., and S.A. Bogdanov. "The Nature and Content of New Generation War." *Military Thought*, no. 4 (February 2013): 12–23.

Chinni, Dante. "Did Biden Win by a Little or a Lot? The Answer Is ... Yes." NBC News, December 20, 2020. https://www.nbcnews.com/politics/meet-the-press/did-biden-win-little-or-lot-answer-yes-n1251845.

Chowdhury, Farhan Asif, Dheeman Saha, Md Rashidul Hasan, Koustuv Saha, and Abdullah Mueen. "Examining Factors Associated with Twitter Account Suspension Following the 2020 U.S. Presidential Election." *ArXiv* 2101, no. 09575 (January 23, 2021). https://arxiv.org/pdf/2101.09575.pdf.

Clement, J. "Social Media Usage in the United States." Statista, May 19, 2020. https://www.statista.com/topics/3196/social-media-usage-in-the-united-states/.

Colton, Timothy J., and Michael McFaul. "Russian Democracy under Putin." *Problems of Post-Communism* 50, no. 4 (July 2003): 12–21. https://doi.org/10.1080/10758216.2003.11656043.

Corasaniti, Nick, Reid J. Epstein, and Jim Rutenberg. "The Times Called Officials in Every State: No Evidence of Voter Fraud." *New York Times*, November 11, 2020. https://www.nytimes.com/2020/11/10/us/politics/voting-fraud.html.

Cybersecurity and Infrastructure Security Agency. "Election Infrastructure Security." Cybersecurity and Infrastructure Security Agency. Accessed June 3, 2020. https://www.cisa.gov/election-security.

Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, Public Law 20 (2018). https://www.hsdl.org/?view&did=829787.

Page 1444 of 3957

Department of Homeland Security and Federal Bureau of Investigation. *GRIZZLY STEPPE – Russian Malicious Cyber Activity*. Washington, DC: Department of Homeland Security and Federal Bureau of Investigation, 2016. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

Department of Homeland Security and Office of the Director of National Intelligence. *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*. Washington, DC: Department of Homeland Security and Office of the Director of National Intelligence, 2016. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

Department of Justice. "Russian National Charged with Interfering in U.S. Political System." United States Attorney's Office Eastern District of Virginia, October 19, 2018. https://www.justice.gov/usao-edva/pr/russian-national-charged-interfering-us-political-system.

———. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." Department of Justice, October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

———. "Special Counsel's Office." Department of Justice Special Counsel's Office, October 16, 2017. https://www.justice.gov/sco.

Department of State. "Senior Administration Official on Russia." U.S. Department of State, August 31, 2017. https://2017-2021.state.gov/senior-administration-official-on-russia/.

DeSilver, Drew. "Turnout Soared in 2020 as Nearly Two-Thirds of Eligible U.S. Voters Cast Ballots for President." *Pew Research Center Fact Tank* (blog), January 28, 2021. https://www.pewresearch.org/fact-tank/2021/01/28/turnout-soared-in-2020-as-nearly-two-thirds-of-eligible-u-s-voters-cast-ballots-for-president/.

DiResta, Renée, and Shelby Grossman. *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*. Palo Alto, CA: Stanford University, 2019. https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks.

DiResta, Renee, Kris Shaffer, Becky Ruppel, Robert Matney, Ryan Fox, Jonathan Albright, Ben Johnson, and Canfield Research. *The Tactics & Tropes of the Internet Research Agency*. New York: New Knowledge, 2018.

Page 1445 of 3957

Elections Infrastructure Government Coordinating Council, and Election Infrastructure Sector Coordinating Executive Committee. "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees," November 12, 2020. https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

Evanina, William. "Statement by NCSC Director William Evanina: 100 Days Until Election 2020." Office of the Director of National Intelligence, July 24, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020.

———. "Statement by NCSC Director William Evanina: Election Threat Update for the American Public." Office of the Director of National Intelligence, August 7, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

Ewing, Philip. "Fact Check: Why Didn't Obama Stop Russia's Election Interference In 2016?" National Public Radio, February 21, 2018. https://www.npr.org/2018/02/21/587614043/fact-check-why-didnt-obama-stop-russia-s-election-interference-in-2016.

Fabian, Sandor. "The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy." *Defense & Security Analysis* 35, no. 3 (2019): 308–25. https://doi.org/10.1080/14751798.2019.1640424.

Facebook. "April 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), May 5, 2020. https://about.fb.com/news/2020/05/april-cib-report/.

———. "August 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), September 1, 2020. https://about.fb.com/wp-content/uploads/2020/09/August-2020-CIB-Report.pdf.

———. "Facebook - Preventing Election Interference." About Facebook, 2020. https://about.fb.com/actions/preventing-election-interference/.

———. "February 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), March 2020. https://about.fb.com/wp-content/uploads/2020/03/February-2020-CIB-Report.pdf.

———. "March 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), April 2, 2020. https://about.fb.com/news/2020/04/march-cib-report/.

———. "October 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), October 27, 2020. https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-mexico-iran-myanmar/.

Page 1446 of 3957

———. "September 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), September 2020. https://about.fb.com/wp-content/uploads/2020/10/September-2020-CIB-Report.pdf.

———. "The State of Influence Operations 2017-2020." *About Facebook* (blog), May 26, 2021. https://about.fb.com/news/2021/05/influence-operations-threat-report/.

Federal Bureau of Investigation. "Combating Foreign Influence." What We Investigate. Accessed October 18, 2020. https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

———. "FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure." FBI Press Releases, January 16, 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-policy-for-notifying-state-and-local-election-officials-of-cyber-intrusions-affecting-election-infrastructure.

———. "FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure — FBI." FBI Press Releases, January 16, 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-policy-for-notifying-state-and-local-election-officials-of-cyber-intrusions-affecting-election-infrastructure.

———. "Protected Voices." Federal Bureau of Investigation. Accessed August 5, 2020. https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices.

Feiner, Lauren, and Megan Graham. "Twitter Unveils Final Details for Political Ad Ban, but It's Still Looking Murky." CNBC, November 15, 2019. https://www.cnbc.com/2019/11/15/twitter-unveils-new-political-ad-policy.html.

Frankovic, Kathy. "Republicans Still Not Convinced of Russian Election Meddling." YouGov, August 10, 2018. https://today.yougov.com/topics/politics/articles-reports/2018/08/10/republicans-still-not-convinced-russian-election-m.

Freelon, Deen, and Tetyana Lokot. "Russian Disinformation Campaigns on Twitter Target Political Communities across the Spectrum. Collaboration between Opposed Political Groups Might Be the Most Effective Way to Counter It." *Harvard Kennedy School Misinformation Review* 1, no. 1 (2020): 1–9. https://doi.org/10.37016/mr-2020-003.

Frey, William H. *Turnout in 2020 Election Spiked among Both Democratic and Republican Voting Groups, New Census Data Shows*. Washington, DC: Brookings, 2021. https://www.brookings.edu/research/turnout-in-2020-spiked-among-both-democratic-and-republican-voting-groups-new-census-data-shows/.

Page 1447 of 3957

Fridman, Ofer. "On the 'Gerasimov Doctrine': Why the West Fails to Beat Russia to the Punch." *PRISM* 8, no. 2 (2019): 100–113.

Galeotti, Mark. "The Mythical 'Gerasimov Doctrine' and the Language of Threat." *Critical Studies on Security* 7, no. 2 (2019): 157–61. https://doi.org/10.1080/21624887.2018.1441623.

Garrett, R. Sam. *Federal Role in U.S. Campaigns and Elections: An Overview*. CRS Report No. R45302. Washington, DC: Congressional Research Service, 2018. https://fas.org/sgp/crs/misc/R45302.pdf.

Gerasimov, Valery. "The Value of Science in Prediction." *Military-Industrial Kurier*, February 27, 2013. https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf.

Global Engagement Center. *Pillars of Russia's Disinformation and Propaganda Ecosystem*. Washington, DC: Department of State, 2020. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

Goodin, Dan. "NSA and FBI Warn That New Linux Malware Threatens National Security." *Ars Technica*, August 13, 2020. https://arstechnica.com/information-technology/2020/08/nsa-and-fbi-warn-that-new-linux-malware-threatens-national-security/.

Google Threat Analysis Group. "Google Safety & Security." *Google* (blog). Accessed May 27, 2020. https://blog.google/technology/safety-security/.

———. "TAG Bulletin: Q2 2020." *Google: Updates from Threat Analysis Group* (blog), August 5, 2020. https://blog.google/threat-analysis-group/tag-bulletin-q2-2020/.

———. "TAG Bulletin: Q4 2020." Google: Updates from Threat Analysis Group, November 17, 2020. https://blog.google/threat-analysis-group/tag-bulletin-q4-2020/.

Gould-Davies, Nigel. "Russia, the West and Sanctions." *Survival* 62, no. 1 (January 2, 2020): 7–28. https://doi.org/10.1080/00396338.2020.1715060.

Graphika Team. *Step Into My Parler; Suspected Russian Operation Targeted Far-Right American Users on Platforms Including Gab and Parler, Resembled Recent IRA-Linked Operation That Targeted Progressives*. New York: Graphika, 2020. https://graphika.com/reports/step-into-my-parler/.

Grimmer, Justin, Haritz Garro, and Andrew Eggers. "No Evidence For Voter Fraud: A Guide To Statistical Claims About The 2020 Election." Text. Palo Alto, CA: Hoover Institution, February 3, 2021. https://www.hoover.org/research/no-evidence-voter-fraud-guide-statistical-claims-about-2020-election.

Page 1448 of 3957

Grossman, Shelby, Daniel Bush, and Renée DiResta. "Evidence of Russia-Linked Influence Operations in Africa." *Stanford Internet Observatory* (blog), October 30, 2019. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf.

Hanlon, Bradley. *A Long Way to Go - Analyzing Facebook, Twitter, and Google's Efforts to Combat Foreign Interference*. Policy Brief No. 41. Washington, DC: German Marshall Fund of the United States, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/12/A-Long-Way-to-Go-Analyzing-Facebook-Twitter-and-Googles-Efforts-to-Combat-Foreign-Interference.pdf.

Hardwick, Joshua. "Top 100 Most Visited Websites by Search Traffic (as of 2020)." *Ahrefs* (blog), May 12, 2020. https://ahrefs.com/blog/most-visited-websites/.

Hartmann, Margaret. "How Conservatives View Russia's Alleged Meddling in the U.S. Election." *New York Magazine*, December 16, 2016. https://nymag.com/intelligencer/2016/12/how-the-right-is-talking-about-russias-election-meddling.html.

Helmus, Todd C., James V. Marrone, Marek N. Posard, and Danielle Schlang. *Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA704-3.html.

Higgins, Tucker. "Obama Response to 2016 Russian Election Meddling Had 'many Flaws,' Senate Report Finds." CNBC, February 6, 2020. https://www.cnbc.com/2020/02/06/obama-response-to-2016-russian-meddling-had-many-flaws-senate-report.html.

Hochschild, Jennifer. "If Democracies Need Informed Voters, How Can They Thrive While Expanding Enfranchisement?" *Election Law Journal: Rules, Politics, and Policy* 9, no. 2 (2010): 111–23.

Howard, Philip N., Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*. Oxford, UK: University of Oxford, Computational Propaganda Research Project, 2019. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs.

Ioffe, Julia. "Why Does the Kremlin Care So Much about the Magnitsky Act?" *The Atlantic*, July 27, 2017. https://www.theatlantic.com/international/archive/2017/07/magnitsky-act-kremlin/535044/.

Page 1449 of 3957

Isaac, Mike, and Kate Conger. "Google, Facebook and Others Broaden Group to Secure U.S. Election." *New York Times*, August 12, 2020. https://www.nytimes.com/2020/08/12/technology/google-facebook-coalition-us-election.html.

ISAO Standards Organization. "Financial Services ISAC." ISAO Standards Organization. Accessed April 21, 2021. https://www.isao.org/information-sharing-group/sector/financial-services-isac/.

Jaspar, Scott. "Why Foreign Election Interference Fizzled in 2020." *Atlantic Council* (blog), November 23, 2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/why-foreign-election-interference-fizzled-in-2020/.

Jojart, Krisztian. "Russia Military Thinking and the Hybrid War." *Scientific Periodical of the Hungarian Military National Security Service*, no. 1 (2019): 82.

Kang, Cecilia, Nicholas Fandos, and Mike Isaac. "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill." *New York Times*, October 31, 2017. https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html.

Kartapolov, A. V. "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods." *Journal of the Academy of Military Science* 51, no. 2 (2015): 26–36.

Kenney, Carolyn, Max Bergmann, and James Lamond. *Understanding and Combating Russian and Chinese Influence Operations*. Washington, DC: Center for American Progress, 2019. https://www.hsdl.org/?view&did=822729.

King, Angus, and Mike Gallagher. *Cybersecurity Lessons from the Pandemic*. CSC White Paper #1. Washington, DC: U.S. Cyberspace Solarium Commission, 2020. https://www.solarium.gov/public-communications/pandemic-white-paper.

Kollars, Nina A., and Michael B. Petersen. "Feed the Bears, Starve the Trolls: Demystifying Russia's Cybered Information Confrontation Strategy." *The Cyber Defense Review* Special edition (2019): 145–60.

Krebs, Christopher. "Statement from CISA Director Krebs Following Final Day of Voting." Cybersecurity and Infrastructure Security Agency, November 4, 2020. https://www.cisa.gov/news/2020/11/04/statement-cisa-director-krebs-following-final-day-voting.

Krogstad, Jens Manuel, and Mark Hugo Lopez. "Black Voter Turnout Fell in 2016, Even as a Record Number of Americans Cast Ballots." FactTank: News in the Numbers, May 12, 2017. https://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/.

Page 1450 of 3957

Laird, Chryl. "Why Black Voter Turnout Fell in 2016." Vox, January 15, 2020. https://www.vox.com/mischiefs-of-faction/2018/1/15/16891020/black-voter-turnout.

Laurence, Peter. "Powerful 'Putin's Chef' Cooks up Murky Deals." *BBC News*. November 4, 2019, Online edition, sec. Europe. https://www.bbc.com/news/world-europe-50264747.

Lee, Sangwon, and Michael Xenos. "Social Distraction? Social Media Use and Political Knowledge in Two U.S. Presidential Elections." *Computers in Human Behavior* 90 (January 2019): 18–25. https://doi.org/10.1016/j.chb.2018.08.006.

Leighton, Heather. "For Instagram's 10th Birthday, Experts Predict The Future Of Meme Culture." *Forbes*, October 7, 2020. https://www.forbes.com/sites/heatherleighton/2020/10/07/for-instagrams-10th-birthday-experts-predict-the-future-of-meme-culture/.

Linvill, Darren L., and Patrick L. Warren. "Engaging with Others: How the IRA Coordinated Information Operation Made Friends." *Harvard Kennedy School Misinformation Review* 1, no. 2 (April 2020): 1–14. https://doi.org/10.37016/mr-2020-011.

Lukito, Josephine. "Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017." *Political Communication* 37, no. 2 (2020): 238–55. https://doi.org/10.1080/10584609.2019.1661889.

Marcellino, William, Christian Johnson, Marek N. Posard, and Todd C. Helmus. *Foreign Interference in the 2020 Election: Tools for Detecting Online Election Interference*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA704-2.html.

Matishak, Martin. "Intelligence Community Creating Hub to Gird against Foreign Influence." *Politico*, April 26, 2021. https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604.

McFaul, Michael, ed. *Securing American Elections*. Palo Alto, CA: Stanford University, Cyber Policy Center, 2019. https://www.hsdl.org/?view&did=827251.

Miller, Gregory A., Edward Perez, E. John Sebes, and Sergio Valente. *Critical Democracy Infrastructure: Protecting American Elections in the Digital Age Threats, Vulnerabilities, and Countermeasures as a National Security Agenda*. 2nd ed. Palo Alto, CA: OSET Institute, 2020. https://trustthevote.org/wp-content/uploads/2020/05/01May20_CDI-2nd.pdf.

Misra, Jordan. "Voter Turnout Rates among All Voting Age and Major Racial and Ethnic Groups Were Higher Than in 2014." Behind the 2018 U.S. Midterm Election Turnout, April 23, 2019. https://www.census.gov/library/stories/2019/04/behind-2018-united-states-midterm-election-turnout.html.

Monje Jr., Carlos. "2018 U.S. Midterm Elections Review." *Twitter Company* (blog), January 31, 2019. https://blog.twitter.com/en_us/topics/company/2019/18_midterm_review.html.

Mueller, Robert. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: Department of Justice, 2019.

———. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: Department of Justice, 2019. https://www.hsdl.org/?view&did=824221.

Murthy, Dhiraj, Alison B. Powell, Ramine Tinati, Nick Anstead, Leslie Carr, Susan J. Halford, and Mark Weal. "Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital." *International Journal of Communication* 10 (2016): 4952–71.

Nakashima, Ellen. "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms." *Washington Post*, February 27, 2019. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

National Museum of American History. "The End of the Cold War." Cold War Timeline, 2000. https://americanhistory.si.edu/subs/history/timeline/end/.

National Security Agency, and Federal Bureau of Investigation. *Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*. Rev 1.0. Washington, DC: National Security Agency & Federal Bureau of Investigation, 2020. https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_drovorub_russian_gru_malware_aug_2020.PDF.

Nimmo, Ben, Camille François, C Shawn Eib, and Léa Ronzaud. "IRA Again: Unlucky Thirteen." New York, NY: Graphika, September 2020. https://public-assets.graphika.com/reports/graphika_report_ira_again_unlucky_thirteen.pdf.

Nimmo, Ben, Camille François, C. Shawn Eib, Lea Ronzaud, Rodrigo Ferreira, Chris Hernon, and Tim Kostelancik. *Secondary Infektion*. New York: Graphika, 2020. https://secondaryinfektion.org/report/secondary-infektion-at-a-glance/.

Nuñez, Michael. "The Surprising Truth about Twitter's Political Ad Ban." *Forbes*, November 1, 2019. https://www.forbes.com/sites/mnunez/2019/11/01/the-surprising-truth-about-twitters-political-ad-ban/.

Page 1452 of 3957

O'Connor, Sarah, Fergus Hanson, Emilia Currey, and Tracy Beattie. *Cyber-Enabled Foreign Interference in Elections and Referendums*. Policy Brief Report No. 41. Canberra, Australia: Australian Strategic Policy Institute, 2020. https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums.

Office of the Director of National Intelligence. *2021 Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, 2021. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2204-2021-annual-threat-assessment-of-the-u-s-intelligence-community.

———. *Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution*. Washington, DC: Office of the Director of National Intelligence, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

———. "Director of National Intelligence Announces Changes to Election Security Briefings." Office of the Director of National Intelligence, May 15, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2118-director-of-national-intelligence-announces-changes-to-election-security-briefings.

———. "DNI Coats Statement on the IC's Response to EO 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a U.S. Election." Office of the Director of National Intelligence, December 21, 2018. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2018/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election.

———. "Intelligence Community Assessment on Foreign Threats to the 2020 U.S. Federal Elections." Intelligence Community Assessment. Washington, DC, March 16, 2021. https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2192-intelligence-community-assessment-on-foreign-threats-to-the-2020-u-s-federal-elections.

———. "Members of the IC." Office of the Director of National Intelligence. Accessed April 27, 2021. https://www.dni.gov/index.php/what-we-do/members-of-the-ic. "Page 1 - Introduction," n.d.

Parks, Miles, and Philip Ewing. "Foreign Interference Persists And Techniques Are Evolving, Big Tech Tells Hill." National Public Radio, June 18, 2020. https://www.npr.org/2020/06/18/880349422/foreign-interference-persists-and-techniques-are-evolving-big-tech-tells-hill.

Polyakova, Alina. "The Kremlin's Plot against Democracy." *Foreign Affairs*, October 2020.

Page 1453 of 3957

Homeland Security Today. "Protecting Every Voice: FBI Expands Suite of Resources on Election Security," October 23, 2019. https://www.hstoday.us/subject-matter-areas/infrastructure-security/protecting-every-voice-fbi-expands-suite-of-resources-on-election-security/.

Rad, Armin A., Mohammad S. Jalali, and Hazhir Rahmandad. "How Exposure to Different Opinions Impacts the Life Cycle of Social Media." *Annals of Operations Research* 268, no. 1 (2018): 63–91. https://doi.org/10.1007/s10479-017-2554-8.

Raines, John R. *Countering Russian Disinformation: Europe Dusts Off the Mighty Wurlitzer*. E-Notes. Philadelphia, PA: Foreign Policy Research Institute, 2015. http://www.fpri.org/docs/haines_-_wurlitzer.pdf.

Reality Check Team. "US Election 2020: Fact-Checking Trump Team's Main Fraud Claims." BBC News, November 23, 2020. https://www.bbc.com/news/election-us-2020-55016029.

Rennack, Dianne E. *U.S. Sanctions on Russia: An Overview*. CRS Report No. IF10779. Washington, DC: Congressional Research Service, 2018. https://www.hsdl.org/?view&did=813693.

Robinson, Ryan. "7 Top Social Media Sites in 2020." Adobe Spark. Accessed July 21, 2021. https://www.adobe.com/express/learn/blog/top-social-media-sites.

Romm, Tony. "5 Things We Learned When Facebook, Google, and Twitter Testified to Congress About Russia's Election Meddling." Recode Daily, October 31, 2017. https://www.vox.com/2017/10/31/16588032/facebook-google-twitter-congress-russia-election-2016-tech-hearings-franken-cruz-graham.

Roozenbeek, Jon, and Sander van der Linden. "Breaking Harmony Square: A Game That 'Inoculates' against Political Misinformation." *Harvard Kennedy School Misinformation Review* 1, no. 8 (2020): 1–26. https://doi.org/10.37016/mr-2020-47.

Roth, Yoel, and Nick Pickles. "Updating Our Approach to Misleading Information." *Only on Twitter* (blog), May 11, 2020. https://blog.twitter.com/en_us /topics/product/2020/updating-our-approach-to-misleading-information.html.

Sattelberger, F. "Optimising Media Marketing Strategies in a Multi-Platform World: An Inter-Relational Approach to Pre-Release Social Media Communication and Online Searching." *Journal of Media Business Studies* 12, no. 1 (2015): 66–88. https://doi.org/10.1080/16522354.2015.1027117.

Savage, Patrick. *Russian Social Media Information Operations: How Russia Has Used Social Media to Influence U.S. Politics*. Washington, DC: American Security Project, 2017. https://www.hsdl.org/?view&did=808713.

Page 1454 of 3957

Shahani, Aarti. "Zuckerberg Denies Fake News on Facebook Had Impact On the Election." *All Things Considered*. Washington, DC: National Public Radio, 11/112016. https://www.npr.org/sections/alltechconsidered/2016/11/11/501743684/zuckerberg-denies-fake-news-on-facebook-had-impact-on-the-election.

Snider, Mike. "What's at Stake for Facebook's Mark Zuckerberg as He Testifies for Day 2." *USA Today*, April 10, 2018. https://www.usatoday.com/story/tech/news/2018/04/10/whats-stake-facebooks-mark-zuckerberg-he-testifies-before-congress/503017002/.

Spaulding, Suzanne E., and Eric Goldstein. *Countering Adversary Threats to Democratic Institutions: An Expert Report*. Washington, DC: Center for Strategic and International Studies, 2018. https://www.csis.org/analysis/countering-adversary-threats-democratic-institutions.

Stanford Internet Observatory. "Analysis of June 2020 Twitter Takedowns Linked to China, Russia, and Turkey." *Stanford Internet Observatory* (blog), June 11, 2020. https://cyber.fsi.stanford.edu/io/news/june-2020-twitter-takedown.

Starbird, Kate, Ahmer Arif, and Tom Wilson. "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations." *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 2019): 1–26. https://doi.org/10.1145/3359229.

Steinmetz, Katy. "Lawmakers Hint at Regulating Social Media During Hearing with Facebook and Twitter Execs." *Time*, September 5, 2018. https://time.com/5387560/senate-intelligence-hearing-facebook-twitter/.

Strohm, Chris. "Russian Hacking Began as 'Grizzly Steppe.'" *Chicago Tribune*, December 30, 2016, sec. Nation & World. https://www.chicagotribune.com/nation-world/ct-russian-hack-grizzly-steppe-20161230-story.html.

Stubbs, Jack. "Duped by Russia, Freelancers Ensnared in Disinformation Campaign by Promise of Easy Money." Reuters, September 3, 2020. https://www.reuters.com/article/us-usa-election-facebook-russia-idUSKBN25T35E.

———. "Exclusive: Russian Operation Masqueraded as Right-Wing News Site to Target U.S. Voters - Sources." Reuters, October 1, 2020. https://www.reuters.com/article/usa-election-russia-disinformation-idUSKBN26M5OP.

Thomas, Timothy. "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking." *Journal of Slavic Military Studies* 29, no. 4 (2016): 554–75. https://doi.org/10.1080/13518046.2016.1232541.

Page 1455 of 3957

———. "The Evolving Nature of Russia's Way of War." *Military Review* 97, no. 4 (August 2017): 34–42.

Thompson, Terry L. "No Silver Bullet: Fighting Russian Disinformation Requires Multiple Actions." *Georgetown Journal of International Affairs* 21 (2020): 182–94. https://doi.org/10.1353/gia.2020.0033.

Thornton, Rod. "The Russian Military's New 'Main Emphasis.'" *RUSI Journal* 162, no. 4 (2017): 18–28. https://doi.org/10.1080/03071847.2017.1381401.

THR Staff. "Donald Trump Caught on Hot Mic in 2005 Talking About Women: 'When You're a Star, They Let You Do It.'" News. Hollywood Reporter, October 7, 2016. https://www.hollywoodreporter.com/news/donald-trump-caught-hot-mic-936343.

Twitter. "Elections Integrity: We're Focused on Serving the Public Conversation." About Twitter, 2020. https://about.twitter.com/en_us/advocacy/elections-integrity.html.

———. "Retrospective Review Twitter, Inc. and the 2018 Midterm Elections in the United States." Twitter, February 4, 2019. https://blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf.

@TwitterSafety. "June 2020: Disclosing Networks of State-Linked Information Operations We've Removed." *Twitter Information Operations* (blog), June 12, 2020. https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.html.

———. "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive." *Twitter Information Operations* (blog), October 8, 2020. https://blog.twitter.com/en_us/topics/company/2020/disclosing-removed-networks-to-our-archive-of-state-linked-information.html.

———. "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive." Social Media. *Twitter Information Operations* (blog), September 1, 2020. https://twitter.com/TwitterSafety/status/1300848632120242181.

Uhlmann, Allon J., and Stephen McCombie. "The Russian Gambit and the U.S. Intelligence Community: Russia's Use of Kompromat and Implausible Deniability to Optimize Its 2016 Information Campaign against the U.S. Presidential Election." *Library Trends* 68, no. 4 (2020): 679–96. https://doi.org/10.1353/lib.2020.0017.

Page 1456 of 3957

U.S. Congress. House Permanent Select Committee on Intelligence. *Report of the House Permanent Select Committee on Intelligence on Russian Active Measures Together with Minority Views*. H.Rept 115-1110. Washington, DC: Government Publishing Office, 2019. https://www.congress.gov/115/crpt/hrpt1110/CRPT-115hrpt1110.pdf.

U.S. Congress. Senate Select Committee on Intelligence. *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts against Election Infrastructure with Additional Views*. Senate, 116th Cong., 1st Sess. Washington, DC: U.S. Congress. Senate, 2017. https://www.intelligence.senate.gov /sites/default/files/documents/Report_Volume1.pdf.

———. *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures, Campaigns, and Interference In the 2016 U.S. Election, Volume 2: Russia's Use Of Social Media With Additional Views*. Senate, 116th Cong., 1st Sess. Washington, DC: U.S. Congress. Senate, 2019. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume 2.pdf.

U.S. Congress. House of Representatives. "HPSCI Minority Open Hearing Exhibits." Permanent Select Committee on Intelligence. Accessed March 20, 2021. https://intelligence.house.gov/hpsci-11-1/hpsci-minority-open-hearing-exhibits.htm.

U.S. Congress. House of Representatives. *Facebook, Google, and Twitter: Examining the Content Filtering Practices of Social Media Giants, House of Representatives*, House of Representatives, 115th Cong., 1st sess., July 17, 2018. https://www.hsdl.org/?view&did=821944.

U.S. Congress. House Permanent Select Committee on Intelligence. *Report on Russian Active Measures*. Washington, DC: U.S. Congress. House, 2018. https://republicans-intelligence.house.gov/uploadedfiles/ final_russia_investigation_report.pdf.

U.S. Congress. Senate. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel I: Hearing before the Select Committee on Intelligence*, Senate, 115th Cong., 1st sess., March 20, 2017, 55.

———. *Mass Violence, Extremism, and Digital Responsibility: Hearing before the Committee on Commerce, Science, and Transportation*, Senate, 116th Cong., 1st sess., September 18, 2019. https://www.commerce.senate.gov/2019/9/mass-violence-extremism-and-digital-responsibility.

Page 1457 of 3957

———. *Examining Irregularities in the 2020 Election: Hearing before the Committee on Homeland Security and Governmental Affairs*, Senate, 116th Cong., 2nd Session, December 16, 2020. https://www.hsgac.senate.gov/imo/media/doc/Testimony-Krebs-2020-12-16.pdf.

U.S. Congress. Senate. Committee on Foreign Relations. *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*. S.Rpt. 115-21. Washington, DC: Government Publishing Office, 2018. https://www.hsdl.org/?view&did=806949.

U.S. vs. Internet Research Agency LLC, No. 18-cr-00032-DLF (U.S. District Court for the District of Columbia February 16, 2018).

Valenzuela, Sebastián. "Unpacking the Use of Social Media for Protest Behavior: The Roles of Information, Opinion Expression, and Activism." *American Behavioral Scientist* 57, no. 7 (July 2013): 920–42. https://doi.org/10.1177/0002764213479375.

Valenzuela, Sebastián, Ingrid Bachmann, and Marcela Aguilar. "Socialized for News Media Use: How Family Communication, Information-Processing Needs, and Gratifications Determine Adolescents' Exposure to News." *Communication Research* 46, no. 8 (2016): 1095–1118. https://doi.org/10.1177/0093650215623833.

Wagner, Kurt. "Facebook Meets With FBI to Discuss 2020 Election Security." Bloomberg, September 4, 2019. https://www.bloomberg.com/news/articles/2019-09-04/facebook-meets-with-fbi-to-discuss-2020-election-security.

Walker, Robert E. "Combating Strategic Weapons of Influence on Social Media." Master's thesis, Naval Postgraduate School, 2019. http://hdl.handle.net/10945/62826.

Wanless, Alicia, and Laura Walters. "How Journalists Become an Unwitting Cog in the Influence Machine." Carnegie Endowment for International Peace, October 13, 2020. https://carnegieendowment.org/2020/10/13/how-journalists-become-unwitting-cog-in-influence-machine-pub-82923.

Ward, Clarissa, Katie Polglase, Sebastian Shukla, Gianluca Mezzofiore, and Tim Lister. "Russian Election Meddling Is Back — Via Ghana and Nigeria — and in Your Feeds." CNN, April 11, 2020. https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html.

Washington, George. "Washington's Farewell Address." Digital History, 1796. http://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=3&psid=160.

Weed, Matthew. *Global Engagement Center: Background and Issues*. CRS Report No. IN10744. Washington, DC: Congressional Research Service, 2017. https://fas.org/sgp/crs/row/IN10744.pdf.

Weir, Kellie J. "Safeguarding Democracy: Increasing Election Integrity through Enhanced Voter Verification." Master's thesis, Naval Postgraduate School, 2018. https://www.hsdl.org/?view&did=811383.

Wiener, Jon. *How We Forgot the Cold War: A Historical Journey Across America*. Berkeley: University of California Press, 2012. https://books.google.com/books?hl=en&lr=&id=w_Sa-F8DXhgC&oi=fnd&pg=PA1&dq=american+memory+of+the+cold+war&ots=kvRphYu1TG&sig=sVpOOZBAdl0fqcHCskio5uy7tiE#v=onepage&q=american%20memory%20of%20the%20cold%20war&f=false.

Wilhelm, Thomas. "A Russian Military Framework for Understanding Influence in the Competition Period." *Military Review* 100, no. 4 (August 2020): 32–41.

Woolley, Samuel C., and Philip N. Howard. "Political Communication, Computational Propaganda, and Autonomous Agents." *National Science Foundation Public Access Repository*, September 3, 2016, 6.

Page 1459 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 1460 of 3957

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

Page 1461 of 3957

STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

INFORMATION OPERATIONS AND COUNTER-PROPAGANDA: MAKING A WEAPON OF PUBLIC AFFAIRS

BY

COLONEL W. C. GARRISON
United States Army

19990608 047

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1999

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

DTIC QUALITY INSPECTED 1

USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS AND COUNTER-PROPAGANDA: MAKING A WEAPON OF PUBLIC AFFAIRS

by

Colonel WC Garrison
United States Army

Colonel Morris E. Price Jr.
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Page 1464 of 3957

ABSTRACT

AUTHOR: WC Garrison, Colonel, U.S. Army

TITLE: Information Operations and Counter-Propaganda: Making a Weapon of Public Affairs

FORMAT: Strategy Research Project

DATE: 17 March 1999 PAGES: 36 CLASSIFICATION: Unclassified

The U.S. military operates in a global information environment and is subject to propaganda influence from both domestic and foreign media. Access to information and disinformantion can now influence attitudes and behavior from the battlefield to the far reaches of the world. Biased information can readily undermine the will of the American people and the American soldier to support military operations. This study examines the role of Public Affairs in information operations. It identifies the need for Public Affairs to change the objectives of its Public Information function. It concludes with recommendations for Military Public Affairs to engage in defined counter-propaganda activity.

Page 1465 of 3957

Page 1466 of 3957

TABLE OF CONTENTS

ABSTRACT iii

INFORMATION OPERATIONS AND COUNTER PROPAGANDA: MAKING A WEAPON OF PUBLIC AFFAIRS 1

KNOW PROPAGANDA 4

STRATEGIC VIEW 8

A CLEARLY DEFINED FUZZINESS 10

A CASE FOR COUNTER-PROPAGANDA 13

NOW KOSOVO 17

RECOMMENDATIONS 21

CONCLUSION 22

ENDNOTES 25

BIBLIOGRAPHY 29

Page 1467 of 3957

Page 1468 of 3957

INFORMATION OPERATIONS AND COUNTER PROPAGANDA: MAKING A WEAPON OF PUBLIC AFFAIRS

> *We are now at a crossroads of military public information. We must choose wisely which direction to go ... we must grow beyond conventional public information tactics... develop new roles ... and more importantly, we must explore strategic information concepts that are better suited to dealing with the challenges of reduced military budgets and manpower, widespread instability around the globe, new military missions and revolutionary advances in communication technology.* [1]
>
> —*Captain Mark Van Dyke*

New advances in technology have revolutionized information access and the way wars are fought. Broadcast media, television in particular, brings real-time images of war and suffering into American living rooms and even those in the jungle.[2] Like the Vietnam war, DESERT STORM had its daily news reports from the battlefield. Currently, images from Bosnia and Kosovo remind us of the power of broadcast media. However, unlike journalistic accounts of previous American war, reports from Southwest Asia were not limited to broadcasts from friendly territory.

The 1991 Gulf War to eject Iraqi forces from Kuwait ushered in a new era: real-time reporting from the battlefield. New technology, satellite relays in particular, allowed U.S. citizens to see Apache helicopter engagements in friendly zones as well as SCUD missile firings from the enemy's heartland. The battlefield of 2010 will feature imaging from space, and a ubiquitous media will monitor soldiers' activities throughout

the depth of the combat zone. In fact, current conflict in the Balkans portends that this new era is here to stay.

The ongoing information revolution calls for changes not only in warfighting but also in policy. Information technologies expand conflict beyond the traditional battlefield and enhance opportunities to conduct asymmetric war.[3] The enemy can now transmit propaganda via television screens.

We must assume that future adversaries will take full advantage of media broadcasts as propaganda tools. Propaganda in modern media will undoubtedly create greater challenges for military public affairs officers. As opportunities for manipulation of telecasts to sway public perceptions increase, military public affairs officers will have to struggle to carry out their support of the mission. In order to thwart hostile attempts to prejudice our broadcast media, Public Affairs must change its way of doing business. Indeed Public Affairs officers may now have to openly challenge broadcast news containing propaganda. To effectively neutralize broadcast news propaganda, Public Affairs must change its policy and the way it thinks about itself.

The coming years will not bring an uncomplicated, stable security environment such as that of the Cold War. The future security environment promises challenges from weapons of mass destruction to Hobbesian societies featuring resource depletion,

Page 1470 of 3957

rapid population growth, environmental damage, new infectious diseases, and uncontrolled refugee migration.[4]

We can expect countries that have ripened for conflict to have little print media circulation beyond the city limits. A war-torn country's citizens who become refugees can hardly afford the expense of or have access to newspapers. Although an evicted population can not be expected to escape with radios and televisions, electronic broadcasts are free. The proliferation of inexpensive pocket radios and televisions make it plausible that a few refugees will have the means to pull transmissions from the airways. Moreover, among the instruments of power—diplomatic, information, economic, military—information can best leverage television and radio for immediate affect on the views of citizens and leaders on both sides of a conflict.

This paper limits the term "media" to broadcast media, radio and television. The restricted definition is appropriate, since radio and television have the greatest potential to shape the future security environment.

Public Affairs involves three activities: Command Information, Community Relations, and Public Information (PI). Command Information is the commander's responsibility to disseminate accurate and timely information to soldiers, their families, and civilian employees and other internal audiences. Community Relations is the Public Affairs activity that helps

civic leaders and local communities understand the military. Public information aims to tell the military story to a wide external audience. Public Information officers work with and support the media.[5]

This study focuses on the Public Information aspect of Public Affairs. It specifically recognizes the Public Information activity as the Public Affairs linkage to the other elements of information operations—civil affairs, psychological operations (PSYOP), command and control warfare, and electronic warfare.[6]

In information operations, Public Affairs conducts information campaigns designed to establish credibility with the media to gain support for the military mission. But Public Affairs proclaim that its public information campaigns are devoid of a most effective tool: counter-propaganda activity.[7]

KNOW PROPAGANDA

Propaganda, in the minds of many, aims to appeal to prejudices by distorting facts with lies. Joint Pub 1-02 defines propaganda as "any form of communication in support of national objectives designed to influence the opinions, emotions attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly."[8] As defined, propaganda

is dissemination of ideas and information for the purpose of inducing or intensifying specific attitudes and actions. Although some propagandists may intentionally distort fact, others may objectively present information. No matter what its objective, propaganda attempts to persuade through rational or emotional appeal or through the organization of personal opinion.[9]

Propaganda can be blatantly obvious, such as that used in Nazi Germany. The Germans had a complex and well-organized system for the spread of propaganda and the control of their culture. During World War II (WWII), the Germans raised their propaganda system to a never obtained level of sophistication. Headed by Joseph Goebbels, the propaganda department influenced most all aspects of the German culture—literature, the press, films, theater, music, broadcasting, tourism, advertising, and the arts.[10] No where could Germany's people or soldiers escape the ever-present themes: Pure-blooded Aryans are the superior race and could not be defeated by the mixed-blooded Allies and their Jewish masters.[11]

On the other hand, it may employ subtle persuasive communication techniques. Propagandistic (i.e., persuasive) communications are not "good" or "evil" in and of themselves. They can be used for good, to reduce drunk driving and lung

Page 1473 of 3957

cancer, while they may also seek to win elections and sell malt liquor.[12]

This study defines counter-propaganda activity as actions to discredit an adversary's use of broadcast media to support their national objectives by influencing the opinions, emotions, attitudes, or behavior of U.S. and friendly audiences. As defined, counter-propaganda allows for truthful, honest opposition to the enemy's media borne propaganda.

Public affairs practitioners attempt to influence target audiences through many propaganda techniques, including "spin." Scott Rodgers cites euphemisms as a propaganda technique in military discourse. As examples, the MX-Missile was renamed the "Peacekeeper," and "collateral damage" often means civilian casualties.[13] Reacting viscerally, public information practitioners blindly avoid association with the term "propaganda." They fear that indulgence in any activity labeled propaganda will create perceptions that public information practitioners lie or deliberately deceive the public. This attempt to maintain their image has made Public Affairs officers overlook their own reliance on spin.

"Disinformation" is the spin euphemism of choice for propaganda. The public affairs community says disinformation is any government-sponsored communication in which deliberately misleading information is passed to targeted individuals,

Page 1474 of 3957

groups, or governments with the purpose of influencing foreign elite or public opinion. This also defines propaganda. Thus, a case can be made that the acknowledged public affairs mission to counter disinformation applies to propaganda.[14]

Alvin and Heidi Toffler categorize six military propaganda techniques: atrocity stories, i.e. emphasis on the brutal torture and killing of innocent men, women and children; hyperbolic inflation of the stakes involved in a war, i.e. left unchecked, the conflict will lead to Armageddon; dehumanization of the opponent, i.e. the enemy leader is a heartless demon; polarization, i.e. those who refuse to join us are not on the side of right; divine sanctions, i.e. God is with us; and, propaganda that discredits the adversary's propaganda.[15] The latter category should be openly recognized and clearly designated as a vital aim of the Public Information function of Public Affairs.

The shift to third-wave information warfare is underway, and the battle for control of information by perception management will intensify. The Gulf War offers classic examples of the use of propaganda and perception management. A young woman appears before television cameras and talks about babies being ripped out of incubators in Kuwait. Later reports linked the young woman to the Kuwaiti embassy, and she was apparently following a script. In the era of real-time broadcast, such

Page 1475 of 3957

televised propaganda is going to become far more important, and it will be managed with far more sophistication.[16]

Public Affairs' potential role, identifying and attacking enemy propaganda broadcast, can be a powerful tool to shape the course of events in time of conflict. A counter-propaganda effort can get needed information to displaced populations and combatants. Victims in a dysfunctional society can use reliable counter-propaganda information to locate relief sites. On the other hand, counter-propaganda may restrain belligerents with warnings that they will be subject to punishment for war crimes.

STRATEGIC VIEW

> *Maintaining a strong military and the willingness to use it in defense of national and common interests remain essential to a strategy of engagement as we approach the 21st century.*[17]

The advent of satellite-based global television broadcasting has created yet another arena for unconventional warfare. Live television coverage provides participants in armed conflicts with unprecedented opportunities to conduct military deception and shape the way distant audiences perceive events on the battlefield. Such "CNN Wars" are likely to become more common—and with disproportionately large political repercussions, especially in societies like the United Slates where policy-

Page 1476 of 3957

making is sometimes driven by transitory public reactions to media images.

Clausewitz asserted that the center of gravity is the hub of all power and movement: "What the theorist has to say is this: one must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed."[18]

National will exemplifies Clausewitz's definition of center of gravity. And, a nation's will, as stated by Clausewitz, is derived from the trinity formed by the government, the army and the people.[19] Thus modern adversaries will seek to exploit broadcast media to target the most susceptible element of national will, the people.

Despite media influence on the people, there is little evidence of U.S. efforts to counter propaganda-laced news broadcasts. The fact is the U.S. military operates in a global information environment, and Americans are subject to propaganda influences through domestic and foreign broadcast. Nearly unlimited access to information threatens to prejudice opinions on the battlefield and at home.

Given the wide array of possible opponents, weapons, and strategies, it becomes increasingly difficult to distinguish

between foreign and domestic propaganda in the news. Sometimes it is difficult to determine who is propagandizing whom. This new uncertainty greatly complicates the traditional public information role of telling the military story.

Furthermore, the possibility arises that the very "facts" of an event can be manipulated via multimedia techniques and widely disseminated by television and radio. Countering such manipulation will increase our ability to build and maintain support for military actions. In short, our Public Affairs practitioners should actively prepare to counter enemy propaganda.

A CLEARLY DEFINED FUZZINESS

Attacking the unabated flow of propaganda across the globe can further blur the functional lines between Public Affairs (PA) and Psychological Operations (PYSOPS). Both PA and PYSOPS are key elements of Information Operations. FM 100-6 defines Information Operations as continuous military operations within the Military Information Environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations.[20]

While acknowledging that the media can dramatically affect strategic direction and the range of military operations,

Page 1478 of 3957

military doctrine does not sanction actions intended to mislead or manipulate media coverage.[21] However, it is widely recognized that visual information displayed by domestic and international news organizations directly and rapidly influenced the nature of US policy objectives and the use of military force in Rwanda, Somalia, and in the former Yugoslavian republics. Images from future conflicts will convey undeniable propaganda designed to disrupt or defeat friendly military operations. Without change in Public Affairs concepts, biased broadcast will fall in the gap between psychological operations and public information activities.

The public affairs mission is to strengthen deterrence and war-fighting powers by timely, accurate and truthful communication to U.S. military, the American public and friendly foreign audiences.[22] Public Affairs is charged with communicating the military perspective to the American public, government, and internal military audiences. Implied in the public affairs charter is the requirement to support legitimate efforts that gain or maintain public support for military operations. Also implied is the responsibility to degrade the impact of negative stories, false reports, and inaccuracies.

As the primary agent for telling the military story, Public Affairs should be most concerned when news broadcasts distort military operations. Yet, military doctrine specifically denies

Page 1479 of 3957

Public Affairs a counter-propaganda role. The services do acknowledge concern about propaganda. Joint Pub 3-53 recognizes the requirement to counter propaganda and makes this a Psychological Operations responsibility. The Joint Pub also makes it policy for PSYOP to use PA channels to provide facts that will counter foreign propaganda, including misinformation directed at the United States.[23] Juxtaposing psychological operations policy with Public Affairs could lead to unintended consequences: one military community, PSYOPS, could dupe another, PA.

Psychological Operations should continue as directed in Joint Pub 3-53: "Operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objectives and reasoning, and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PYSOPS is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives."[24]

Public Information and Psychological Operations communicate information to civilian and military audiences to influence their perception of military operations. While PA communicates to U.S. and friendly audiences, PSYOPS targets enemy audiences. Both PA and PSYOPS contribute to achieving information dominance—the aim of Information Operations. Moreover, PA and

PSYOPS often communicate their messages through the same mediums. But, in the global information environment, neither PA nor PYSOPS can isolate their target audiences. Friend and foe will hear and view the same information. As important, news anchors willingly or unwittingly serve as agents for enemy propaganda.

Unlike Psychological Operations, Public Affairs policy not only ignores a counter-propaganda requirement but also asserts that it has no association with propaganda. This assertion aims to sustain Public Affairs' cloak of credibility. This protective public affairs garment, however, is woven with false threads. An honest look at military media operations reveals that Public Affairs is already engaged in counter-propaganda activities—censorship, message shaping, and spin.

A CASE FOR COUNTER-PROPAGANDA

Misinformation concerning Bosnia appeared in the media before the ethic cleansing started. Croatian propaganda described Serbian nationalists as Cetniks and presented the World War II (WWII) Cetnik leader as a genocidal monster. Serb propaganda described Croatian nationalists as Ustasa, and suggested that the Bosnian Muslims were either Nazis or fundamentalists, or both.[25]

Some analysts are convinced that it was propaganda-laced media that ignited the ethic flames that swept across Yugoslavia.[26] Media-espoused hate themes in the former Republic of Yugoslavia caused citizens to demonize neighbors, friends, and even family. Without benefit of truth-based counter-propaganda, the people of Yugoslavia have continued to villianize each other despite their recent history of peaceful coexistence.

Television has played a major role in the events leading to the war and disintegration of Yugoslavia. The political leaders in the republics blatantly used the media for their propagandist purposes and shaped public opinion in the direction that best suited their interests. During the Yugoslav era, media were used to support the existing political system and were controlled by the League of Communists in each republic.[27]

The new power holders, particularly in Serbia and in Croatia, simply stepped in for the old regime and increased their influence over the media. The few independent media organizations were sidelined and were not able to reach such massive audiences as the state-controlled television and radio did. The media was the tool that generated nationalist euphoria, ethnic hatred, and war psychosis. Media organizations included journalists who were devoted to the most extreme propagandist presentations. Such was the power of the media

Page 1482 of 3957

that many experts of the Yugoslav crisis are convinced that the war could not have erupted without media influence.[28].

In Bosnia-Herzegovina, the media were widely controlled by the ruling parties. The political elite used the media to govern the population and support nationalistic propaganda. However, few alternative media emerged in the Republika Srpska at the end of 1995. In the government-controlled territories, and particularly in Sarajevo, the media had more space to maneuver—but often only with the help of international donations, which in turn created an artificial media market.[29]

Broadcast news played a crucial role in events within the former Yugoslavia, but it helped to shape the policies of the international community. The war—first in Slovenia, then in Croatia, and finally in Bosnia—was played out in real time on television screens throughout the world. The images of tanks, refugees, concentration camps, and crimes against humanity shook the world and challenged the international community to do something.[30]

In 1997, the nationalist, state-run broadcast media in Bosnia painted NATO peacekeepers as an "occupying force." NATO commanders responded with threats to jam transmitters and then closed four transmission stations of Bosnian Serb radio and television because of what a United Nations spokesman called ongoing "distortion of the truth."

After the takeover of the towers, rival Bosnian Serb fractions in Pale and Banja Luka agreed to alternate daily broadcasts until parliamentary elections. The television network served as an effective counterweight to Serbian propaganda broadcasts. Studio interviews with opposing candidates and various international election observers presented listeners in and outside of the cities with a clear picture of the campaign. Although this balanced coverage helped bring some moderates to power, the counter-propaganda effort was too little too late.

With few independent electronic news sources and a public conditioned to obey authority, people readily accept what they are told. Obviously, leaders like Slobadam Milosevic know very well how to leverage broadcast media for propaganda purposes. He used Serb-controlled radio and television stations during his drive for a "Greater Serbia" to re-ignite Serb nationalism throughout the former Yugoslavia. Moreover, his unchecked messages of hate fed an international media that was hungry for news.

Some say it was "words, not bullets" that sparked the bloodshed in Bosnia-Herzegovina. According to Michael Ignatieff, "long before a shot was fired in Yugoslavia, the media of both Croatia and Serbia were readying their populations to think of the other side as vermin, insects, dogs, and other

Page 1484 of 3957

noisome creatures."[31] Several analysts have gone so far as to suggest some government journalists ought to be tried as war criminals.[32] Through uncontested broadcast propaganda, Milosevic successfully isolated the public. His news railed against the West and Serbia's neighbors, blaming them for the country's woes. Serbians became more xenophobic and convinced that former friends where their enemies. Counter-propaganda through independent media could have brought another perspective and offered hope by informing and educating the warring factions about how a democratic society works.

NOW KOSOVO

As of this writing, conflict rages in Kosovo. With over a million refugees fleeing their homes for sanctuary in nearby Albania and Macedonia, the U.S. military and North Atlantic Treaty Organization (NATO) forces are supporting a massive humanitarian relief effort. Yet little is being done in the way of counter propaganda to dispel lies and keep Kosovo's displaced citizens informed.

Some refugees have transistor radios and are able to tune in to the British Broadcasting Corporation (BBC) World Service, Radio Tirana, and other stations to find out what is happening. But even then, the information they receive is not specifically geared to their needs. Reliable information is clearly not

coming from the government-controlled media of President Slobodam Milosovic.

As NATO bombs rain on Belgrade, Serb state-run radio and television broadcasts call President Clinton "Adolf Clinton." NATO soldiers are referred to as "assassins." U.S. Secretary of State Madeleine Albright is "bloodthirsty."[33] The Serb leader's use of propaganda parallels that of Germay's WWII leader. Milosevic apparently desires to strengthen resolve of both his people and his military. Christopher Bennet says that "the key to Milosevic's rule and an understanding of modern Serb nationalism is the Serbian media and their sustained campaign to generate national hysteria. Indeed, the Serbian media have played a very similar role in Milosevic's Serbia to that played by the Nazi media in Hitler's Germany, though on account of technological advances in the intervening half century, their influence has been more pervasive and more insidious."[34]

As the Serbian propaganda machine has greater access to its population than NATO, we can expect it to also have a greater influence. The Serbian people have grown up with a strong bias in their media, and propaganda messages have had a lifetime to take hold. By implanting his views without challenge, Milosevic easily influences the Serbian people to do what he wants or lay blame on others. In the case of the Serbian military, it

appears soldiers are willing to fight and die based on Milosevic's propaganda.

Radio-Television Serbia voices its propaganda over images of bombed out buildings and anti-NATO rallies. This propaganda, which is closely controlled by Milosevic's regime, has already played a major role in the survival of the Yugoslav President. It will likely become even more crucial as the war drags on and life becomes more difficult. We can not afford to ignore Milosevic's rhetoric as it fuels nationalist frenzy. Serbs are now burning U.S. flags, destroying anything that is a symbol of a NATO country, and claiming they are already to fight to the death.

Some Serbian people may question the state radio and television broadcasts. But, they have few alternative messages that can cause serious doubt. Serbian media present a picture that Yugoslavia is winning the war and America and its NATO allies have gone mad. In the face of this distortion of the truth, President Clinton made an attempt at counter-propaganda. He sent a message to the Serbian people via satellite transmission. Clinton said the bombing was directed not at the Serbian people but at their leader. The US President's message contended with propaganda filters in Serbia. Most likely, few Serbians head the message, and even fewer believed the message.

Page 1487 of 3957

The fact is that there is almost no credible information countering Belgrade's view of its security operations. The only direct Western effort to respond to this monopoly is NATO's demand that Serb-controlled radio and television broadcast six hours of uncensored Western broadcasts a day. The majority of the Serbs and Kosovars rely on government station as their main news source, and, Milosevic can be counted on to deliver a daily dose of propaganda.

After Afghanistan, Somalia, and Rwanda, we should have learned to make propaganda one of the first casualties in a conflict. Balanced reporting is effective counter-propaganda ammunition. News broadcasts by the BBC, Voice of America, or Radio Free Europe could easily carry counter-propaganda messages aimed at shaping attitudes about the conflict in Kosovo. Counter-propaganda programming tailored to the local theater could help dispel rumors by challenging Serbian broadcasts. It could also help the Serbian military and people better understand NATO's intervention. Despite past experiences, however, we have not only been slow to demonize Milosevic but also slow to recognize the need for a PA counter-propaganda program as part of our overall military strategy.

Public affairs practitioners should give credence to how useful counter propaganda can be for shaping the security environment and alleviating crises. Better information access

Page 1488 of 3957

can help reduce conflict, particularly if aimed at the belligerents themselves. Some human rights sources believe Serb security forces might be less enthusiastic in their repression if warned by counter-propaganda broadcasts that they may be held accountable for their actions.

RECOMMENDATIONS

> *In a society under assault across its entire infosphere, it will become increasingly difficult for members of that society to verify internally the truth or accuracy of anything.... The End State may not be bloodless surrender but total disruption of the targeted society.*[35]
>
> *-George Stein*

We should openly acknowledgment that Public Affairs is already engaged in the fight against propaganda. This can spur debate on a Public Affairs strategy with ends, ways and means that are aligned for information operations in 2010.

The Public Information function of Public Affairs should include counter-propaganda operations as an objective. The aim should be to degrade the enemy's propaganda impact on the conflict and to maintain domestic and international support for U.S. military operations. Public Affairs must further legitimize its Public Information link to PYSOPS to facilitate a unified counter-propaganda effort. Public Information activities must use truth-based, counter-propaganda messages.

Page 1489 of 3957

PSYOP should conduct only offensive propaganda operations—at the theater and below in wartime. PSYOPS should assist Public Affairs with counter-propaganda activities at the strategic level.

Our military has the means to support this new Public Affairs role. So the Public Affairs infrastructure need not change. Additional instructors specializing in counter-propaganda at the Defense Information School (DINFOS) may be necessary.

Public Affairs organizations need not set up radio stations to conduct counter-propaganda. A number of independent media channels can be used for disseminating counter-propaganda messages. In the case of Kosovo, the BBC and Radio Tirana, independent media, are already transmitting Albanian-language broadcasts which reach much of the Balkans.

CONCLUSION

> The howitzers of the mass media ... will not long remain the property of the West: The world's skies will fill with private satellites, and channels of communications will continue to multiply....[36]

Whatever the means employed, it is questionable whether American public opinion can be induced to support military operations that do not support U.S. interests, especially when

adversaries use unchecked propaganda in the media to weaken American will.

The anticipated wars of the future will require Public Affairs to actively launch counter-propaganda operations. Such initiative will be critical to gaining and maintaining public support in the global information environment of the future. The Information Age is merging both internal and external audiences. Therefore, we should accept that counter-propaganda messages borne in the modern media atmosphere would impact both the enemy and friendly public. More important, lessons form Vietnam, DESERT STORM, and Bosnia teach future adversaries a common strategy: use propaganda in the media to attack the American will. This strategy of demoralization will remain viable for the foreseeable future.

The further the world advances toward embracing information technology, the less likely military Public Affairs can rely on traditional management of the media through censorship. A change in policy can bring the needed focus to public information objectives and support a specific counter-propaganda role. This does not mean that Public Affairs should mortgage its credibility that has been built on honesty for action supported by lies. To be effective tellers and protectors of the military story, Public Affairs must hammer out doctrinal change on an anvil of truth. By so doing, public information

operations can effectively counter propaganda in broadcast media and contribute to maintaining the national will for victory today and tomorrow.

WORD COUNT:4530

Page 1492 of 3957

ENDNOTES

[1] Captain Mark A. Van Dyke, U.S. Navy, "Strategic Information Operations: IFOR Case Studies," World Wide Public Information Conference, The Pentagon, Washington, D.C., 20 February 1997.

[2] Michael Ignatieff, The Warrior's Honor: Ethic War and the Modem Conscience (New York: Metropolis Books, 1997), 83.

[3] Larry Wentz, ed, Lessons from Bosnia: The IFOR Experience (Washington, D.C.: National Defense Univeristy, January 1998), xi-xiii.

[4] The White House, A National Security Strategy for a New Century (Washington, D.C.: The White House, October 1998, 1.

[5] Department of the Army, Public Affairs Operations, Field Manual 46-1 (Washington D.C.: U.S. Department of the Army, 23 July 1992), 1-1 to 1-3.

[6] Department of the Army, Information operations, Field Manual 100-6 (Washington, D.C.: U.S. Department of the Army, 27 August 1996), 2-4.

[7] Department of Defense, Doctrine for Public Affairs in Joint Operations, Joint Publication 3-61 (Washington D.C.: U.S. Department of Defense, 14 May 1997), II-2.

[8] Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02 (Washington, D.C.: U.S. Department of Defense, 10 June 1998), 359.

[9] Microsoft Bookshelf 98, Reference Library, (Redmond, WA: Microsoft Corporation, 1997).

[10] Terence H. Qualter, Propaganda and Psyschological Warfare (New York: Random House, 1962),145-146.

[11] Omar Bartov, Hitler's Army (New York: Oxford University Press, 1991), 135, 155.

[12] R. Scott Rodgers, "Propaganda in the Information Age," Soldier-Scholar, Fall 1996, 20.

[13] Ibid., 22.

Page 1493 of 3957

[14] Department of the Army, Field Manual 46-1, 11.

[15] Alvin Toffler and Heidi Toffler, War and Anti-War, Survival at the Dawn of the 21st Century (Boston: Little, Brown & Co., 1993), 67-69.

[16] Peter Millson and Kate O'Sullivan, eds. The Predator (London: Broadcasting Support Services for the BBC Horizon, 1994).

[17] Department of Defense, Report of the Quadrennial Defense Review (Washington, D.C.: U.S. Department of Defense, May 1997), 8.

[18] Anthony M. Coroalles, "On War in the Information Age: A Conversation with Carl von Clausewitz," Army, May 1996, 32.

[19] Carl von Clausewitz, On War, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1989), 89.

[20] Department of the Army, Information Operations, Field Manual 100-6 (Washington D.C.: U.S. Department of the Army, 27 August 1996), 2-4.

[21] Ibid., 1-13.

[22] Department of the Army, Field Manual 46-1, 1-1.

[23] Department of Defense, Doctrine for Joint Psychological Operations, Joint Publication 3-53 (Washington, DC: U.S. Department of Defense, 30 July 1993), 1-5.

[24] Ibid.

[25] Noel Malcolm, Bosnia A Short History (New York: University Press, 1994), xxiii.

[26] Pascale Combelles Siegel, Target Bosnia: Integrating Information Activities in Peace Operations (Washington, D.C.: National Defense University, January 1999), 6.

[27] Mark Thompson, Forging War, The Media in Serbia, Croatia and Bosnia-Herzegovina (Bath Press, 1994),7.

[28] Ibid., 5.

Page 1494 of 3957

[29] International Crisis Group Report: "Media in Bosnia and Herzegovina: How International Support Can Be More Effective." International Crisis Group, 7 March 1997, 4-6 and 9-10.

[30] Martin Bell, In Harms Way—Reflections of a War Zone Thug, London: Hamish Hamilton Ltd., 1995), 142-145.

[31] Michael Ignatieff, 55-56.

[32] Michael J. Jordan, "Cracks in the Serb Media Monopoly," The Christian Science Monitor, 2 October 1997, 5.

[33] Justin Brown, "Why Serb Chief Whips Up Anti-US Fervor," Christian Science Monitor, 1 April 1999, 1.

[34] Christopher Bennet, Yugoslavia's Bloody Collapse—Causes, Course, Consequences (London: Hurst and Company, 1995), 248.

[35] George J. Stein, "Information-Cyberwar-Netwar," Battlefield of the Future," 21st Century Warfare Issues, (Maxwell AFB, AL: Air University Press, 1995), 158.

[36] Alvin Toffler and Heidi Toffler, "Preparing for Conflict in the Information Age," Futurist, June/July 1998, 26-29.

Page 1495 of 3957

Page 1496 of 3957

BIBLIOGRAPHY

Bartov, Bartov. Hitler's Army. New York, Oxford University Press, 1992.

Bell, Martin. In Harm's Way. New York: Penguin Books, 1996.

Bennet, Christopher. Yugoslavia's Bloody Collapse—Causes, Course, Consequences. London: Hurst and Company, 1995.

Brown, Justin. "Why Serb Chief Whips Up Anti-US Fervor." Christian Science Monitor, 1 April 1999, p. 1.

Clausewitz, Carl von. On War. Princeton, N.J.: Princeton University Press, 1989.

Coroalles, Anthony M. "On War in the Information Age: A Conversation with Carl von Clausewitz." Army, May 1996, 32.

Ignatieff, Michael. The Warrior's Honor: Ethic War and the Modem Conscience. New York: Metropolis Books, 1997.

International Crisis Group Report: "Media in Bosnia and Herzegovina: How International Support Can Be More Effective." International Crisis Group, 7 March 1997.

Jordan, Michael J. "Cracks in the Serb Media Monopoly." Christian Science Monitor, 2 October 1997, p.5.

Malcolm, Noel. Bosnia A Short History. New York: University Press, 1994.

Microsoft Bookshelf 98, Reference Library. Redmond, WA: Microsoft Corporation, 1997.

Rogers, R. Scott. "Propaganda in the Information Age." Soldier-Scholar, Fall 1996, 20.

Siegel, Pascale Combelles. Target Bosnia: Integrating Information Activities in Peace Operations. Washington, D.C.: National Defense University, January 1999.

Stein, George J. "Information-Cyberwar-Netwar, Battlefield of the Future." 21st Century Warfare Issues Maxwell AFB, AL: Air University Press, 1995.

Page 1497 of 3957

Thompson, Mark. Forging War, The Media in Serbia, Croatia and Bosnia-Herzegovina. Bath Press, 1994.

Toffler, Alvin, and Heidi Toffler. "Preparing for Conflict in the Information Age." Futurist, June/July 1998, 26-29.

Toffler, Alvin, and Heidi Toffler. War and Anti-War, Survival at the Dawn of the 21st Century. Boston: Little, Brown & Co., 1993.

U.S. Department of the Army. Information Operations. Field Manual 100-6. Washington, D.C.: U.S. Department of the Army, 27 August 1996.

U.S. Department of the Army. Public Affairs Operations. Field Manual 46-1. Washington, D.C.: U.S. Department of the Army, 23 July 1992.

U.S. Department of Defense. Department of Defense Dictionary of Military and Associated Terms. Publication 1-02. Washington, D.C.: U.S. Department of Defense, March 1994.

U.S. Department of Defense. Doctrine for Joint Psychological Operations. Joint Publication 3-53. Washington DC: U.S. Department of Defense, 30 July 1993.

U.S. Department of Defense, Doctrine for Public Affairs in Joint Operations. Joint Publication 3-61. Washington, D.C.: U.S. Department of Defense, 14 May 1997.

U.S. Department of Defense. Report of the Quadrennial Defense Review. Washington, D.C.: U.S. Department of Defense, May 1997.

Wentz, Larry, ed. Lessons from Bosnia: The IFOR Experience. Washington, D.C.: National Defense University, January 1998.

White House. A National Security Strategy for a New Century. Washington, D.C.: The White House, October 1998.

Wualter, Terence H. Propaganda and Psychological Warfare. New York: Random House, 1962.

Page 1498 of 3957

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
FORT GEORGE G. MEADE, MARYLAND 20755-5995

REPLY TO
ATTENTION OF:

FEB 27 2007

Freedom of Information/
Privacy Office

Mr. John Young
CRYPTOME
251 West 89th Street
Suite 6E
New York, New York 10024

Dear Mr. Young:

References:

a. Your Freedom of Information Act request of March 29, 2001, for information pertaining to the Internal Counterintelligence Program (ICIP), ZF011946W (#123F-06).

b. Our letter of December 20, 2005, informing you we needed additional time to review the records, and informing you we were unable to comply with the statutory 20-day time limit in processing your request.

c. Our letters of March 22, 2006 and January 30, 2007, informing you we were still reviewing the records you have requested and will respond to you once the review has been completed.

We have conducted checks of the automated Defense Central Index of Investigations and a search of the Investigative Records Repository to determine the existence of Army intelligence investigative records responsive to your request. We have located records pertaining to your request on ICIP, ZF011946W.

We have completed a mandatory declassification review in accordance with Executive Order (EO) 12958, as amended. As a result of our review, information has been sanitized and nine pages of records are denied in their entirety as the information is currently and properly classified SECRET and CONFIDENTIAL according to Sections 1.2(a)(2), 1.2(a)(3) and 1.4(c) of EO 12958, as amended. This information is exempt from the public disclosure provisions of the FOIA pursuant to Title 5 U.S. Code 552(b)(1). On March 9, 1999, the President exempted the file series in which these records are maintained from the automatic declassification provisions of EO 12958, Section 3.4, as amended, pertaining to classified records more than 25 years old. It is not possible to reasonably segregate meaningful portions of the withheld pages for release. The records are enclosed for your use. A brief explanation of the applicable sections follows:

Section 1.2(a)(2) of EO 12958, as amended, provides that information shall be classified SECRET if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

Section 1.2(a)(3) of EO 12958, as amended, provides that information shall be classified CONFIDENTIAL if its unauthorized disclosure reasonably could be expected to cause damage to the national security.

Section 1.4(c) of EO 12958, as amended, provides that information pertaining to intelligence activities, intelligence sources or methods, and cryptologic information shall be considered for classification protection.

Since the release of the information would result in an unwarranted invasion of the privacy rights of the individuals concerned, this information is exempt from the public disclosure provisions of the FOIA per Title 5 U.S. Code 552 (b)(6).

In addition, we have sanitized information that would reveal the identity of confidential sources. This information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(7)(D) of the FOIA. The significant and legitimate governmental purpose to be served by withholding is that a viable and effective intelligence investigative capability is dependent upon protection of confidential sources.

The withholding of the information described above is a partial denial of your request. This denial is made on behalf of Major General John Defreitas, III, the Commanding General, U.S. Army Intelligence and Security Command, who is the Initial Denial Authority for Army intelligence investigative and security records under the FOIA. You have the right to appeal this decision to the Secretary of the Army. If you wish to file an appeal, you should forward it to this office. Your appeal must be postmarked no later than 60 calendar days from the date of this letter. After the 60-day period, the case may be considered closed; however, such closure does not preclude you from filing litigation in the courts.

We have been informed by the FBI that their information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(1) of the FOIA.

The withholding of the information by the FBI constitutes a partial denial of your request and you have the right to appeal this decision. If you decide to file an appeal, it should be sent to the Co-Director, Office of Information and Privacy, U.S. Department of Justice, 1425 New York Avenue, Northwest, Suite 11050, Washington, DC 20530-0001 within 60 days from the receipt of this letter. The envelope and the letter should be clearly marked "Freedom of Information Appeal" or Information Appeal." Please cite FBI FOI/PA #429014 assigned to your request so that it may be easily identified.

We are forwarding a copy of this letter to the FBI (FOI/PA #429014).

During the processing of your request, information was disclosed which is under the purview of another government agency. This office has no authority to release this record and it is being referred, along with your request, for appropriate action under the FOIA, and direct reply to you.

Additionally, we are coordinating with other government agencies concerning the releasability of their information contained in the records. We will inform you as to the releasability of the information upon completion of our coordination.

If you have any questions concerning this action, please feel free to contact this office at (301) 677-6410. Please refer to case #123F-06.

Sincerely,

Susan J. Butterfield
Director
Freedom of Information/Privacy Office
Investigative Records Repository

Enclosure

THIS MUST REMAIN T O P D O C U M E N T

DOSSIER NO. ZF0119 W
Vol 1 of 7 Vols

As of 18 Sep 85 (Date) all material included in this file conforms with DA policies currently in effect.

Delmar Smith (Signature) 18 Sep 85 (Date Signed)

Delmar Smith (Printed Name) GS5 (Grade)

Reviewed for Retention
Criteria UP AR 381-10
Reviewer L. Grant Date 4 Jan 93

THIS MUST REMAIN T O P D O C U M E N T

IA (HQ) Form 2214
(1 Sep 78)

Replaces MIIA Fm 315, 1 Jun 75, which may be used until supplies are exhausted.

TRANSMITTAL OF MATERIAL TO IRR*

*NOTE: This form is not required when material is forwarded to IRR with DA Form 2784-R, but may be used as a supplement to DA Form 2784-R to provide additional instructions.

1. TO:
( ) Records Processing Division
(XX) Special Records Division

2. FROM:
Director
USA FCA, USAINSCOM
AIA05

3. DATE 27 Aug 85

4. PERSONAL/IMPERSONAL SUBJECT (Establish dossier or add material to existing dossier)

a. SUBJECT: Internal Counterintelligence Program (ICIP)

b. DOB:

c. POB:

d. SSN:

e. Alias/Nee

5. PERSONAL/IMPERSONAL INDEX CROSS-REFERENCES (Continue on plain bond paper if needed)

Name/Impersonal Title	DOB	POB	SSN	Alias/Nee
USASA FIELD STATION, BERLIN				
DLI, PRESIDIO OF MONTERREY, CA				
DET N, USASA FIELD STATION AUGSBURG, GE				
USA MISSILE COMMAND, REDSTONE ARSENAL, AL				
ABERDEEN PROVING GROUND, ABERDEEN, MD.				
WHITE SANDS MISSILE RANGE, NM				

6. FORWARD DOSSIER TO:

(X) Files

( ) Account Number: _____

7. REGULATORY REVIEW (Check one or both)

(XX) Attached material meets retention criteria of AR 381-10

( ) Material contains financial data under criteria of AR 190-6

8. DISPOSITION OF CASE (If not reflected on DA Form 2784-R)

CASE CLOSED

9. REQUEST FOR CONTROL (For controlled dossier material only; enter data required by para 3-4, AR 381-45)

Category I
Paragraph 3-2b(3), AR 381-45
Cannot be pre-determined
See Block 4

10. IRR USE ONLY

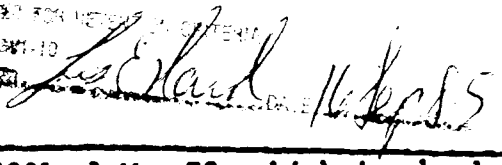
( ) AR 190-6

( ) AR 381-10

( ) AR 381-45

Dossier No: _____

Aging Criteria: _____



IA(HQ) Form 2201-R, 1 Nov 84 (Replaces IA(HQ) Form 2201, 1 May 78, which is obsolete)

I * C * I * P Quarterly Reports

1972

3

3 Qtr 72

~~SECRET~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Quarterly ACIP Report

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 18 October 1972

ACTION REQUIRED: To provide USofA with the third quarterly ACIP report.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By Memorandum dated 8 February 72, the Under Secretary of the Army requested the Vice Chief of Staff, US Army to provide quarterly reports on all ACIP's (BLUE TAB B).

b. The second quarterly report, which contained a specially requested additional analysis, was submitted to the Under Secretary of the Army on 1 August 72 (BLUE TAB C).*

c. Written input from USAINTC for the current quarterly report is attached at BLUE TAB D.

2. DISCUSSION: Memorandum at BLUE TAB A to Under Secretary of the Army through the Vice Chief of Staff, US Army, provides required third quarterly report as desired by USofA memorandum of 8 February 1972.

3. RECOMMENDATION: That Memorandum (BLUE TAB A) be approved and signed.

* SECOND QUARTERLY REPORT PROMISED A COMPLETE ANALYSIS OF ACIPS IN FOURTH QUARTERLY REPORT. THIS IS THIRD QUARTER'S REPORT.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR	WRW	18 Oct 72
			DIV		
			DIR	MK	19 Oct 72
			EX		
			ACSI	WRW	20 Oct 72
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

W. WEBB, MAJ/57471 WRWebb

SPECIAL ACTIONS BR
RECORDS COPY

ACSI FORM 28, 13 Sep 71

~~SECRET~~

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

CURRENT ACIP OPERATIONS

LOCATION	ACIP NICKNAME	DATE APPROVED	NUMBER OF SOURCES
Edgewood Arsenal, Maryland	CANAL LOOP	16 February 72	5
Fort Ritchie, Maryland	CANARY EFFORT	16 February 72	3
Fort Bliss, Texas (Language School)	CANCER PORCH	28 December 71	1
Fort Ord, California	CANDID FROLIC	21 December 71	2
Fort Monmouth, New Jersey	CENTRAL TAXI	16 February 72	3
Aberdeen Proving Grounds, Maryland	GONDOLA STAR	16 February 72	2
Picatinny Arsenal, New Jersey	GONG SILK	16 February 72	3
Philadelphia, Pennsylvania (Electronics Command)	LANDLESS TIME	19 January 72	4
Washington, D.C. (Language School)	LANYARD MOOD	22 December 71	0
Carlisle Barracks, Pennsylvania (Army War College)	LENIENT CLOUD	16 February 72	4
Presidio of Monterey, California	LENTIL MONKEY	26 October 71	3
TOTALS 11	11		30

Off-post Information

There were no instances in which information on non-affiliated civilians was collected off-post.

Classified by DAMI-DO
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS
DECLASSIFIED ON 31 DECEMBER 1978

~~CONFIDENTIAL~~

CONFIDENTIAL

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE COMMAND
FORT HOLABIRD, MARYLAND 21219

16 OCT 1972

ICDISO-OC

SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

HQDA (DAMI-DOI-S)
WASH DC 20310

1. (U) References:

a. Ltr, DAMI-DOI-S, 8 Mar 72, subject as above.

b. Ltr, ICDISO-OC, 18 Apr 72, subject as above.

2. (U) In compliance with reference a, above, the ACIP quarterly report for the period 1 July - 30 September 1972 is forwarded herewith.

3. (U)(e) The following operational and administrative control measures remain in effect concerning all reported ACIP to assure compliance with DOD and DA policies relative to the acquisition of information on non-DOD affiliated personnel:

a. Each ACIP is restricted to on-post target coverage of DOD affiliated personnel and utilizes employees or military personnel of the serviced command as sources. These constraints generally preclude the possibility of violations of current collection restrictions regarding non-DOD affiliated personnel.

b. Sources are selected from a civilian/military work force only after detailed assessment. Generally, only long term employees or personnel of known reliability and proven loyalty are selected for recruitment.

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS. DECLASSIFIED ON 31 DEC 1978

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DoD 5200.1R

7

CONFIDENTIAL

CONFIDENTIAL

ICDISO-OC
SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

c. Each individual and/or source involved in the conduct or control of each ACIP is briefed on current policies and restrictions pertaining to the program and program associated activities as concerns persons and organizations not affiliated with DOD.

d. ACIP reporting is scrutinized at each level of command to insure the acceptability of information provided or collected. Information of a questionable nature is not disseminated at the local level until a determination is made by this headquarters concerning the propriety of collection reporting and the information developed.

4.(U)~~(C)~~ Commanders of the facilities supported by the ACIP were queried in May 1971 concerning their recommendations relative to continuation of the program. Expressed desire for continuation was unanimous. To date, supported commanders' views remain unchanged and in view of this it is recommended that these programs be continued.

FOR THE COMMANDER:

11 Incl
Op Anal

RAY W. CHAMBERS
LTC, MI
Acting Assistant Adjutant General

REGRADED UNCLASSIFIED
ON Sep. 5, 1997
BY USAINSCOM FOIPA
Auth Para 4-102 DOD 5200.1R

CONFIDENTIAL

Page 1508 of 3957

CONFIDENTIAL

1. CANAL LOOP (OACSI approval - 16 Feb 72)

a. Location: Edgewood Arsenal, MD

b. Confidential Source Utilization: Five sources were used during this reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Personnel transfers have created a turbulence in both the project control officer and project liaison officer functions. It is anticipated that the operation will become more effective after permanent personnel assignments are made in the near future.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ...DISO USAINTC.....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1978.....

CONFIDENTIAL

CONFIDENTIAL

2. CANARY EFFORT (OACSI approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three sources were used during the reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Continuation is recommended because of the installation's sensitive mission with DOD as the Alternate National Command Post and the role assigned to USAINTC of executing the Alternate Joint Communications Center Counterintelligence Program. The commander of Fort Ritchie and the US Army element located within Site "R" desires the continuation of the ACIP.

REGRADED UNCLASSIFIED
ON Sep. 5, 1997
BY USAINSCOM FOIPA
Auth Para 4-102 DOD 5200.1R

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE [illegible] ORDER 11652
AUTOMATICALLY [illegible] TWO YEAR
INTERVALS DECLASSIFIED ON 31 DEC 1978

CONFIDENTIAL

Page 1510 of 3957

3. CANCER PORCH (OACSI approval - 28 Dec 71)

a. Location: Defense Language Institute, Southwest Branch, Fort Bliss, TX

b. Confidential Source Utilization: One confidential source was approved during this reporting period for recruitment.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The Defense Language Institute has recommended that the operation continue despite the reduction in the number of Vietnamese language students trained at the Institute.

REGRADED UNCLASSIFIED
ON Sep. 5, 1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE
AUTOMATICALLY
INTERVALS: DECLASSIFIED
YEAR 1977

~~CONFIDENTIAL~~

4. CANDID FROLIC (OACSI approval - 21 Dec 71)

a. Location: Fort Ord, CA

b. Confidential Source Utilization: Two confidential sources were used during the reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: One of the sources identified two military personnel assigned to Fort Ord and a USMA cadet who were allegedly members of the Vietnam Veterans Against the War (VVAW) who distributed VVAW literature on a military post and who encouraged military personnel to attend VVAW meetings.

e. Operational Status: Fort Ord is the only major US Army training center on the West Coast and is a major test site for Modern Volunteer Army concepts. Additionally, the US Army Combat Developments Experimentation Command is located on the post with field testing conducted at Hunter-Liggett Military Reservation. Disruption of these elements could have a serious adverse impact upon the mission of the Army in that area. As the site of the Pvt Billy Smith "fragging" court-martial, Fort Ord has become a focal point for dissident/subversive activity for both local groups as well as supporters of Angela Davis from the San Francisco area. Because of the foregoing factors, recommend that CANDID FROLIC be continued.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

DISO USAINTC

1978

~~CONFIDENTIAL~~ 12

~~CONFIDENTIAL~~

5. CENTRAL TAXI (OACSI approval - 16 Feb 72)

a. Location: HQ, US Army Electronics Command, Fort Monmouth, NJ

b. Confidential Source Utilization: Three confidential sources were used during the reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Information which identified four potential security problem areas was obtained and passed to the serviced command for appropriate action.

e. Operational Status: The full potential for this operation has not been achieved due to the frequent change of control personnel. This situation is expected to stabilize in the near future, resulting in subsequent improvement of the operation.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISO USAINTC
... GENERAL ... CATION
... TWO YEAR
INTERVALS; DECLASSIFIED ON 31 DEC 1978

~~CONFIDENTIAL~~ 13

CONFIDENTIAL

6. GONDOLA STAR (OACSI approval - 17 Feb 72)

a. Location: Aberdeen Proving Ground, Aberdeen, MD

b. Confidential Source Utilization: Two confidential sources were used during this reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: A turbulent project control officer and project liaison officer situation which exists as a result of USAINTC reorganization and ensuing personnel transfers has prevented the program from attaining maximum effectiveness. This particular situation is expected to be resolved during the next quarter and increased coverage of the installation will be accomplished. High priority tenant activities covered by the ACIP include the US Army Test and Evaluation Command, Land Warfare Laboratory, Human Engineering Laboratory and the Ballistic Research Laboratory.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by .....DISO USAINTC.....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1978.....

14

CONFIDENTIAL

~~CONFIDENTIAL~~

7. GONG SILK (OACSI approval - 16 Feb 72)

a. Location: Picatinny Arsenal, Dover, New Jersey

b. Confidential Source Utilization: Three confidential sources were used during the reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Information which identified three potential security problem areas was obtained through the sources and passed to the serviced command for action.

e. Operational Status: Because of the sensitivity of the mission performed by Picatinny Arsenal and the US Army Munitions Command, it is recommended that the operation be continued. Due to the relatively new status of the personnel involved in the ACIP, its full potential has not been reached. Improvement in effectiveness is anticipated.

REGRADED UNCLASSIFIED
ON SEP 5 ..7
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY ... YEAR
INTERVALS DECLASSIFIED ON 31 DEC 1978

15

~~CONFIDENTIAL~~

CONFI

8. LANDLESS TIME (OACSI approval - 19 Jan 72)

a. Location: Philadelphia Facility, US Army Electronics Command

b. Confidential Source Utilization: Four confidential sources were utilized during the reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The relatively recent reactivation of sources and newly assigned personnel have prevented this operation from reaching its full potential. Improvement in effectiveness is anticipated.

REGRADED UNCLASSIFIED
ON SEP - 5 1996
BY CDR USAINSCOM FOIPA
AUTH Para 1-603 DOD 5200.1-R

Classified by ....DISO USAINTC.....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC ..1978....

CONFI

9. LANYARD MOOD (OACSI approval - 22 Dec 71)

a. Location: Defense Language Institute East Coast Branch, Anacostia Naval Annex, Washington, DC

b. Confidential Source Utilization: No confidential sources were used during this reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Pending development of a more permanent source at this installation, conventional sources of information will continue activity to cover sensitive targets designated by the supported commander.

REGRADED UNCLASSIFIED
ON
BY OSEP US5 11997 OM FOIPO
AUTH Para 1-603 DOD 5200.1R

Classified by ..... DISO USAINTC .....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1978

17

CONFIDENTIAL

10. LENIENT CLOUD (OACSI approval - 16 Feb 72)

a. Location: US Army War College, Carlisle Barracks, PA

b. Confidential Source Utilization: Four confidential sources were utilized during the reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Due to the sensitivity of the installation itself and the large volume of classified material handled at the facility, recommend continuation of the operation.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ....DISO USAINTC.....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC ...1978.....

18

CONFIDENTIAL

CONFIDENTIAL

11. LENTIL MONKEY (OACSI approval - 26 Oct 71)

a. Location: Defense Language Institute West Coast Branch, Presidio of Monterey, CA

b. Confidential Source Utilization: Three confidential sources were used during the reporting period.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Two individuals assigned as instructors at the DLIWC have been shown to possess weaknesses which could be exploited by hostile intelligence services.

e. Operational Status: Faculty members of the DLIWC must be considered potential targets of hostile intelligence agencies which may be operating in the area of the DLIWC; especially with the establishment of a Soviet consulate in San Francisco and the loosening of restrictions on communications with the People's Republic of China. Three foreign language departments are now covered by confidential sources and two additional departments will be covered upon recruitment of two more sources.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DoD 5200.1R

Classified by D.S.O. USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1978

19

CONFIDENTIAL

SECRET

ACTION SHEET

CONTROL NUMBER

SUBJECT: Quarterly Report to USofA re: Aggressive Counterintelligence Program (ACIP) Operations (U)

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 31 July 1972

ACTION REQUIRED

To provide USofA with the second quarterly report on ACIPs.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By memorandum dated 8 February 1972, the Under Secretary of the Army requested that the Vice Chief of Staff, US Army provide quarterly reports on ACIPs (BLUE TAB D). He further requested that the report for the period ending 30 June 1972 provide a full analysis of the program.

b. The first quarterly report was submitted to the Under Secretary of the Army on 21 April 1972 (BLUE TAB C).

c. Written input from USAINTC for the current quarterly report is attached at BLUE TAB B. Subsequent coordination between USAINTC and OACSI representatives amplified their input which resulted in the information outlined in the memorandum to the Under Secretary of the Army (BLUE TAB A). To date, ICF in the total of $140.73 have been expended on these 11 ACIPs.

2. DISCUSSION: Memorandum to Under Secretary of the Army through Vice Chief of Staff, US Army, at BLUE TAB A provides required second quarterly report as desired by the USofA memorandum of 8 February 1972.

3. RECOMMENDATION: That Memorandum at BLUE TAB A be approved and signed.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		1 Aug 72
			DIV		1 Aug 72
			DIR	MK	1 Aug 72
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

J. MARTINS, MAJ/57471 J. D. Martins 31 July 1972

SPECIAL ACTIONS BR
RECORDS COPY

ACSI FORM 28, 13 Sep 71

SECRET

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

CONFIDENTIAL

8 AUG 1972

DAMI-DOI-S

MEMORANDUM THRU: VICE CHIEF OF STAFF, UNITED STATES ARMY

FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations (U)

1. Reference your memorandum of 8 February 1972, subject as cited.

2. The 11 ACIP operations reported to you in my 21 April 1972 memorandum, subject as above, remain in effect. No additional ACIP operations have been approved. A quarterly report of current operations is attached (TAB A). At TAB B is the evaluation you requested.

3. I do not believe we have yet had sufficient experience with this program under the new control limitations for a solid evaluation of its long-term merit. I will continue to submit quarterly reports to you on it, and will furnish you another evaluation at the end of the fourth quarter of operations under the new controls.

(sgd) Phillip B. Davidson, Jr.

2 Incl
as (CONFIDENTIAL)

PHILLIP B. DAVIDSON, JR.
Major General, GS
ACofS for Intelligence

Regraded UNCLASSIFIED when separated from classified inclosures

SPECIAL ACTIONS BR
RECORDS COPY

CONFIDENTIAL

~~CONFIDENTIAL~~

CURRENT ACIP OPERATIONS

LOCATION	ACIP NICKNAME	DATE APPROVED	NUMBER OF SOURCES
Edgewood Arsenal, Maryland	CANAL LOOP	16 February 72	5
Fort Ritchie, Maryland	CANARY EFFORT	16 February 72	4
Fort Bliss, Texas (Language School)	CANCER PORCH	28 December 71	0
Fort Ord, California	CANDID FROLIC	21 December 71	1
Fort Monmouth, New Jersey	CENTRAL TAXI	16 February 72	3
Aberdeen Proving Grounds, Maryland	GONDOLA STAR	16 February 72	3
Picatinny Arsenal, New Jersey	GONG SILK	16 February 72	3
Philadelphia, Pennsylvania (Electronics Command)	LANDLESS TIME	19 January 72	7
Washington, D.C. (Language School)	LANYARD MOOD	22 December 71	0
Carlisle Barracks, Pennsylvania (Army War College)	LENIENT CLOUD	16 February 72	4
Presidio of Monterey, California	LENTIL MONKEY	26 October 71	1
TOTALS 11	11		31

Off-post Information

There were no instances in which information on non-affiliated civilians was collected off-post.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ACSI, DA
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS
DECLASSIFIED ON 31 DECEMBER 1978

~~CONFIDENTIAL~~

CONFIDENTIAL

Information obtained:

Useful information was obtained, but except for prior warning of demonstrations at Fort Ord, California, no positive statements on specific security weaknesses or immediate threats to the Army were developed in this quarter. Inasmuch as these operations are a form of intensified security watchfulness, negative reports in themselves are frequently of value to a commander in planning for the security requirements of a given installation or activity. The placement and access of current sources, and those under consideration, are such that the chances of detecting a developing security threat situation in a sensitive installation or unit are greater with these sources operating.

Continuance of operations:

The eleven ACIP operations are being continued for the original stated purposes.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

CONFIDENTIAL

PROGRAM EVALUATION

Scope and Value: ACIP operations are defensive, on-post, security services, initiated at the request of a local commander. These operations are to provide commanders an intensified method of detecting internal security weaknesses and security threats to the supported command. Information is obtained from carefully selected sources who have on-post access to sensitive or critical defensive target areas. Activities to be covered are selected after joint discussions and agreements between the requesting commander and the supporting USAINTC element. Information is gathered through the use of both overt and covert sources who are selected from the DoD military or civilian workforce at the serviced installation. The primary values of ACIP operations are in the early warning and problem detection areas. The ultimate merit of the program cannot be assessed on a short term basis. Supported commands currently evaluate reported ACIPs as worthwhile security activities.

Number and placement of sources: To date, 31 sources have been recruited. (All sources were reactivated from operations which were in effect prior to curtailment of all ACIP operations in February 1971.) Continued recruitment and training of sources should produce, at a minimum, information for the supported command on personnel attitudes, possible disaffection, dissident activities and character weakness information of the type normally sought by foreign intelligence spotter personnel. During contacts, sources are debriefed, trained as necessary, and given specific guidance on future reporting objectives. In all cases, emergency contact procedures exist to insure rapid notification of significant information.

Adequacy of controls: DIRC inspections of Army intelligence field elements, plus inspections by OACSI and of DA field commands, show strict operational compliance with pertinent directives, keen awareness of DIRC investigative policies, and extreme caution about any acts which might cause criticism to the Army. In addition, the following control measures have been imposed upon USAINTC and subordinate field elements:

a. The ACIP is restricted to on-post target coverage of DoD affiliated personnel utilizing employees of the serviced command as sources. These restraints reduce to a minimum the possibility of violations of current collection restrictions regarding non-DoD affiliated personnel.

b. Sources are selected from the military/civilian workforce only after a long and detailed assessment. Normally only long-term employees of known reliability and loyalty are selected for recruitment.

Classified by ACSI, DA
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS
DECLASSIFIED ON 31 DECEMBER 1978

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

24

CONFIDENTIAL

~~CONFIDENTIAL~~

c. Each individual involved in the conduct or control of the ACIP is briefed on current policies and constraints pertaining to the program and activities as they concern persons and organizations not affiliated with the DoD.

No additional controls are recommended.

DOWNGRADED UNCLASSIFIED
ON SEP -5 1997
BY OSD LITIGATION R&I/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE COMMAND
FORT HOLABIRD, MARYLAND 21219

ICDISO-OC

17 JUL 1972

SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

HQDA (DAMI-DOI-S)
WASH DC 20310

1. (U) References:

a. Letter DAMI-DOI-S, 8 March 1972, subject as above.

b. Letter ICDISO-OC, 18 April 1972, subject as above.

2. (U) Forwarded herewith in compliance with reference a, above, is the ACIP quarterly report for the period 1 April 1972 - 30 June 1972.

3. (U) ~~(C)~~ The following operational and administrative control measures remain in effect concerning all reported ACIPs to assure compliance with DoD and DA policies relative to the acquisition of information on non-DoD affiliated personnel:

a. Each ACIP is restricted to on-post target coverage of DoD affiliated personnel and utilizes employees of the serviced command as sources. These constraints generally preclude the possibility of violations of current collection restrictions regarding non-DoD affiliated personnel.

b. Sources are selected from a civilian/military work force only after long and detailed assessment. Generally, only long term employees of known reliability and proven loyalty are selected for recruitment.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

26

~~CONFIDENTIAL~~

17 JUL 1972

ICDISO-OC
SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

c. Each individual and/or source involved in the conduct or control of each ACIP is briefed on current policies and restrictions pertaining to the program and program associated activities as concerns persons and organizations not affiliated with DoD.

d. ACIP reporting is scrutinized at each level of command to insure the acceptability of information provided or collected. Information of a questionable nature is not disseminated at the local level until a determination is made by this headquarters concerning the propriety of collection reporting and informational products.

4. (~~S~~)(U) Commanders of the facilities supported by the ACIP were queried in May 1971 concerning their recommendations relative to continuation of the program. Expressed desire for continuation was unanimous. To date, supported commanders' views remain unchanged and in view of this it is recommended that these programs be continued.

FOR THE COMMANDER:

DAVID L. BRUENING
CPT, MI
Acting Assistant Adjutant General

11 Incl
Op Anal

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

Page 1527 of 3957

~~CONFIDENTIAL~~

1. CANAL LOOP (OACSI Approval - 16 Feb 72)

a. Location: Edgewood Arsenal, Edgewood, MD

b. Confidential Source Utilization: Contact with five confidential sources formerly used in the program has been made. Four have been reactivated and regularly scheduled contacts effected. One former source has been transferred to another DoD installation and has been terminated.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: While little information of substantive value has been developed to date, confidential and overt sources of information will continue activity in support of coverage of sensitive targets designated by the supported commander.

e. Operational Status: Although regular contact has been established with all former sources, full utilization has been impeded by Army Intelligence personnel transfers and the requirement to train newly assigned personnel involved in source contact. Continuation of the ACIP CANAL LOOP is recommended because of the extreme sensitivity of the target installation.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

DECLASSIFIED UNCLASSIFIED
ON SEP - 5 1997
BY ODR USAINSCOM FOIA/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1528 of 3957

2. CANARY EFFORT: (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Contact with four confidential sources formerly used in the program has been made. All four sources have been reactivated and regularly scheduled contacts effected.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: While little information of substantive value has been developed to date, confidential and overt sources of information will continue activity in support of coverage of sensitive targets designated by the supported commander.

e. Operational Status: Although regular contact has been established with all former sources, full utilization has been impeded by Army Intelligence personnel transfers and the requirement to train newly assigned personnel involved in source contact. Continuation of ACIP CANARY EFFORT is recommended because of the installation's sensitive mission within DoD as the Alternate National Command Post; and the role of the ACIP in USAINTC' DA assigned mission of executing the Alternate Joint Communications Center Counterintelligence Program.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

29

~~CONFIDENTIAL~~

3. CANCER PORCH: (OACSI Approval - 28 Dec 71)

a. Location: Defense Language Institute Southwest Branch, Fort Bliss, TX

b. Confidential Source Utilization: None

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status: The scaledown of US participation in the Vietnam War has effected a steady reduction in the mission of the DLISW Vietnamese Language School, and a resultant decrease in student input and instructor cadre. On 1 May 1972, this Command requested DLI Headquarters reassess their need for ACIP support at the Southwest Branch. DLI requested that ACIP coverage continue until an exact projection of future Vietnamese Language requirements could be made.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

4. CANDID FROLIC: (OACSI Approval 21 Dec 71)

a. Location: Fort Ord, CA

b. Confidential Source Utilization: Regularly scheduled meetings were conducted with one confidential source during the reporting period. One other prospective source has been spotted and approved for recruitment.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Early warning was provided the Commanding General, Fort Ord, concerning the 29 April 1972 demonstration outside the main gate of Fort Ord, in support of Billy Dean Smith, and the 20 May 1972, Armed Forces Day March against the Presidio of Monterey.

e. Operational Status: As the only major US Army training facility on the West Coast; a test post for the Modern Volunteer Army concept, and the site of the Billy Dean Smith "fragging" trial, Fort Ord remains the focal point for dissident and/or subversive activity from both local radicals and from revolutionary elements in the San Francisco area. CANDID FROLIC is providing the CG, Fort Ord, with early warning type information upon which he can plan preventive measures to preclude disruption of post activities. Recommend continuation of ACIP CANDID FROLIC.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXEUCTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM MD
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

5. CENTRAL TAXI: (OACSI Approval 16 Feb 72)

a. Location: HQS, US Army Electronics Command, Fort Monmouth, NJ

b. Confidential Source Utilization: Contact with three confidential sources formerly used in the program has been effected. All three sources have been reactivated and regularly scheduled contacts effected.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: While little information of substantive value has been developed to date, confidential and overt sources of information will continue activity in support of coverage of sensitive targets designated by the supported commander.

e. Operational Status: Although regular contact has been established with all former sources, full utilization has been impeded by Army Intelligence personnel transfers and the requirement to train newly assigned personnel involved in source contact. Continuation of ACIP CENTRAL TAXI is recommended because of the extreme sensitivity of HQS, US Army Electronics Command and its supporting laboratories and the command's mission in the development and procurement of electronic warfare equipment and systems.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652.
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAIC
AUTH Para 1-603 DCID

32

CONFIDENTIAL

6. GONDOLA STAR: (OACSI Approval - 17 Feb 72)

a. Location: Aberdeen Proving Ground, Aberdeen, MD

b. Confidential Source Utilization: Contact with four confidential sources formerly used in the operation has been effected. Three sources have been reactivated and regularly scheduled contacts effected. One former source has been terminated since a realignment of functions at the installation prevents his participation in the program.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: While little information of substantive value has been developed to date, confidential and overt sources of information will continue activity in support of coverage of sensitive targets designated by the supported commander.

e. Operational Status: Although regular contact has been established with all former sources, full utilization has been impeded by Army Intelligence personnel transfers and the requirement to orient and familiarize newly assigned personnel with the operation. Continuation of ACIP GONDOLA STAR is recommended because of the sensitivity of the installation and the mission of tenant units, which include US Army Test and Evaluation Command, Land Warfare Laboratory, Human Engineering Laboratory and the Ballistic Research Laboratory.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

DEGRADED UNCLASSIFIED
ON SEP -5 1997
BY ODR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

CONFIDENTIAL

Page 1533 of 3957

7. GONG SILK: (OACSI Approval - 16 Feb 72)

a. Location: Picatinny Arsenal, Dover, NJ

b. Confidential Source Utilization: Contact with three confidential sources formerly used in the operation has been effected. All three sources have been reactivated and regularly scheduled contacts re-established.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: While little information of substantive value has been developed to date, confidential and overt sources of information will continue activity in support of coverage of sensitive targets designated by the supported commander.

e. Operational Status: Although regular contact has been established with all former sources, full utilization has been impeded by Army Intelligence personnel transfers and the requirement to train newly assigned personnel involved in source contact. Continuation of ACIP GONG SILK is recommended because of the sensitivity and criticality of the mission performed by Picatinny Arsenal and the US Army Munitions Command.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

34

~~CONFIDENTIAL~~

8. LANDLESS TIME: (OACSI Approval - 19 Jan 72)

a. Location: Philadelphia Facility, US Army Electronics Command

b. Confidential Source Utilization: Contact with seven confidential sources formerly used in the operation has been established. All sources have been reactivated and regularly scheduled contacts effected.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: While little information of substantive value has been developed to date, confidential and overt sources of information will continue activity in support of coverage of sensitive targets designated by the supported commander.

e. Operational Status: Although regular contact has been established with all former sources, full utilization has been impeded by Army Intelligence personnel transfers and the requirement to train newly assigned personnel involved in source contact. Continuation of the ACIP LANDLESS TIME is recommended because of the sensitive mission performed by the facility and by the National Inventory Control Point, which provides worldwide materiel inventory management of the Army's communications-electronics systems.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED on 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY OSD/WHS/DOCSVCS/FOI/PO
AUTH Para 1-603 DOD 5200.1R

35

~~CONFIDENTIAL~~

9. LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute East Coast Branch, Anacostia Naval Annex, Washington, DC

b. Confidential Source Utilization: None

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: While little information of substantive value has been developed to date, conventional and overt sources of information will continue activity in support of coverage of sensitive targets designated by the supported commander.

e. Operational Status: Reporting under LANYARD MOOD is concentrated principally on classroom monitoring by language students, the majority of whom are servicemen assigned Army Intelligence. The school is currently between classes and new student rosters are being screened for potential student sources. Although the DLI branch schools are relatively non-sensitive installations, the target represented by the language students requires some form of coverage or monitoring as many of the servicemen are destined for sensitive assignments in Communist Bloc countries. Recommend continuation of ACIP LANYARD MOOD.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1-R

36

~~CONFIDENTIAL~~

10. LENIENT CLOUD: (OACSI Approval - 16 Feb 72)

a. Location: US Army War College, Carlisle Barracks, PA

b. Confidential Source Utilization: Contact with four confidential sources formerly used in the operation has been established. All four sources have been reactivated and regularly scheduled contacts effected.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: While little information of substantive value has been developed to date, confidential and overt sources of information will continue activity in support of coverage of sensitive targets designated by the supported commander.

e. Operational Status: Although regular contact has been established with all former sources, full utilization has been impeded by Army Intelligence personnel transfers and the requirement to orient and familiarize newly assigned personnel with the operation. Recommend continuation of ACIP LENIENT CLOUD because of the sensitive training mission of the War College and classified mission of the Army Alternate Command Element, a tenant activity of Carlisle Barracks.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

37

~~CONFIDENTIAL~~

11. LENTIL MONKEY: (OACSI Approval - 26 Oct 71)

a. Location: Defense Language Institute West Coast Branch, Presidio of Monterey, CA

b. Confidential Source Utilization: One confidential source was recruited during the reporting period. No confidential sources were utilized in the program prior to the 17 Feb 71 suspension.

c. Information Obtained Off-post and Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: While little information of substantive value has been developed to date, confidential and overt sources of information will continue activity in support of coverage of sensitive targets designated by the supported commander. Suitability type information has been developed concerning an instructor who has made five trips to CSR since entering the United States in 1959.

e. Operational Status: Reporting under LENTIL MONKEY is concentrated principally on classroom monitoring by language students, the majority of whom are servicemen assigned to Army Intelligence. Although the DLI branch schools are relatively non-sensitive installations, the target represented by the language students requires coverage as many of the servicemen are destined for sensitive assignments in Communist Bloc countries. Recommend continuation of ACIP LENTIL MONKEY.

CLASSIFIED BY DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 78.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AR 380-5 DOD 5200.1R

Page 1538 of 3957

~~SECRET~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Quarterly Report to US of A Re: Aggressive Counter-intelligence Program (ACIP) Operations

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 17 April 1972

ACTION REQUIRED: To provide USofA with the initial Quarterly Report on ACIP's

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By Memorandum dated 8 Feb 72, the US of A requested that the Vice Chief of Staff, Army provide a Quarterly Report on Aggressive Counterintelligence Programs (TAB B). YELLOW

b. By note and referal slip dated 10 Feb 72 the VCofS, Army forwarded the action to the ACSI and directed that required reports and recommendations be submitted through his office (TAB C). YELLOW

c. By letter dated 8 Mar 72, CG USAINTC was formally tasked to provide required information to this office (TAB D) YELLOW in accordance with provisions of the US of A Memorandum.

d. By letter dated 14 Apr 72, CG USAINTC transmitted the required data to OACSI, DA (TAB E). YELLOW

2. DISCUSSION: Memorandum to USofA through VCofS, Army at TAB A YELLOW provides required report.

3. RECOMMENDATION: That memorandum at TAB A YELLOW be approved and signed.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		19 APR 72
			DIV	WB	19 April 72
			DIR		20 Apr 72
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

MAJOR W. WEBB/78874

~~SECRET~~

SPECIAL ACTIONS BR RECORDS COPY

ACSI FORM 28, 13 Sep 71

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~SECRET~~
SECRET

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

8 MAR 1972

DAMI-DOI-S

SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations

Commanding General
United States Army Intelligence Command
ATTN: ICDSO-O-S
Fort Holabird, Maryland 21219

1. References:

a. Paragraph 4, DAMI-DOI-S Letter, dated 16 February 1972, Subject: Aggressive Counterintelligence Program (ACIP) Operations.

b. Attached Memorandum from the Under Secretary of the Army, to the Vice Chief of Staff, United States Army, dated 8 February 1972, Subject: Aggressive Counterintelligence Program (ACIP) Operations.

2. The Under Secretary of the Army Memorandum directs that quarterly reports be provided his office, commencing with the quarter ending March 31, 1972. USAINTC input for these reports should be forwarded so as to arrive at DAMI-DOI-S no later than the 10th working day of the month following the close of the calendar quarter which they cover.

FOR THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE

CHARLES W. ALLEN
Colonel, GS
Director of Operations

1 Incl
as (SECRET)

Regraded UNCLASSIFIED when separated from classified inclosures

40

~~SECRET~~
SECRET

DCS 10 FEB 1972

DEPARTMENT OF THE ARMY
OFFICE CHIEF OF STAFF
WASHINGTON

10 February 1972

ACSI -

For action -- Please submit quarterly reports and recommendations thru me.

B. P.

41

41

SPECIAL INTEREST
ACTION

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF

REFERRAL SLIP

FILE NUMBER	DATE	CASE NUMBER	SUSPENSE DATE(S)
	10 February 1972	No 43496	

SUMMARY (Sources, date, and subject or short title)
Quarterly Report to USofA re ACIP Operations

OC of SA: 20 April 1972*
OASA( )
OUS of A: 20 April 1972*
OSA
OSD

ROUTING									
	OSA		CRD		C of F		CNGB		COPO
	CLL		CORC		TSG		CINFO		C of Spts
	DCSOPS		ACSFOR		C of Ch		CMH		CUSAAA
	DCSPER	XX	ACSI		TJAG		CAR		
	DCSLOG		TAG		TIG		TPMG		
	COA		C of Engrs		CC-E				

ATTENTION

ACTIONS					
X	APPROPRIATE ACTION		NOTE AND (Forward) (Return)	X	ADVANCE COPY provided
	DIRECT REPLY, COPY OF REPLY TO		INFORMATION ON WHICH TO BASE A REPLY		ACTION ASSIGNED TO
	PREPARE (Draft) (Final) REPLY FOR SIGNATURE OF		REPORT ESTIMATED COMPLETION DATE BY		PROVIDE ASSISTANCE AS REQUIRED
	INFORMATION		COORDINATE WITH	X	COPY FURNISHED TO DOMS, DSGS (CAR)

REMARKS

*This RS will remain in effect indefinitely; new suspense will be announced each quarter.

BY DIRECTION OF THE CHIEF OF STAFF:
Harry S B Sul
HARRY E. B. SULLIVAN
LTC, GS
Assistant Secretary of
the General Staff

~~CLASSIFIED~~ ~~separate from~~ ~~CLASSIFIED inclosures~~

TRANSFERS	DATE	AGENCY	ACTION TAKEN	SIGNATURE

RECEIPT	RECEIPT OF DOCUMENT IDENTIFIED ABOVE IS ACKNOWLEDGED:	DATE
	42	

OCofSA FORM 2 1 JAN 66 — REPLACES OCSA FORM 2, 3 AUG 64, AND OCSA FORM 7, 14 OCT 57, WHICH ARE OBSOLETE. — REMAINS WITH CORRESPONDENCE 1

MFR 19 APRIL 1972

DAMI-DOI-S

SUBJECT: Quaterly ACIP Report

1. USAINTC submitted their input for the quarterly ACIP report on 14 Apr 72. As result DAMI-DOI-S prepared the required package to forward their report to CSA.

2. On 17 Apr 72 Col IADOROSA, USAINTC called with request that USAINTC be allowed to expand their initial report. He explained that BG Epp did not get to see original reports prior to dispatch and was not happy with them when he finally did get to see them.

3. By letter ,undated, USAINTC provided DAMI-DOI-S with revised reports for each ACIP. Reports were received from USAINTC LN on 19 Apr 72. Per phoncon with Mr Arnold, USAINTC, I established the date of 18 Apr 72 as that which should be placed on the undated letter transmitting the reports received on 19 APR.

WALDO R WEBB
MAJ GS

45

43

DAMI-DOI-S

21 APR 1972

MEMORANDUM THRU: VICE CHIEF OF STAFF, UNITED STATES ARMY

FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

1. In your 8 February 1972 Memorandum, subject as cited, you requested quarterly reports on status of ACIP operations. Attached are reports on those operations in progress for the quarter ending 31 March 1972.

2. Your Memorandum accepted the fact that the closing date of the first quarter report would be too soon for any sound evaluation of these projects. This is borne out by attached reports. They indicate a cautious selection of potential confidential sources. Such a process is necessary for ACIP operations to provide the Army security threat information not obtainable through routine counterintelligence investigative and liaison work.

(sgd) Phillip B. Davidson, Jr.

11 Incl
as (CONFIDENTIAL)

PHILLIP B. DAVIDSON, JR.
Major General, GS
ACofS for Intelligence

44

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE COMMAND
FORT HOLABIRD, MARYLAND 21219

18 APR 1972

ICDISO-OC

SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

HQDA (DAMI-DOI-S)
WASH DC 20310

WARNING NOTICE: Sensitive Sources and Methods Involved

1. (U) Reference letter DAMI-DOI-S, 8 Mar 72, subject as above.

2. (U) Forwarded herewith in compliance with referenced letter is the quarterly report covering the period 1 Jan 72 - 31 Mar 72.

3. (U) ~~(C)~~ The following comments are submitted in order to better portray the role of the ACIP in enhancement of the security of the supported commands:

a. The Aggressive Counterintelligence Program is a defensive, on-post security service initiated at the request of the local commander. It provides a monitoring or surveillance of sensitive or critical areas of a command which are selected or recommended for ACIP coverage by the serviced commander. This is accomplished through the use of both overt and covert sources of information, selected exclusively from the DoD civilian and military workforce at the serviced installation.

b. The ACIP must be considered a long-range operation if it is to provide reliable, accurate and continuing access to information not obtainable through routine collection efforts.

4. (U) ~~(C)~~ Due to the lapse of time since the ACIPs were suspended, considerable effort and time is involved in the reactivation of approved ACIPs. ACIPs in the process of reactivation by this Command are subjected to continuous scrutiny to insure that they fall within the parameters of

45
45

GROUP 3
Downgraded at 12 year intervals; not automatically declassified

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

CONFIDENTIAL

ICDISO-OC
SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

current National level guidance and policy. All ACIPs are subject to continuing evaluation to determine their viability in support of accepted counterintelligence objectives.

James R. Waldie

11 Incl
as (dupe)

JAMES R. WALDIE
Colonel, Infantry
Deputy Commander

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FT BELVOIR
AUTH para 1-603 DOD 5200.1R

46

46

CONFIDENTIAL

CONFIDENTIAL

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

WARNING NOTICE: Sensitive Sources and Methods Involved

1. (U) NICKNAME: LENTIL MONKEY (U)

2. (U) LOCATION: Defense Language Institute, West Coast, Monterey, CA

3. (U) DATE APPROVED: 26 October 1971, per ACSI letter DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations.

4. (U)(C) BACKGROUND:

ACIP coverage of the Defense Language Institute, West Coast (DLIWC) was initiated by letter DLIWC, dated 11 September 1967, subject: Request for Aggressive Counterintelligence Support. Operation was suspended on 17 February 1971 in compliance to ACSI Memorandum, dated 16 February 1971, subject: Suspension of Certain Army Counterintelligence Programs. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his regular contact with the installation security office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator during which the progress of the program is discussed and recommendations made for future coverage.

5. (C) THREAT ANALYSIS:

a. General: The Defense Language Institute, West Coast, conducts training in a variety of foreign languages for students from all the military services.

b1

CONFIDENTIAL

47

JACL 1

b. Indicated Threat: Previous information developed through this ACIP revealed at least ten instances of instructors visiting communist bloc countries and being contacted by foreign nationals. Two of these visits resulted in direct solicitation of information concerning DLIWC. Future reporting will determine whether or not a threat continues to exist at this installation.

6. (U)(C) CONFIDENTIAL SOURCES UTILIZED: None. The program was in the initiation phase during this reporting period. One Confidential Source is to be recruited in April 1972. Additional sources for possible inclusion into the operation are presently under assessment. All sources recruited will be civilian or military personnel assigned to the installation.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None

8. (U)(C) USEFUL INFORMATION OBTAINED: Review of personal records identify three individuals, all members of the faculty of the Czechoslovakian Language Department, Defense Language Institute, West Coast (DLIWC), Presidio of Monterey, California, as possible targets of hostile intelligence.

9. (U)(C) OPERATIONAL STATUS: Operation should be continued. Faculty members of DLIWC must be considered potentially lucrative targets of hostile intelligence agencies which may be operating in the California area; especially with the impending establishment of a USSR Consulate in San Francisco, California.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOR
AUTH Para 1-603 DOD 5200.1-R

48

2 48

CONFIDENTIAL

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

WARNING NOTICE: Sensitive Sources and Methods Involved

1. (U) NICKNAME: CANDID FROLIC (U)

2. (U) LOCATION: Fort Ord, CA

3. (U) DATE APPROVED: 21 December 1971 per ACSI letter DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations (U).

4. (U)(~~C~~) COORDINATION: ACIP coverage of Fort Ord, CA was requested by the Commanding General, 26 November 1971 per letter AMNOR-B, HQS, Fort Ord, subject: Request for Aggressive Counterintelligence Support (U). Approval to initiate the program was contained in ACSI letter cited in paragraph three above. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his normal contact with the installation security/intelligence office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator, during which the progress of the program is discussed and recommendations made for future coverage.

5 (U)(~~C~~) THREAT ANALYSIS: ACIP CANDID FROLIC was initiated to provide the Commanding General, Fort Ord with a substitute Special Counter-intelligence Coverage to replace that formerly provided by GRADE PROGRESS, an Offensive Counterintelligence Operation currently under suspension. Fort Ord as the only major US Army training facility on the West Coast and as a test post for the Modern Volunteer Army is under constant, concerted attack by local anti-war and anti-Army civilian organizations. These organizations have extended their operations on-post under the legal guise of soldier counselling. An additional factor which contri-butes to the threat to the installation is the trial of PVT Billy Dean Smith, now in the Fort Ord Confinement Facility accused of the murder of two Army officers in Vietnam. Radicals and other groups have already given this impending event wide publicity and are attempting to charac-terize the trial as racial oppression. These efforts are expected to find adherents among the population of the Fort Ord complex who will undoubtedly attempt disruption either by outside direction or on their own initiative. Already, several off-post demonstrations, at the Fort Ord main gate, connected with this case have been conducted; a building which is being rehabilitated as a court room for the trial has been set afire and damaged by arsonist(s); and disruptive gatherings have been held on post to discuss and protest the trial.

6. (U)(~~C~~) CONFIDENTIAL SOURCES UTILIZED: None. The program was in the initiation phase during this first quarter. However, the first Confidential

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH Para 1-603 DOD 5200.1R

Downgraded at 12 year intervals; not automatically declassified DOD DIR 5200.10

CONFIDENTIAL

Source has been recruited and four others are under development. In addition, seven individuals are currently under assessment. Only DoD civilian and military personnel assigned the installation are recruited as confidential sources.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None.

8. (U)(C) USEFUL INFORMATION OBTAINED: During the reporting period, the following useful information was obtained through official liaison with local investigative agencies and through overt contact sources on the military installation. An Army chaplain's assistant is alleged to be assisting the MLP on-post at Fort Ord. In addition, a JAGC officer is alleged to have referred military personnel stationed at Fort Ord to PCS/MLP for legal counsel in obtaining discharges from the military service.

9. (U)(C) OPERATIONAL STATUS: It is recommended that the operation be continued in order to provide the Commanding General, Fort Ord, with early warning information upon which to base counter-actions against local dissident/subversive organizations who, through recruitment of servicemen, have extended their operations onto the government facility.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Page 1550 of 3957

CONFIDENTIAL

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

~~WARNING NOTICE: Sensitive Sources and Methods Involved~~

1. (U) NICKNAME: LANYARD MOOD (U)

2. (U) LOCATION: Defense Language Institute, East Coast, Anacostia Annex, US Naval Station, Washington, DC

3. (U) DATE APPROVED: 22 December 1971, per ACSI letter, DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations.

4. (U) ~~(C)~~ BACKGROUND:

ACIP coverage of Defense Language Institute, East Coast (DLI, EC) was initiated by letter request DLIEC, dated 16 November 1971, subject: Request for Aggressive Counterintelligence Support. It was suspended on 17 February 1971 by ACSI Memorandum dated 16 February 1971, subject: Suspension of Certain Army Counterintelligence Programs. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his regular contact with the installation security office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator during which the progress of the program is discussed and recommendations made for future coverage.

5. (C) THREAT ANALYSIS:

The Defense Language Institute East Coast Branch (DLIEC) conducts training in approximately 50 languages for an average student body of 1100, with responsibility for classroom training being placed upon civilian contract schools. No classified material is provided DLIEC instructors or students; therefore, there is no justification for the program exclusively to protect the security of the facility.

b1

The students reside at scattered locations throughout the Washington, DC area and the administrative control and supervision over them is decentralized among several headquarters.

GROUP 3
Downgraded at 12 year intervals; not automatically declassified

CONFIDENTIAL

51

Tab C 3

CONFIDENTIAL

Most of the students are young, impressionable servicemen, subjected to minimum military control, who are encouraged to socialize with their instructors and to attend functions at the various embassies and legations in the Washington area. The instructors are principally alien employees of a civilian contract school over whom DLIEC exercises virtually no administrative or supervisory control.

b1

6. (C) CONFIDENTIAL SOURCES UTILIZED: Spotting and assessing program for the recruitment of Confidential Sources has been instituted. The recruitment of sources will be limited to DoD civilians and military personnel assigned to the school.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None

8. (C) USEFUL INFORMATION OBTAINED: None. Sources have not been reactivated.

9. (C) OPERATIONAL STATUS: Aggressive Counterintelligence Program LANYARD MOOD should be continued because of the extreme sensitivity of the personnel assigned the installation. Current activity centers around the recruitment of sources to assure coverage of sensitive areas designated by the responsible commanders.

2 52

52

CONFIDENTIAL

~~CONFIDENTIAL~~

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

WARNING NOTICE: Sensitive Sources and Methods Involved

1. (U) NICKNAME: CANCER PORCH (U)

2. (U) LOCATION: Defense Language Institute Southwest, Biggs Field, Ft. Bliss, TX

3. (U) DATE APPROVED: 28 December 1971, per ACSI letter DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations.

4. (U) ~~(C)~~ BACKGROUND:

ACIP coverage of the Defense Language Institute Southwest (DLI, SW) was requested by letter DLISC-S2/3, DLI, SW, dated 23 October 1967, subject: Request for Aggressive Counterintelligence Support and was instituted by this Command in 1968. Coverage was suspended on 17 February 1971 per ACSI Memorandum, dated 16 February 1971, subject: Suspension of Certain Army Counterintelligence Programs. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his regular contact with the installation security intelligence office. Formal quarterly briefings are given the Commandant of the serviced installation or his designated ACIP Coordinator during which the progress of the program is discussed and recommendations made for future coverage.

5. (~~C~~) THREAT ANALYSIS:

a. General: The Defense Language Institute Southwest Branch (DLISW) is a subordinate facility of Headquarters, Defense Language Institute (DLI), and was activated 1 August 1966, to provide Vietnamese Language instruction to Department of the Army personnel. The instructors are native born Vietnamese, employed by civilian contract schools, over whom the DLI exercises little or no control. No classified material is provided DLISW instructors or students; therefore, there is no justification for the program exclusively to protect the security of the facility. Principal cover emphasis is placed upon the protection and/or the surveillance of the military student body which consists primarily of young impressionable servicemen.

53

55

~~CONFIDENTIAL~~

GROUP 3
Downgraded at 12 year intervals; not automatically declassified

Page 4

the majority of whom are faced with a Southeast Asia assignment. Many of these servicemen have a preconceived opposition to the US policy in Southeast Asia, while others, apprehensive about their pending assignment to Vietnam, are susceptible to the influences of their fellow students or to subtle suggestions made by their Vietnamese instructors. Information has been received from the Vietnamese Government indicating that a group of "left-wing" Vietnamese students were planning to use Vietnamese Language instructors to encourage resistance to the US policy in Southeast Asia. Although the school has an established student/instructor non-fraternization policy, the close, long-term contact initiated during prolonged courses of instruction often results in the establishment of close friendships.

b1

6. (C) CONFIDENTIAL SOURCES UTILIZED: Two prospective Confidential Sources, with placement and access, have been spotted and are currently being assessed and developed. Sources utilized in the ACIP are DoD civilian and military employees of the serviced facility.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None

8. (C) USEFUL INFORMATION OBTAINED: None. Sources have not been reactivated.

9(U)(C) OPERATIONAL STATUS: Aggressive Counterintelligence Program CANCER PORCH should be continued because of the extreme sensitivity of the personnel assigned to the installation. Current activity centers around the reactivation of former confidential sources and the recruitment of new sources to assure coverage of sensitive areas designated by the responsible commanders.

~~CONFIDENTIAL~~

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

~~WARNING NOTICE: Sensitive Sources and Methods Involved~~

1. (U) NICKNAME: LANDLESS TIME (U)

2. (U) LOCATION: US Army Electronics Command, Philadelphia Facility, Philadelphia, PA.

3. (U) DATE APPROVED: 19 January 1972 per ACSI letter DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations (U).

4. (U) ~~(C)~~ BACKGROUND: ACIP coverage of the Philadelphia Facility, US Army Electronics Command, was initiated 8 October 1965 per letter AMSEL-SE-P, HQS, US Army Electronics Command, Fort Monmouth, NJ, subject: Request for Aggressive Counterintelligence Program (ACIP) Support (U). On 17 February 1971, LANDLESS TIME was suspended per instructions contained in ACSI Memorandum dated 16 February 1971, subject: Suspension of Certain Army Counterintelligence Programs. This operation was reactivated per authority contained in ACSI letter cited in paragraph three above. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his normal contact with the installation security/intelligence office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator, during which the progress of the program is discussed and recommendations made for future coverage.

5. (C) THREAT ANALYSIS:

a. General:

b1

55

~~CONFIDENTIAL~~

Downgraded at 12 year intervals; not automatically declassified DOD DIR 5200.10

INCL 5

CONFIDENTIAL

b1

b. Developed Information:

During the existence of LANDLESS TIME, one instance was reported involving an employee in which the employee had been in close personal contact with a foreign national. Investigation revealed the interest of hostile intelligence in this individual and subsequent contact by the foreign national was indicative of a preliminary assessment. Information of a suitability nature was also reported concerning several employees.

6. (C) CONFIDENTIAL SOURCES UTILIZED: None. The Project Liaison Officer is checking to determine the location, status, and continued suitability of previous Confidential Sources for reactivation by the Project Control Officer. Sources utilized in LANDLESS TIME will be recruited only from DoD civilian and military personnel assigned the serviced installation.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None

8. (C) USEFUL INFORMATION: Because the operation is in its initial phase of reactivation, no useful information of counterintelligence interest to MI and the serviced command, Philadelphia Facility, US Army Electronics Command, was developed.

9. (C) OPERATIONAL STATUS: The operation should be continued because of the current sensitivity of the installation. Current activity centers around the reactivation of former confidential sources and the recruitment of new sources to assure coverage of sensitive areas designated by the Commander of the facility.

56

CONFIDENTIAL

Page 1556 of 3957

CONFIDENTIAL

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

~~WARNING NOTICE: Sensitive Sources and Methods Involved~~

1. (U) NICKNAME: GONDOLA STAR (U)

2. (U) LOCATION: Aberdeen Proving Ground, MD

3. (U) DATE APPROVED: 16 February 1972, per ACSI letter DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations.

4. (U) (c) BACKGROUND:

ACIP coverage of Aberdeen Proving Ground was initiated by letter AMCIS-SI, US Army Materiel Command, dated 29 November 1965, subject: Request for Aggressive Counterintelligence Program (ACIP) (U). On 17 February 1971, GONDOLA STAR was suspended per instructions ACSI-STF Memorandum, dated 16 February 1971, subject: Suspension of Certain Army Counterintelligence Programs. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his regular contact with the installation security office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator during which the progress of the program is discussed and recommendations made for future coverage.

5. (c) THREAT ANALYSIS:

a. General:

b1

(1)

b1

CONFIDENTIAL

GROUP 3
Downgraded at 12 year intervals; not automatically declassified

CONFIDENTIAL

(2) b1

(3) b1

(4) b1

b. b1

6. (C) CONFIDENTIAL SOURCES UTILIZED: Initial contact has been made with two sources utilized prior to GONDOLA STAR's suspension. Also, action is being taken to recruit additional sources. Activation of these sources must await their complete assessment.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None

8. (C) USEFUL INFORMATION OBTAINED: None. Sources have not been reactivated.

9. (C) OPERATIONAL STATUS: Aggressive Counterintelligence Program GONDOLA STAR should be continued because of the extreme sensitivity of the installation and because of the potential threat to the National security posed by the sensitive mission performed by Aberdeen Proving Ground. Current activity centers around the reactivation of former confidential sources and the recruitment of new sources to assure coverage of sensitive areas designated by the responsible commanders.

CONFIDENTIAL

58

Page 1558 of 3957

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

~~WARNING NOTICE: Sensitive Sources and Methods Involved~~

1. (U) NICKNAME: GONG SILK (U)

2. (U) LOCATION: Picatinny Arsenal, NJ

3. (U) DATE APPROVED: 16 February 1972 per ACSI letter DAMI-DOI-S, Subject: Aggressive Counterintelligence Program (ACIP) Operations (U).

4. (C) BACKGROUND:

ACIP coverage of the US Army Munitions Command and Picatinny Arsenal, NJ, was initiated 15 May 1968 per letter AMSMU-SS-S, HQS US Army Munitions Command, subject: Request for Aggressive Counterintelligence Program (ACIP) Support (U). On 17 February 1971, GONG SILK was suspended per instructions contained in ACSI Memorandum dated 16 February 1971, subject Suspension of Certain Army Counterintelligence Programs. The operation was reactivated per authority contained in ACSI letter cited in paragraph three above. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his normal contact with the installation security office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator during which the progress of the program is discussed and recommendations made for future coverage.

5. (C) THREAT ANALYSIS

a. General:

b1

GROUP 3

Incl 7

59

CONFIDENTIAL

b1

b. Developed Information: Previously, GOMG SILK provided extensive information concerning contact, both personal and through correspondence, between scientific personnel employed at Picatinny Arsenal and foreign scientists. Instances were also reported concerning foreign individuals seeking scientific papers published by the employees. Many instances were reported concerning character weaknesses and behavior problems of employees, six of which resulted in termination of employment.

6. (C) CONFIDENTIAL SOURCES UTILIZED: None. The Project Liaison Officer is conducting discreet checks to determine the location, status and continued suitability of previous Confidential Sources for reactivation by the Project Control Officer. Sources utilized in GOMG SILK will be recruited only from DoD civilian and military personnel assigned at the serviced installation.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None

8. (C) USEFUL INFORMATION OBTAINED: Because the operation is in its initial phase of reinstitution, no useful information of counter-intelligence interest was developed.

9. (C) OPERATIONAL STATUS: The operation should be continued because of the extreme sensitivity of the installation and the criticality of the mission it performs for the Department of the Army. Current activity centers around the reactivation of former confidential sources and the recruitment of new sources to assure coverage of sensitive areas designated by the Commanding General, USAMUCOM.

CONFIDENTIAL

Page 1560 of 3957

CONFIDENTIAL

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

[redacted] and Methods Involved

1. (U) NICKNAME: CENTRAL TAXI (U)

2. (U) LOCATION: Fort Monmouth, NJ

3. (U) DATE APPROVED: 16 February 1972, per ACSI letter DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations.

4. (U) BACKGROUND: ACIP coverage of the US Army Electronics Command, Fort Monmouth, NJ, was initiated 4 October 1967 per letter AMSEL-EI, HQS, US Army Electronics Command, subject: Request for Aggressive Counter-intelligence Support (U). On 17 February 1971, CENTRAL TAXI was suspended per instructions contained in ACSI Memorandum, dated 16 February 1971, subject: Suspension of Certain Army Counterintelligence Programs. The operation was reinitiated per authority contained in letter cited in paragraph 3 above. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his normal contact with the installation security office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator during which the progress of the program is discussed and recommendations made for future coverage.

5. (C) THREAT ANALYSIS:

b1

CONFIDENTIAL

Downgraded at 12 year intervals; not automatically declassified DOD DIR 5200.10

CONFIDENTIAL

b1

6. (C) CONFIDENTIAL SOURCES UTILIZED: None. The Project Liaison Officer is conducting discreet checks to determine the location, status, and continued suitability of previous Confidential Sources for reactivation by the Project Control Officer. Sources utilized in CENTRAL TAXI are recruited only from among the DoD civilian and military personnel assigned the serviced facility.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None

8. (C) USEFUL INFORMATION OBTAINED: Because the operation is in its initial phase of reinstitution, no useful information of counterintelligence interest was developed.

9. (C) OPERATIONAL STATUS: The operation should be continued because of the current sensitivity of the installation, and the criticality of the mission it performs for the Department of the Army. Current activity centers around the reactivation of former confidential sources and the recruitment of new sources to assure coverage of sensitive areas designated by the Commanding General, USAECOM.

CONFIDENTIAL

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

~~WARNING NOTICE: Sensitive Sources and Methods Involved~~

1. (U) NICKNAME: CANARY EFFORT (U)

2. (U) LOCATION: Fort Ritchie, MD

3. (U) DATE APPROVED: 16 February 1972, per ACSI letter DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations (U).

4. (C) BACKGROUND:

Aggressive Counterintelligence Program coverage of Fort Ritchie, MD, was initiated 11 August 1965, per letter SCCJ-B, HQS, US Army Joint Support Command, subject: Aggressive Counterintelligence Program. On 17 February 1971, CANARY EFFORT was suspended per instructions contained in ACSI Memorandum dated 16 February 1971, subject: Suspension of Certain Army Counterintelligence Programs. The operation was reinitiated per authority contained in letter cited in paragraph 3, above. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his regular contact with the installation security office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator during which the progress of the program is discussed and recommendations made for future coverage.

5. (C) THREAT ANALYSIS:

b1

63

CONFIDENTIAL

GROUP 3
12 year

Tab 9

CONFIDENTIAL

b1

6. (C) CONFIDENTIAL SOURCES UTILIZED: Initial contact made with three Confidential Sources previously utilized prior to suspension of operation. One of the three has been reassigned on base and reassessment will be made to determine whether he is now within a legitimate target. Reactivation of the other two sources is taking place. Sources utilized in the ACIP are DoD civilian and military employees of the serviced facility.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None

8. (C) USEFUL INFORMATION: None. Sources have not been fully reactivated.

9. (C) OPERATIONAL STATUS: Aggressive Counterintelligence Program CANARY EFFORT should be continued because of the extreme sensitivity of the installation and its mission within DoD as an Alternate National Command Post in time of emergency. Current activity centers around the reactivation of former confidential sources and the recruitment of new sources to assure coverage of sensitive targets or areas designated by the commander.

64

CONFIDENTIAL

CONFIDENTIAL

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

WARNING NOTICE: Sensitive Sources and Methods Involved

1. (U) NICKNAME: LENIENT CLOUD (U)

2. (U) LOCATION: Carlisle Barracks, PA

3. (U) DATE APPROVED: 16 February 1972 per ACSI letter DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations (U).

4. (C) BACKGROUND:

ACIP coverage of Carlisle Barracks and the US Army War College was initiated 13 August 1965 per letter AIBCB, HQS, Carlisle Barracks, subject: Counterintelligence Program. On 17 February 1971, LENIENT CLOUD was suspended per instructions contained in ACSI Memorandum dated 16 February 1971, subject: Suspension of Certain Army Counterintelligence Programs. This operation was reactivated per authority contained in ACSI letter cited in paragraph three above. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his normal contact with the installation security/intelligence office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator, during which the progress of the program is discussed and recommendations made for future coverage.

5. (C) THREAT ANALYSIS:

b1

CONFIDENTIAL

CONFIDENTIAL

a. b1

b. b1

c. b1

d. b1

e. b1

f. b1

6. (C) CONFIDENTIAL SOURCES UTILIZED: None. Four confidential sources formerly used in the operation have not been recontacted. Sources utilized in the ACTP will be limited to DoD civilian and military personnel assigned the serviced installation.

66

CONFIDENTIAL

CONFIDENTIAL

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-DoD AFFILIATED CIVILIANS: None

8. (U) USEFUL INFORMATION OBTAINED: Because the operation is in its initial phase of reinitiation, no useful information of counterintelligence significance was developed.

9. (C) OPERATIONAL STATUS: This operation should be continued because of the sensitivity of the installation and the criticality of the mission it performs for the Department of the Army. Current activity includes the briefing of the Commanding General, USAMC, who has assumed his position since the suspension of the operation. Following this briefing, recontact of former confidential sources will be attempted.

REGRADED UNCLASSIFIED
ON 7661 6 JJS
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

67

CONFIDENTIAL

CONFIDENTIAL

ACIP QUARTERLY REPORT

Period Ending: 31 March 1972

~~WARNING NOTICE: Sensitive Sources and Methods Involved~~

1. (U) NICKNAME: CANAL LOOP (U)

2. (U) LOCATION: Edgewood Arsenal, MD

3. (U) DATE APPROVED: 16 February 1972, per ACSI letter DAMI-DOI-S, subject: Aggressive Counterintelligence Program (ACIP) Operations.

4. (U) BACKGROUND:

ACIP coverage of Edgewood Arsenal was initiated 15 June 1965 by letter of request of the Commanding Officer, Edgewood Arsenal, thru the Commanding Generals, US Army Munitions Command and US Army Materiel Command. On 17 February 1971, CANAL LOOP was suspended per instructions contained in ACSI Memorandum dated 16 February 1971, subject: Suspension of Certain Army Counterintelligence Programs. This operation was reinitiated per authority contained in letter cited in paragraph three above. Information developed by the ACIP is provided the serviced command on a regular basis by the Project Liaison Officer in his regular contact with the installation security office. Formal quarterly briefings are given the Commander of the serviced installation or his designated ACIP Coordinator during which the progress of the program is discussed and recommendations made for future coverage.

5. (C) THREAT ANALYSIS:

a. General:

b1

GROUP 3
Downgraded at 12 year intervals; not automatically declassified

68

CONFIDENTIAL

Encl 11

CONFIDENTIAL

(1) b1

(2) b1

(3) b1

(4) b1

b. b1

6. (C) CONFIDENTIAL SOURCES UTILIZED: Initial contact made with five Confidential Sources previously utilized prior to suspension of operation. Activation of these sources will take place following further assessment. Sources recruited for utilization within the AKIP are limited to DoD civilians and military personnel assigned the serviced facility.

7. (U) INFORMATION OBTAINED OFF-POST AND REPORTED ON NON-AFFILIATED CIVILIANS: None

8. (C) USEFUL INFORMATION OBTAINED: None. Sources have not been reactivated.

69

2 69

CONFIDENTIAL

9. (C) OPERATIONAL STATUS: Aggressive Counterintelligence Program CANAL LOOP should be continued because of the extreme sensitivity of the installation and because of the potential threat to the National security posed by the sensitive mission performed by Edgewood Arsenal. Current activity centers around the reactivation of former confidential sources and the recruitment of new sources to assure coverage of sensitive areas designated by the responsible commanders.

REGRADED UNCLASSIFIED
ON 27 SEP 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

DCSOPS 10 FEB 1972

DEPARTMENT OF THE ARMY
OFFICE CHIEF OF STAFF
WASHINGTON

10 February 1972

ACSI -

For action — Please submit quarterly reports and recommendations thru me.

B. P.

71

71

SPECIAL INTEREST
ACTION

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF

REFERRAL SLIP

FILE NUMBER	DATE	CASE NUMBER	SUSPENSE DATE(S)
	10 February 1972	No 43496	

SUMMARY (Sources, date, and subject or short title)
Quarterly Report to USofA re ACIP Operations

OC of SA: 20 April 1972*
OASA( )
OUS of A: 20 April 1972*
OSA
OSD

ROUTING									
	OSA		CRD		C of F		CNGB		COPO
	CLL		CORC		TSG		CINFO		C of Spts
	DCSOPS		ACSFOR		C of Ch		CMH		CUSAAA
	DCSPER	XX	ACSI		TJAG		CAR		
	DCSLOG		TAG		TIG		TPMG		
	COA		C of Engrs		CC-E				

ATTENTION

ACTIONS					
X	APPROPRIATE ACTION		NOTE AND (Forward) (Return)	X	ADVANCE COPY provided
	DIRECT REPLY, COPY OF REPLY TO		INFORMATION ON WHICH TO BASE A REPLY		ACTION ASSIGNED TO
	PREPARE (Draft) (Final) REPLY FOR SIGNATURE OF		REPORT ESTIMATED COMPLETION DATE BY		PROVIDE ASSISTANCE AS REQUIRED
	INFORMATION		COORDINATE WITH	X	COPY FURNISHED TO DOMS, DSGS (CAR)

REMARKS

*This RS will remain in effect indefinitely; new suspense will be announced each quarter.

BY DIRECTION OF THE CHIEF OF STAFF:

Harry S/S Sul

HARRY E. B. SULLIVAN
LTC, GS
Assistant Secretary of
the General Staff

TRANSFERS	DATE	AGENCY	ACTION TAKEN	SIGNATURE

RECEIPT

RECEIPT OF DOCUMENT IDENTIFIED ABOVE IS ACKNOWLEDGED:

DATE

SIGNATURE OF PERSON TO WHOM ROUTED AND DESIGNATION

SIGNATURE

12 72

OCofSA FORM 2 1 JAN 65

REPLACES OCSA FORM 2, 3 AUG 64, AND OCSA FORM 7, 14 OCT 57, WHICH ARE OBSOLETE.

REMAINS WITH CORRESPONDENCE

~~SECRET~~

OSA,OGC/RGreene/pf/13Jan72

8 FEB 1972

MEMORANDUM FOR THE VICE CHIEF OF STAFF
United States Army

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

On 4 December 1971 you forwarded to me a memorandum from the Assistant Chief of Staff for Intelligence, SUBJECT: Counterintelligence Policy Guidance, which informed me of the ACSI's decision to reactivate certain Aggressive Counterintelligence Program (ACIP) Operations. Attached to the memorandum was the operation plan for one such operation. I have reviewed that memorandum and the attached plan, and although I appreciate the conscientious steps which have been taken to assure adherence to current policies in this area, I remain concerned that this program may be placing us in a highly vulnerable position.

DoD Directive 5200.27 and the implementing Army policy letter dated 1 June 1971 impose two restrictions which are particularly relevant to ACIP operations. First, they require that there be "no covert or otherwise deceptive surveillance or penetration of civilian organizations" without the prior approval of the Chairman, DIRC (now the Assistant Secretary of Defense (Comptroller)). Second, they prohibit assigning DoD personnel "to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information the collection of which is authorized" without my prior approval, except in emergency situations. These prohibitions apply whether or not the formal "target" of the operation is affiliated with the Department of Defense. Although the ACSI letter approving the first reactivated ACIP operation incorporates these restrictions by reference (paragraph 3a), the operation plan and related documents obviously assume that confidential sources working in the operation may obtain and report information which they receive in the course of activities off military installations. While the plan prohibits extending the collection effort "directly" to non-DoD personnel (paragraph 4a(a)), and while the ACSI approval letter prohibits making non-DoD personnel "targets" of off-post surveillance, I would assume that it is entirely possible that in the course of their off-post activities confidential sources might obtain and report information

OSA,OGC - cnt
OSA,ASG
USA - cnt
Mr. Greene

~~SECRET~~

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY OSD USAINSCOM FOI/PO
FILE 1-603 DOD 5200.1R

FILE

73-2770B

OSA, ASG Control No. 2220 F

OSA 350.05 DOMESTIC INTELLIGENCE (2/8/72) FW 1/7/71

on non-affiliated civilians. Although such activity might not in all situations be forbidden by DoD Directive 5200.27, it is clearly on the borderline, and I therefore feel it is very important that these operations be closely supervised and tightly controlled.

In order to make an informed decision about whether further controls are necessary (including possible Under Secretary or DIRC review of each operation), I would appreciate your taking the following steps:

1. Beginning March 31, 1972, I would like to receive a quarterly report containing the following information on each ACIP operation in progress at any time during the reporting period: Date approved, code-name, location, number of confidential sources used during reporting period, number of instances in which information on non-affiliated civilians is obtained off-post and reported, and a brief narrative statement explaining whether useful information was obtained during the reporting period, whether the operation is to be continued, and if so, why. These reports may be submitted 30 days after the close of the calendar quarter which they cover.

2. With the second quarterly report, which will be due July 31, 1972, I would like to receive a full analysis of this program, including its value in terms of producing useful information and the adequacy of the controls which have been imposed. Recommendations for any further necessary controls should be included.

(sgd) Kenneth E. BeLieu

Kenneth E. BeLieu
Under Secretary of the Army

SECRETARY OF THE ARMY
OFFICE
FEB 8 10 01 AM '72
DISPATCHED
ADMINISTRATIVE
OFFICE

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

2

74

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☐ Information has been withheld in its entirety in accordance with the following exemption(s):

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☑ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 75-78

IAGPA-CSF Form 6-R
1 Sep 93

THIS MUST REMAIN T O P D O C U M E N T

DOSSIER NO. ZF011946W
Vol 2 of 7 Vols

As of 18 Sep 85 (Date) all material included in this file conforms with DA policies currently in effect.

Delmar Smith (Signature) 18 Sep 85 (Date Signed)

Delmar Smith (Printed Name) GS5 (Grade)

Reviewed for Retention
Criteria UP AR 381-10
Reviewer [illegible] Date 4/20/93

THIS MUST REMAIN T O P D O C U M E N T

IA (HQ) Form 2214
(1 Sep 78)

Replaces MIIA Fm 315, 1 Jun 75, which may be used until supplies are exhausted.

79

I C I P

CY 73

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

7 Nov 73

ACSI ~~ACSI~~ Hqrs

Sir, pls note Gen Weyand's comment to his approval.

D/O has directed USAINTC to study the problem and I have told D/O to insure that the study concludes with a new title less "aggressive."

CINCUSARPAC deleted some words. It's a big improvement

81

OLIVER B. PATTON
Brigadier General, GS
Deputy ACofS for Intelligence

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, D.C. 20310

2 November 1973

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations (U)

1. (U) Reference is made to memorandum, Under Secretary of the Army, dated 8 February 1972, subject as above.

2. (U~~C~~) The nine Aggressive Counterintelligence Program (ACIP) Operations reported by memorandum to you last quarter, all remain active. Two new operations CANARY STONE at Dugway Proving Ground, Utah and CENTAUR RACE at Fort Lewis, Washington were requested by the installation commanders, approved by ACSI, DA and implemented during the reporting period. These operations bring the total to 11 active ACIP's. At present, five ACIP proposals have been submitted by CONUS field commanders for consideration. The report of current operations for the quarter ending 30 September 1973 is attached.

3. (U~~C~~) The primary values of ACIP operations are in their potential for early warning and detecting internal security weakness and security threats to the supported command. Inasmuch as these operations are a form of intensified security watchfulness, negative reports in themselves are frequently of value to a commander in planning for security requirements of a given installation or activity.

1 Incl
as (CONFIDENTIAL)

FRED C. WEYAND
General, United States Army
Vice Chief of Staff

DOWNGRADED UNCLASSIFIED
ON Sep. 5, 1997
BY USAINSCOM FOIPA
Auth Para 4-102 DOD 5200.1R

Classified by DAMI-DO
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 1979

82
02

~~CONFIDENTIAL~~

~~SECRET~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

REPLY TO ATTENTION OF: DAMI-DOI-S

29 OCT 1973

MEMORANDUM FOR: VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above (Inclosure 2).

2. Recommend your approval and signature of the memorandum at Inclosure 1 which transmits the report required by the cited reference.

3. Coordination: None required.

OLIVER B. PATTON
Brigadier General, GS
Acting ACofS for Intelligence

2 Incl
1. Memo for USofA w/attachment ~~(CONFIDENTIAL)~~
2. Memo for VCSA, 8 Feb 72 ~~(SECRET)~~

2 Nov 1973

APPROVED - VCSA w/comment: "Why the title 'Aggressive CIP'? Drop the 'aggressive' unless there's some rationale for it that escapes me."

[redacted] F. [redacted]MIRE
MAJ, GS
Assistant Secretary of the General Staff

- Regraded UNCLASSIFIED when separated from classified inclosures.

83
85

~~SECRET~~

LTC Strom/bjs/77017

ACTION SHEET ~~SECRET~~

CONTROL NUMBER

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 19 October 1973

ACTION REQUIRED: To obtain approval of the quarterly ACIP report.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By memorandum dated 8 February 1972 (GREEN TAB B) the Under Secretary of the Army requested the Vice Chief of Staff, US Army, provide quarterly reports on all ACIPs.

b. This is the sixth such quarterly report.

c. USAINTC input is at GREEN TAB C.

2. DISCUSSION: The memorandum at GREEN TAB A forwards a memorandum to the VCSA to forward the report for the quarter ending 30 September 1973.

3. RECOMMENDATION: That the memorandum to the VCSA at GREEN TAB A be approved and signed.

(Continue on plain bond)

IMPLICATIONS CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV	WFS	24 Oct 73
			DIR	WFS	24 Oct 73
			EX		
			ACSI		
			DISPATCHED (DTG)		

Regraded unclassified when separated from Classified Inclosures.

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

84

ACTION OFFICER *(Name, grade, phone and signature)*

R.M. STROM, LTC/77017

~~SECRET~~

SPECIAL ACTIONS BR
RECORDS COPY

ACSI FORM 28, 13 Sep 71

REGRADED
WHEN SEPARATED FROM CLASSIFIED
DOCUMENT

~~CONFIDENTIAL~~

CURRENT ACIP OPERATIONS

LOCATION	ACIP NICKNAME	DATE APPROVED	NUMBER CONFIDENTIAL SOURCES
Edgewood Arsenal, Maryland	CANAL LOOP	16 Feb 72	5
Fort Ritchie, Maryland	CANARY EFFORT	16 Feb 72	3
Dugway Proving Ground, Utah	CANARY STONE	18 Jul 73	0
Fort Lewis, Washington	CENTAUR RACE	30 Jul 73	0
Fort Monmouth, New Jersey	CENTRAL TAXI	16 Feb 72	3
Aberdeen Proving Grounds, Maryland	GONDOLA STAR	16 Feb 72	2
Picatinny Arsenal, New Jersey	GONG SILK	16 Feb 72	3
Philadelphia, Pennsylvania (Electronics Command)	LANDLESS TIME	19 Feb 72	3
Washington, D.C. (Language School)	LANYARD MOOD	22 Dec 71	0
Carlisle Barracks, Pennsylvania (Army War College)	LENIENT CLOUD	16 Feb 72	4
Presidio of Monterey, California	LENTIL MONKEY	26 Oct 71	1
TOTALS	11	11	24

Declassified by DAMI-DO
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS
DECLASSIFIED ON 31 DECEMBER 1979

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY ODR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

85

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U S ARMY INTELLIGENCE COMMAND
FORT MEADE, MARYLAND 20755

OCT 16 1973

ICDO-OP

SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

HQDA (DAMI-DOI-S)
WASH DC 20310

1. (U) References:

a. Letter, DAMI-DOI-S, 8 March 1972, subject as above.

b. Letter, ICDISO-OC, 11 October 1972, subject as above.

c. Letter, ICDO-OP, 12 July 1973, subject as above.

2. (U) In compliance with reference a, above, the ACIP quarterly report for the period 1 July - 30 September 1973 is forwarded herewith.

3. (U) Operational and administrative control measures outlined in reference b, above, remained in effect during the reporting period. There were no reported instances of acquisition of information on non-DoD affiliated personnel.

4. (U) ~~(e)~~ During the reporting period emphasis was placed upon improving the viability of the program and stressing its importance at all levels throughout the Command. The scope of existing operations is currently being broadened to provide source coverage in depth of the designated target areas. The result should be an increase in significant items reported to the supported commanders.

5. (U) ~~(e)~~ ACIP briefings were given to appropriate staff members of the newly formed major commands, TRADOC and FORSCOM. Procedures were implemented to have the same briefing presented to selected commanders at the local level. This effort is expected to result in additional ACIP requests. In conjunction with these actions, the ACIP implementation process is being examined with a view towards decreasing the length of

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FRIPO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

86
86

~~CONFIDENTIAL~~

ICDO-OP
SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

time between the receipt of a request for an operation and the date it becomes productive. Two plans for new operations are being processed and will be forwarded for approval. These, plus the recently approved operations at Seneca Army Depot the Management Systems Support Agency, will add four ACIP gains during the next quarter.

FOR THE COMMANDER:

11 Incl
as

JESSE D. JOY, JR.
Colonel, GS
Deputy Chief of Staff, Operations

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

87

[redacted]

1. CANAL LOOP: (OACSI Approval - 16 Feb 72)

a. Location: Edgewood Arsenal, Edgewood, MD

b. Confidential Source Utilization: Five sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The sensitivity of the activities serviced has not diminished and the supported command desires that the operation be continued.

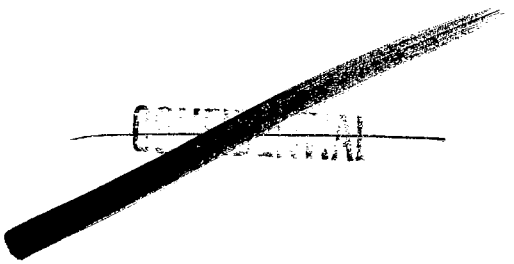
REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC

1979

88

[redacted]



2. CANARY EFFORT: (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: A civilian staff member at the installation has projected a trip to the USSR. This matter will be monitored on a continuing basis to determine if attempts to exploit have been or will be made by hostile intelligence.

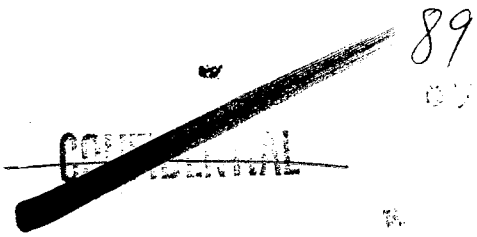
e. Operational Status: Continuation of the operation is desired by the supported commander. A new Project Liaison Officer has just reported and assumed his duties.

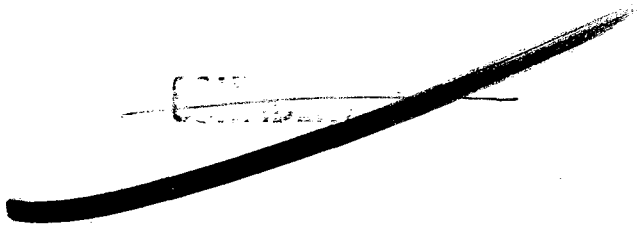
REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC

1979

89





3. CANARY STONE: (OACSI Approval - 18 Jul 73)

a. Location: Dugway Proving Ground, Utah

b. Confidential Source Utilization: No sources were recruited during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status: This operation was implemented with the briefing of the commander on 21 August 1973, and has not yet become fully operational.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ..... DCSOPS USAINTC .....
SUBJECT TO GENERAL DECLASSIFICATION
[illegible] 1974

90

4. CENTAUR RACE: (OACSI Approval - 30 Jul 73)

a. Location: Fort Lewis, WA

b. Confidential Source Utilization: No sources were recruited during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status: This operation was implemented with the briefing of the commander and staff on 23 August 1973, and has not yet become fully operational.

RECRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAITC

Page 1588 of 3957

[redacted]

5. CENTRAL TAXI: (OACSI Approval - 16 Feb 72)

a. Location: Headquarters, US Army Electronics Command, Fort Monmouth, NJ

b. Confidential Source Utilization: Three sources were used during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The Director of Security believes that the mission and function of this command place it high on hostile intelligence target priorities. One additional source was approved for recruitment during the reporting period.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT 2 YEAR
INTERVALS; NOT AUTOMATICALLY DECLASSIFIED
1979

[redacted]

[redacted]

6. GONDOLA STAR: (OACSI Approval - 17 Feb 73)

a. Location: Aberdeen Proving Ground, MD

b. Confidential Source Utilization: Two sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Inasmuch as the sensitivity of the activities serviced remains the same, the commander desires that the operation continue. The Project Liaison Officer retired on 31 July 1973, and his replacement is not expected until 1 November 1973. This will unfortunately delay the planned expansion in source coverage.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAMJC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF [illegible]
EXEMPTION CATEGORY [illegible] NO YEAR
IMPOSSIBLE DECLASSIFICATION ON 31 DEC 1979

[redacted]

Page 1590 of 3957

[redacted]

7. GONG SILK: (OACSI Approval - 16 Feb 72)

a. Location: Picatinny Arsenal, Dover, NJ

b. Confidential Source Utilization: Three sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The sensitivity of the activities covered remains extreme, so that the operation should be continued. Some target areas were cancelled with the departure of the Munitions Command, so that coverage should be somewhat simplified.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJ... GENERAL DECLASSIFICATION
SCH...
AU...
INDEFINITE ... YEAR 1979

94

[redacted]

8. LANDLESS TIME: (OACSI Approval - 19 Jan 72)

a. Location: Philadelphia Facility, US Army Electronics Command

b. Confidential Source Utilization: Three sources were contacted during the reporting period.

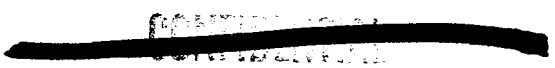
c. Information Obtained: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Of the three sources contacted, one retired and one transferred to another DoD facility, leaving the single source indicated in the previous report. The Project Liaison Officer will spot and assess prospective sources among the personnel moving to Fort Monmouth for utilization when this operation is incorporated into CENTRAL TAXI. At the request of the commander, coverage will continue until the facility is phased out.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS DECLASSIFIED ON 31 DEC 1979



Page 1592 of 3957

[redacted]

9. LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute East Coast Branch
Anacostia Naval Annex, Washington, DC

b. Confidential Source Utilization: To date, this operation has been using conventional sources.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Effective with the beginning of the new reporting period, the modus operandi is being changed to develop confidential sources in addition to the conventional sources used heretofore. Targets will be reconfirmed and redefined as necessary.

DECLASSIFIED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FT MEADE
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS; NOT AUTOMATICALLY DECLASSIFIED
1979

[redacted] 96

10. LENIENT CLOUD: (OACSI Approval - 16 Feb 72)

a. Location: US Army War College, Carlisle Barracks, PA

b. Confidential Source Utilization: Four sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Two security hazards and three instances of suitability information were reported. Foreign travel by one employee was not considered significant.

e. Operational Status: An additional target is being added. During the period, the newly assigned Project Liaison Officer developed a total of 25 conventional sources who are being contacted on a regular basis.

REGRADED UNCLASSIFIED ON SEP 5 7 BY CDR USAINSCOM F91/PO AUTH Para 1-603 DOD 5200.1R

DCSOPS USAINTC

19 79

11. LENTIL MONKEY: (OACSI Approval - 26 Oct 71)

a. Location: Defense Language Institute West Coast Branch
Presidio of Monterey, CA

b. Confidential Source Utilization: One source was recruited during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Seven additional students are being processed for use as confidential sources, and 20 conventional sources were recruited for broad coverage of target language departments. In addition, all of the 132 class monitors have been given SAEDA briefings and directed to report any incidents occurring in the classes.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY COR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAUTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF E
AUTO
INTERVALS. DE
YEAR
1979

98

ACTION SHEET

CONTROL NUMBER

SUBJECT: Aggressive Counterintelligence Program Operations

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 19 July 1973

ACTION REQUIRED: To obtain approval of a quarterly report.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By memorandum dated 8 February 1972 (GREEN TAB B) the Under Secretary of the Army requested the Vice Chief of Staff, US Army, provide quarterly reports on all ACIPs.

b. This is the fifth such quarterly report.

c. USAINTC Input is at GREEN TAB C.

2. DISCUSSION: The memorandum at GREEN TAB A forwards a memorandum to the VCSA to forward the report for the quarter ending 30 June 1973.

3. RECOMMENDATION: That the memorandum to the VCSA at GREEN TAB A be approved and signed.

(Continue on plain bond)

IMPLICATIONS CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		19 JULY 73
			DIV		26 Jul 73
			DIR		26
			EX		
			ACSI		27 Jul 73
			DISPATCH	APPROVED	31 JUL 1973

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*
R. MYERS, CPT/77017

99

SPECIAL ACTIONS BR
RECORDS COPY

ACSI FORM 28, 13 Sep 71

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~SECRET~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

REPLY TO ATTENTION OF: DAMI-DOI-S

31 JUL 1973

MEMORANDUM FOR: VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above (Inclosure 2).

2. Recommend your approval and signature on the memorandum at Inclosure 1 which transmits the report required by cited reference.

3. Coordination: None required.

2 Incl
1. Memo for USofA w/attachment (CONFIDENTIAL)
2. Memo for VCSA, 8 Feb 72 (SECRET)

for WILLIAM E. POTTS
Major General, GS
ACofS for Intelligence

OLIVER B. PATTON
Brigadier General, GS
Deputy ACofS for Intelligence

1 AUG 1973

APPROVED - VCSA.

MICHAEL P. SPIGELMIRE
MAJ, GS
Assistant Secretary of the General Staff

Regraded UNCLASSIFIED when separated from classified inclosures

100

~~SECRET~~

CPT Myers/bah/77017

[redacted]

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, D.C. 20310

1 August 1973

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Aggressive Counterintelligence Program Operations

1. Reference memorandum, Under Secretary of the Army, dated 8 February 1972, subject as above.

2. Of the 11 Aggressive Counterintelligence Program (ACIP) Operations reported to you by memorandum from this office, dated 4 May 1973, subject as above, nine remain in effect. Operation CANCER PORCH at the Defense Language Institute, Southeast Branch was terminated with the closing of the activity on 31 May 1973. Operation CANDID FROLIC at Fort Ord, California, was terminated on 12 June 1973 at the request of the installation commander. No new ACIP operations were initiated. The report of current operations for the quarter ending 30 June 1973 is attached.

3. The primary values of ACIP operations are in their potential for early warning and for detecting internal security weakness and security threats to the supported command. Inasmuch as these operations are a form of intensified security watchfulness, negative reports in themselves are frequently of value to a commander in planning for security requirements of a given installation or activity.

1 Incl
as (CONFIDENTIAL)

FRED C. WEYAND
General, United States Army
Vice Chief of Staff

CPT Myers/bah/77017

101

[redacted]

REGRADED UNCLASSIFIED
WHEN SEPARATED FROM

[redacted]

DAMI-DOI-S

21 Dec 1973

MEMORANDUM FOR: ACTING VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above (Inclosure 2).

2. Recommend your approval and signature on the memorandum at Inclosure 1 which transmits the report required by cited reference.

3. Coordination: None required.

(Sgd) Oliver B. Patton

WILLIAM E. POTTS
Major General, GS
ACofS for Intelligence

2 Incl
1. Memo for USofA
w/attachment (CONFIDENTIAL)
2. Memo for VCSA, 8 Feb 72
(SECRET)

OLIVER B. PATTON
Brigadier General, GS
Deputy ACofS for Intelligence

CONFIDENTIAL when
[illegible] detached

ACTION BR
RECORDS COPY

102

[redacted]

CONFIDENTIAL

CPT Myers/bah/77017

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, D.C. 203[redacted]

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Aggressive Counterintelligence Program Operations

1. Reference memorandum, Under Secretary of the Army, dated 8 February 1972, subject as above.

2. Of the 11 Aggressive Counterintelligence Program (ACIP) Operations reported to you by memorandum from this office dated 4 May 1973, subject as above, nine remain in effect. Operation CANCER PORCH at the Defense Language Institute, Southwest Branch was terminated with the closing of the activity on 31 May 1973. Operation CANDID FROLIC at Fort Ord, California, was terminated on 12 June 1973 at the request of the installation commander. No new ACIP operations were initiated. The report of current operations for the quarter ending 30 June 1973 is attached.

3. The primary values of ACIP operations are in their potential for early warning and detecting internal security weakness and security threats to the supported command. Inasmuch as these operations are a form of intensified security watchfulness, negative reports in themselves are frequently of value to a commander in planning for security requirements of a given installation or activity.

1 Incl
as (~~CONFIDENTIAL~~)

FRED C. WEYAND
General, United States Army
Acting Vice Chief of Staff

Regraded UNCLASSIFIED when separated from classified inclosures

103

CPT Myers/bah/77017

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

CURRENT ACIP OPERATIONS

LOCATION	ACIP NICKNAME	DATE APPROVED	NUMBER CONFIDENTIAL SOURCES
Edgewood Arsenal, Maryland	CANAL LOOP	16 February 72	5
Fort Ritchie, Maryland	CANARY EFFORT	16 February 72	3
Fort Monmouth, New Jersey	CENTRAL TAXI	16 February 72	3
Aberdeen Proving Grounds, Maryland	GONDOLA STAR	16 February 72	2
Picatinny Arsenal, New Jersey	GONG SILK	16 February 72	3
Philadelphia, Pennsylvania (Electronics Command)	LANDLESS TIME	19 January 72	4
Washington, D.C. (Language School)	LANYARD MOOD	22 December 71	0
Carlisle Barracks, Pennsylvania (Army War College)	LENIENT CLOUD	16 February 72	4
Presidio of Monterey, California	LENTIL MONKEY	26 October 71	0
TOTALS 9	9		24

Off-post Information

Operational LENTIL MONKEY obtained information off-post by coincidence and not as part of the operation. A source who was accompanying his student group on a field trip was among those of the group shown pictures of three Czech females who were looking for pen-pals. The source reported the incident.

Classified by DAMI-DO
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS
DECLASSIFIED ON 31 DECEMBER 1979

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM-F01/PO
AUTH Para 1-603 DOD 5200.1R

104

Information Obtained:

No information to indicate the existence of a hostile threat to the installations or a possible security hazard was developed during this reporting period.

Continuance of Operations:

Nine ACIP operations are being continued for the originally stated purposes.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAIMSCOM FOIA/PO
AUTH Para 1-603 DOD 5200.1R

105

Page 1602 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE COMMAND
FORT HOLABIRD, MARYLAND 21219

JUL 12 1973

ICDO-OP

SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

HQDA (DAMI-DOI-S)
WASH DC 20310

1. (U) References:

a. Letter, DAMI-DOI-S, 8 March 1972, subject as above.

b. Letter, ICDISO-OC, 11 October 1972, subject as above.

c. Letter, ICDO-OP, 11 April 1973, subject as above.

2. (U) In compliance with reference a, above, the ACIP quarterly report for the period 1 April - 30 June 1973 is forwarded herewith.

3. (U) Operational and administrative control measures outlined in reference b, above, remained in effect during the reporting period. There was one instance of acquisition of information on non-DoD affiliated personnel, described in the inclosure covering LENTIL MONKEY (U).

4. (U) Supported commanders continue to indicate satisfaction with the program. They view the lack of contradictory information as reassurance that their employees are observing security regulations, and that no apparent hostile intelligence activities have been mounted against the installation. A certain amount of suitability information was developed during the reporting period at some of the installations, but was either minor or had not yet been confirmed. In such cases, the information is not passed to the supported commander.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ....DCSOPS USAINTC.....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC ....1979....

106

~~CONFIDENTIAL~~

[redacted]

JUL 1 2 1973

ICDO-OP
SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

5. (U) Operations CANCER PORCH (U) and CANDID FROLIC (U) were terminated during the period covered by this report.

6. (U) Processing of the requests for ACIP support set forth in reference c, above, except for the Deseret Test Center, have not yet been completed. Additionally, an Operation Plan regarding ACIP support at Fort Lewis was forwarded on 7 July 1973. It is anticipated that future ACIP operations will result primarily from the recently established Sensitive Activity Vulnerability Estimate (SAVE) program.

FOR THE COMMANDER:

11 Incl
as

EDWARD H. BORT
LTC, MI
Acting Deputy Chief of Staff,
Operations

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

[redacted]

~~CONFIDENTIAL~~

1. CANAL LOOP: (OACSI Approval - 16 Feb 72)

a. Location: Edgewood Arsenal, Edgewood, MD

b. Confidential Source Utilization: Five sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The sensitivity and criticality of activities covered warrant the continuation of the support provided.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USATAC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

2. CANARY EFFORT (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Continuation of the operation is desired by the supported commander. Inasmuch as a new Project Control Officer is being assigned during the next quarter, recruitment of additional sources is being delayed until he assumes his duties.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS AND DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

Page 1606 of 3957

~~CONFIDENTIAL~~

3. CANCER PORCH: (OACSI Approval - 28 Dec 71)

a. Location: Defense Language Institute Southwest Branch
Fort Bliss, TX

b. Confidential Source Utilization: One source was contacted during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The operation was terminated with the closing of the activity on 31 May 1973. The source has been transferred to the Defense Language Institute West Coast, where contact will be re-established with him.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FT MEO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 79

~~110~~

~~CONFIDENTIAL~~

4. CANDID FROLIC: [redacted] (OACSI Approval - 21 Dec 71)

a. Location: Fort Ord, CA

b. Confidential Source Utilization: Two sources were contacted during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: As the result of discussion during a quarterly briefing on 16 May 73, on 18 May 73 the CG requested that the operation be terminated. No significant information had been produced to justify the risk of possible compromise or the further expenditure of manhours. Operational activity ceased at once, and the operation was officially terminated on 12 Jun 73, on which date security debriefings of the sources involved were concluded.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1-R

Classified by DCSOPS USAINSCOM
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1977

~~CONFIDENTIAL~~

Page 1608 of 3957

[redacted]

5. CENTRAL TAXI: (OACSI Approval - 16 Feb 72)

a. Location: Headquarters, US Army Electronics Command, Fort Monmouth, NJ

b. Confidential Source Utilization: Three sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The Commander desires that the operation continue. The impending assignment of a new Project Control Officer will allow the expansion of the operation by recruitment of additional sources.

DECLASSIFIED UNCLASSIFIED
SEP -5 1997
BY USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

[redacted]

Page 1609 of 3957

~~CONFIDENTIAL~~

6. GONDOLA STAR: (OACSI Approval - 17 Feb 72)

a. Location: Aberdeen Proving Ground, MD

b. Confidential Source Utilization: Two sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: In view of the sensitivity/criticality of this installation, the supported commander desires that the operation continue.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINSCOM
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

Page 1610 of 3957

7. GONG SILK: (OACSI Approval - 16 Feb 72)

a. Location: Picatinny Arsenal, Dover, NJ

b. Confidential Source Utilization: Three sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Despite the fact that modifications of the operation may be necessitated by forthcoming organizational changes, the Commander desires that the operation be continued.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1974

Page 1611 of 3957

~~CONFIDENTIAL~~

8. LANDLESS TIME: (OACSI Approval - 19 Jan 72)

a. Location: Philadelphia Facility, US Army Electronics Command

b. Confidential Source Utilization: Four sources were utilized during the reporting period. This includes one source who was reluctant to be reactivated when the operation was revalidated, but finally agreed.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: By 30 Jun 74, this activity will be completely relocated to Fort Monmouth, and the operation will be terminated. One source transferred during the period, rather than make the move. Another is scheduled to move in Nov 73, and plans to do so. He will be transferred to the Monmouth operation at that time. Coverage will be difficult during the phaseout, but the commander has requested that the operation continue as long as possible.

DECLASSIFIED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF [illegible] UNDER [illegible]
AUTOMATICALLY [illegible] AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

~~115~~

~~CONFIDENTIAL~~

9. LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute East Coast Branch
Anacostia Naval Annex, Washington, DC

b. Confidential Source Utilization: This operation uses conventional sources from the student body, primarily Army MI personnel.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The combination of alien instructors and students who are generally scheduled for sensitive assignments overseas makes this operation a necessity. With classrooms teaching 50 languages at various locations in the DC area, coverage is dependent on the availability of sources.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DASOPS USAINSCOM
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 77

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

10. LENIENT CLOUD: (OACSI Approval - 16 Feb 72)

a. Location: US Army War College, Carlisle Barracks, PA

b. Confidential Source Utilization: Four sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The Commander continues to be appreciative of information provided and desires that the operation continue.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAIMTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

116A

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

11. LENTIL MONKEY: (OACSI Approval - 26 Oct 71)

a. Location: Defense Language Institute West Coast Branch
Presidio of Monterey, CA

b. Confidential Source Utilization: Three sources were utilized during the reporting period, but all were eventually terminated due to graduation.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: On 18 May 73, students of a Czech class visited a Czech restaurant in San Francisco on a field trip. While they were there, the owner showed the students pictures of three girls residing in Czechoslovakia who were looking for American pen-pals. Each of three students received the name and address of one of the girls. One of the students who received this data was a Confidential Source, and reported the incident. The other two students are now en route to Army Security Agency school at Fort Devens, MA, and will eventually be assigned in USAREUR.

d. Useful Information Obtained: The above information assumes significance only if this proves to be an operational technique of Czech Intelligence. Consideration is being given to utilizing the source, now on TDY at Fort Huachuca, AZ, to probe this situation by establishing correspondence with the Czech girl. Under the circumstances, reporting this information is not considered a violation of the 1 June 71 letter.

e. Operational Status: Just as in LANYARD MOOD, the combination of alien-born instructors and students destined for sensitive assignments overseas is considered to offer a challenge to hostile intelligence. Additional MI students have reported to the institute, and no problems are anticipated in recruiting new sources.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINTELCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

117

~~CONFIDENTIAL~~

1st Qtr 73

~~SECRET~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Quarterly ACIP Report

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 23 April 1973

ACTION REQUIRED: To forward memorandum requesting VCSA sign memorandum to USA.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By Memorandum dated 8 February 1972, the Under Secretary of the Army requested the Vice Chief of Staff, US Army provide quarterly reports on all ACIP's (BLUE TAB B).

b. The fourth quarterly report for 1972 was submitted to the Under Secretary of the Army on 12 February 1973 (BLUE TAB C).

c. Written input from USAINTC for the current quarterly report is attached at BLUE TAB D.

2. DISCUSSION:

a. Word received from the SGS on 1 February 73 revealed the new VCSA desires to personally sign all memoranda to the Under Secretary of the Army. How long this new policy is to be effective is currently unknown. Based on DA memoranda 340-15 and 340-17, the ACSI has signed previous memoranda concerning this subject for the VCSA.

b. The memorandum at BLUE TAB A forwards a memorandum to the VCSA requesting he sign and forward to the Under Secretary of the Army, the first quarterly ACIP report for 1973. Per agreement SGS and DAMI, this same procedure was used to forward the previous quarterly report.

3. RECOMMENDATION: That the Memorandum to the VCSA at BLUE TAB A be approved and signed.

(Continue on plain bond)

IMPLICATIONS CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		23 Apr 73
			DIV		23 Apr 73
			DIR		24 Apr 73
			EX		
			ACSI		26 Apr 73
			DISPATCHED (DTG)		
			26 APR 1973		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

W. WEBB, MAJ/77017

SPECIAL ACTIONS BR
RECORDS COPY

118

~~SECRET~~

ACSI FORM 28, 13 Sep 71

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED

~~SECRET~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

REPLY TO ATTENTION OF: DAMI-DOI-S

26 APR 1973

MEMORANDUM FOR: VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above (TAB B).

2. Recommend your approval and signature on the memorandum at TAB A which transmits the report required by cited reference.

WILLIAM E. POTTS for
Major General, GS
ACofS for Intelligence

THOMAS W. BOWEN
Brigadier General, GS
Director of Intelligence
Support

2 Incl
TAB A - Memo for USofA (~~CONFIDENTIAL~~)
TAB B - USofA memo, 8 Feb 72 (~~SECRET~~)

CS 350.09 (26 Apr 73)

4 MAY 1973

APPROVED - OCSA

PETER B. PETERSEN
LTC, GS
Assistant Secretary of the General Staff

Regraded UNCLASSIFIED when separated from classified inclosures

119

~~SECRET~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, D.C. 20310

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Aggressive Counterintelligence Program Operations

1. Reference your memorandum of 8 February 1972, subject as above.

2. The 11 Aggressive Counterintelligence Program (ACIP) operations reported to you by my memorandum, dated 12 February 1973, subject as above, remain in effect. No additional ACIP operations have been approved. A quarterly report of current operations is attached.

1 Incl
as ~~(CONFIDENTIAL)~~

ALEXANDER M. HAIG, JR.
General, United States Army
Vice Chief of Staff

Regraded UNCLASSIFIED when separated from classified Inclosures

120

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

CURRENT ACIP OPERATIONS

LOCATION	ACIP NICKNAME	DATE APPROVED	NUMBER OF SOURCES
Edgewood Arsenal, Maryland	CANAL LOOP	16 February 72	5
Fort Ritchie, Maryland	CANARY EFFORT	16 February 72	3
Fort Bliss, Texas (Language School)	CANCER PORCH	28 December 71	1
Fort Ord, California	CANDID FROLIC	21 December 71	2
Fort Monmouth, New Jersey	CENTRAL TAXI	16 February 72	3
Aberdeen Proving Grounds, Maryland	GONDOLA STAR	16 February 72	2
Picatinny Arsenal, New Jersey	GONG SILK	16 February 72	3
Philadelphia, Pennsylvania (Electronics Command)	LANDLESS TIME	19 January 72	4
Washington, D.C. (Language School)	LANYARD MOOD	22 December 71	0
Carlisle Barracks, Pennsylvania (Army War College)	LENIENT CLOUD	16 February 72	4
Presidio of Monterey, California	LENTIL MONKEY	26 October 71	3
TOTALS 11	11		30

Off-post Information

There were no instances in which information on non-affiliated civilians was collected off-post.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DAMI-DO
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS
DECLASSIFIED ON 31 DECEMBER 1978

121

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Information Obtained:

a. During the first quarter of 1973, none of the ACIP operations produced information which would indicate the existence of an active hostile threat to the supported installation nor were any reports received concerning potential security hazards to the supported installations. As emphasized in each quarterly report submitted to date, ACIP operations are a form of intensified security watchfulness. As such, the lack of reportable information from these operations is also of value to a commander in planning for his security requirements. The placement and access of current sources, and those under consideration, are such that the chances of detecting a developing security threat situation in a sensitive installation or unit are greater with these sources already operating.

b. Significantly, supported commanders have voiced satisfaction with ACIP operational results to date and have reiterated their desire that these operations continue.

Continuance of Operations:

The eleven ACIP operations are being continued for the originally stated purposes.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1620 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE COMMAND
FORT HOLABIRD, MARYLAND 21219

11 APR 1973

ICDO-OP

SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

HQDA (DAMI-DOI-S)
WASH DC 20310

1. (U) References:

a. Letter, DAMI-DOI-S, 8 Mar 72, subject as above.

b. Letter, ICDISO-OC, 11 Oct 72, subject as above.

c. Letter, ICDISO-OC, 15 Jan 73, subject as above.

d. Letter, DAMI-DOI-P, 26 Feb 73, subject: Counterintelligence Support for Security of Nuclear Weapons, with 1st Indorsement, ICDO, 12 Mar 73.

2. (U) In compliance with reference a, above, the ACIP quarterly report for the period 1 January - 31 March 1973 is forwarded herewith.

3. (U) Operational and administrative control measures outlined in reference b, above, remained in effect during the reporting period. There were no instances of acquisition of information on non-DoD affiliated personnel.

4. (U) ~~(C)~~ Utilization of the ACIP to enhance the security of chemical and nuclear weapons, as set forth in reference c, above, has been integrated into the overall counterintelligence support to the US Army Materiel Command (AMC) and HQ, US Army Air Defense Command. Action taken on this program will be reported as outlined in reference d, above. In the future, this quarterly report will pertain only to operations in progress and those in the planning stage.

REGRADED UNCLASSIFIED ON SEP - 5 1997 BY CDR USAINSCOM FOI/PO AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS. DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

Page 1621 of 3957

~~CONFIDENTIAL~~

ICDO-OP 11 APR 1973
SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

5. (U) ~~(C)~~ In the area of chemical and nuclear weapons, the Commander of Seneca Army Depot has formally requested an ACIP operation. The Commander, Savanna Army Depot, has requested an ACIP briefing. Additional assessment of the Sierra Army Depot will be necessary to determine the applicability of the ACIP. Requests for the program have been received from Harry Diamond Laboratories, US Army Mobility Equipment and Development Center, and Deseret Test Center, all subordinate to AMC. The Commander, US Army Management Systems Support Agency, an automatic data processing facility in the Pentagon supporting the Office of the Vice Chief of Staff, has also submitted a formal request for the program. The assessments necessary to justify the program in each case have been accomplished or are underway, and individual Operations Plans are expected in the near future.

6. (U) ~~(C)~~ In an effort to replace the expertise and continuity which have been lost through the reduction of civilian Excepted Service Position spaces in the MI Groups, an effort is underway to obtain Great Skills personnel for inclusion in the program.

FOR THE COMMANDER:

Walter J. Cronin, Jr.

11 Incl
as

WALTER J. CRONIN, JR.
Colonel, GS
Deputy Chief of Staff, Operations

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

1. CANAL LOOP: (OACSI Approval - 16 Feb 72)

a. Location: Edgewood Arsenal, Edgewood, MD

b. Confidential Source Utilization: Five sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The operation should be continued because of the criticality and sensitivity of the installation, as well as the reiterated desires of the Commander that this support be continued.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH: Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

2. CANARY EFFORT: (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The Commander desires continuation of the operation in view of the sensitivity/criticality of the facility and the extensive volume of classified material and equipment maintained. The Liaison Officer has identified and assessed two additional sources for recruitment during the next reporting period.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 79

126

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

3. CANCER PORCH: (ACSI Approval - 28 Dec 71)

a. Location: Defense Language Institute Southwest Branch
Fort Bliss, TX

b. Confidential Source Utilization: One such source was utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Closing date of the facility remains 30 June 1973, but operations will cease on 31 May 1973.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

4. CANDID FROLIC: (OACSI Approval - 21 Dec 71)

a. Location: Fort Ord, CA

b. Confidential Source Utilization: Two sources were contacted during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The Cdr, Ft Ord, has voiced his satisfaction with the operation as part of the overall counterintelligence support rendered his Command. Four additional sources are currently under assessment for inclusion in the operation.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11...
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

128

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

5. CENTRAL TAXI: (OACSI Approval - 16 Feb 72)

a. Location: Headquarters, US Army Electronics Command, Fort Monmouth, NJ

b. Confidential Source Utilization: Three sources were contacted on a regular basis during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: Continuation of the operation is dictated by its sensitivity and criticality; the desire of the Commanding General for this support is unchanged.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by .....DCSOPS USAINTC.....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC .....1979.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

6. GONDOLA STAR (OACSI Approval - 17 Feb 72)

a. Location: Aberdeen Proving Ground, MD

b. Confidential Source Utilization: Two sources were contacted regularly during the period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The Commander desires that the operation be continued. The sensitivity of facilities at the installation justify this desire.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FD1/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

130

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

7. GONG SILK: (OACSI Approval - 16 Feb 72)

a. Location: Picatinny Arsenal, Dover, NJ

b. Confidential Source Utilization: Regular contact was maintained with three sources during the period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: This operation may be affected by forthcoming organizational changes, which will involve the move of a portion of the major command to another installation.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

Page 1629 of 3957

~~CONFIDENTIAL~~

8. LANDLESS TIME: (OACSI Approval - 19 Jan 72)

a. Location: Philadelphia Facility, US Army Electronics Command

b. Confidential Source Utilization: Three sources were contacted regularly.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The criticality of portions of this facility is considered to warrant continuation of the operation.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USATNTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

132

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

9. LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute East Coast Branch
Anacostia Naval Annex, Washington, DC

b. Confidential Source Utilization: This operation utilizes conventional sources drawn from the student population.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: With students who will be assigned to sensitive positions, this facility is an ideal location for spotting and assessing by hostile intelligence.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

10. LENIENT CLOUD (OACSI Approval - 16 Feb 72)

a. Location: US Army War College, Carlisle Barracks, PA

b. Confidential Source Utilization: Four sources were contacted on a regular basis during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The CG continues to reiterate his desire for support provided by the operation.

REGRADED UNCLASSIFIED
ON SEP - 8 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

134

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

11. LENTIL MONKEY: (OACSI Approval - 26 Oct 71)

a. Location: Defense Language Institute West Coast Branch
Presidio of Monterey, CA

b. Confidential Source Utilization: One source was lost through graduation, reducing the number to three prior to the end of the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: As with other branches of the Defense Language Institute, this facility continues to offer a lucrative target to hostile intelligence. The manning of the Soviet Embassy in San Francisco presents an additional external security threat.

DECLASSIFIED
SEP - 5 1997
OSD USARMSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

Page 1633 of 3957

~~SECRET~~

4 Oct 72

ACTION SHEET

CONTROL NUMBER

SUBJECT: Quarterly ACIP Report

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 2 February 1973

ACTION REQUIRED: To forward memorandum requesting VCSA sign memorandum to USA.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By Memorandum dated 8 February 1972, the Under Secretary of the Army requested the Vice Chief of Staff, US Army provide quarterly reports on all ACIP's (BLUE TAB B).

b. The third quarterly report for 1972 was submitted to the Under Secretary of the Army on 20 October 1972 (BLUE TAB C).

c. Written input from USAINTC for the current quarterly report is attached at BLUE TAB D.

2. DISCUSSION:

a. Word received from the SGS on 1 February 73 revealed the new VCSA desires to personally sign all memoranda to the Under Secretary of the Army. How long this new policy is to be effective is currently unknown.

b. Based on DA memoranda 340-15 and 340-17, the ACSI had signed a previous memorandum on this action for the VCSA (BLUE TAB E). This action was returned by SGS on 1 Feb 73 for compliance with new policy.

c. The memorandum at BLUE TAB A forwards a memorandum to the VCSA requesting he sign and forward to the USA the fourth quarterly ACIP report for 1972.

3. RECOMMENDATION: That the memorandum to the VCSA at BLUE TAB A be approved and signed.

(Continue on plain bond)

IMPLICATIONS — CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		
			DIR		6 Feb 73
			EX	APPROVED	
			ACSI		8 FEB 1973
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

W. WEBB, MAJ/77017 Waldo W. Webb 136

SPECIAL ACTIONS BR
RECORDS COPY

~~SECRET~~

ACSI FORM 28, 13 Sep 71

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~SECRET~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

DAMI-DOI-S

8 February 1973

MEMORANDUM FOR: VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above (TAB B).

2. Recommend your approval and signature on the memorandum at TAB A which transmits the report required by cited reference.

OLIVER B. PATTON
Brigadier General, GS
Acting ACofS for Intelligence

2 Incl
TAB A - Memo for USofA (~~CONFIDENTIAL~~)
TAB B - USofA memo, 8 Feb 72 (~~SECRET~~)

12 FEB 1973

APPROVED - VCSA

PETER B. PETERSEN
LTC, GS
Assistant Secretary of the General Staff

~~SECRET~~

137

...ED When ... from classified ...

73-338

CONFIDENTIAL

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, D.C. 20310

12 February 1973

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Aggressive Counterintelligence Program Operations

1. Reference your memorandum of 8 February 1972, subject as above.

2. The 11 Aggressive Counterintelligence Program (ACIP) operations reported to you by OACSI memorandum, dated 20 October 1972, subject as above, remain in effect. No additional ACIP operations have been approved. A quarterly report of current operations is attached.

1 Incl
as (CONFIDENTIAL)

ALEXANDER M. HAIG, JR.
General, United States Army
Vice Chief of Staff

Regraded UNCLASSIFIED
when separated from
classified inclosures

138

CONFIDENTIAL

~~CONFIDENTIAL~~

CURRENT ACIP OPERATIONS

LOCATION	ACIP NICKNAME	DATE APPROVED	NUMBER CONFIDENTIAL SOURCES
Edgewood Arsenal, Maryland	CANAL LOOP	16 February 72	5
Fort Ritchie, Maryland	CANARY EFFORT	16 February 72	3
Fort Bliss, Texas (Language School)	CANCER PORCH	28 December 71	1
Fort Ord, California	CANDID FROLIC	21 December 71	2
Fort Monmouth, New Jersey	CENTRAL TAXI	16 February 72	3
Aberdeen Proving Grounds, Maryland	GONDOLA STAR	16 February 72	2
Picatinny Arsenal, New Jersey	GONG SILK	16 February 72	3
Philadelphia, Pennsylvania (Electronics Command)	LANDLESS TIME	19 January 72	3
Washington, D.C. (Language School)	LANYARD MOOD	22 December 71	0
Carlisle Barracks, Pennsylvania (Army War College)	LENIENT CLOUD	16 February 72	4
Presidio of Monterey, California	LENTIL MONKEY	26 October 71	4
TOTALS 11	11		30

Off-post Information

There were no instances in which information on non-affiliated civilians was collected off-post.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DAMI-DO
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS
DECLASSIFIED ON 31 DECEMBER 1979

139

TAB A

~~CONFIDENTIAL~~

CONFIDENTIAL

Information Obtained:

a. During the fourth quarter 1972, useful information was obtained from seven of the eleven Aggressive Counterintelligence Programs. The operations at Ft. Ritchie, Maryland, the Electronics Command, the Army War College, Ft. Monmouth, New Jersey and Picatinny Arsenal, each identified one or more potential personnel or physical security problems which were reported to the respective serviced commanders. The program at Ft. Ord, California, continued to identify military personnel affiliated with the Vietnam Veterans Against the War (VVAW) and also military personnel associated with the proposed making of an anti-war film on the Ft. Ord reservation. This information was passed to representatives of the supported commander. A characterization of the VVAW is attached. The operation at the Presidio of California developed information on what appears to be a program of fraudulent immigration from a Communist Country. Additionally, classroom statements by an Army student identified his father as a Soviet-born key employee of another US intelligence agency. In each case, the supported commander was informed and a summary of information report was forwarded to the appropriate federal agency.

b. The other four operations reported no information, during the fourth quarter, which would indicate the existence of a hostile intelligence threat or possible security hazard. Inasmuch as these operations are a form of intensified security watchfulness, negative reports in themselves are frequently of value to a commander in planning for the security requirements of a given installation or activity. The placement and access of current sources, and those under consideration, are such that the chances of detecting a developing security threat situation in a sensitive installation or unit are greater with these sources operating.

Continuance of Operations:

The eleven ACIP operations are being continued for the original stated purposes.

1 Incl
as (CONFIDENTIAL)

Regraded UNCLASSIFIED when
separated from classified
Inclosures

140

CONFIDENTIAL

~~CONFIDENTIAL~~

VIETNAM VETERANS AGAINST THE WAR

(U)

1. (C) General: The Vietnam Veterans Against the War, Incorporated (VVAW) was founded in the spring of 1967 in New York City. The objectives of the VVAW include: the demand for an immediate cessation of fighting and withdrawal of American troops from Vietnam; and to support all military personnel refusing to serve in wars of aggression at home or abroad. The VVAW reportedly has chapters in all 50 states and Vietnam. The national office is located at 25 West 26 Street, New York, New York. VVAW policy is established by its National Steering Committee composed of 26 regional coordinators. The local chapters often act independently of the national office. (There have been indications that some local chapters of the VVAW have been taken over by youth groups of Marxist-Leninist organizations.) This is in keeping with the recent resignation of four of the five members of the Executive Committee of the National Steering Committee. During a November 1971 meeting of the Steering Committee, statements were made that conservative VVAW members would be replaced by more militant members who would take action rather than talk. Many of the VVAW officials and members are presently or have in the past been affiliated with organizations identified as being threats to Army morale and discipline, such as CPUSA, Socialist Workers Party, Progressive Labor Party, and People's Coalition for Peace and Justice. Total VVAW membership is reportedly approaching 10,000. Financial support appears to come from private donations.

(U)

2. (C) Relationship to the Army: The VVAW, reportedly, has counseled US Army deserters to go to Sweden rather than return to the US from Canada; and has provided deserters with funds and false draft registration cards. The organization has attempted to recruit active duty soldiers to the ranks of the VVAW and has urged inductees to "resist the Army and join the VVAW." VVAW local chapters have allied themselves with antimilitary dissident soldier organizations in an attempt to undermine morale and discipline of service personnel.

3. (U) Foregoing information falls under provisions of para 4a(1) and 4a(2), DA letter, AGDA-A(M)(1 Jun 71) CS, subject: Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense.

Classified by DAMI-DOA (Continued)
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS
DECLASSIFIED ON 31 DECEMBER 1978

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM
AUTH Para 1-603 DODD 5200.1R

141

~~CONFIDENTIAL~~

~~SECRET~~ 4th Qtr 72

ACTION SHEET

CONTROL NUMBER

SUBJECT: Quarterly ACIP Report

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 18 January 1973

ACTION REQUIRED: To provide Under Secretary of the Army with the fourth quarterly report for 1972.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By memorandum dated 8 February 1972, the Under Secretary of the Army requested the Vice Chief of Staff, US Army, to provide quarterly reports on all ACIP's (BLUE TAB B).

b. The third quarterly report was submitted to the Under Secretary of the Army on 20 October 1972 (BLUE TAB C).

c. Written input from USAINTC for the current quarterly report is attached at BLUE TAB D.

2. DISCUSSION: Memorandum at BLUE TAB A to Under Secretary of the Army through the Vice Chief of Staff, US Army, provides required fourth quarterly report for 1972.

3. RECOMMENDATION: That the Memorandum at BLUE TAB A be approved and signed.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		18 JAN 73
			DIV		18 JAN 73
			DIR	MK	18 Jan 73
			EX		
			ASA	APPROVED	24 Jan 73
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

W. WEBB, MAJ/77017 Webb 1/22

~~SECRET~~

SPECIAL ACTIONS BR
RECORDS COPY

REGRADED UNCLASSIFIED

Page 1640 of 3957

CONFIDENTIAL

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

REPLY TO ATTENTION OF: DAMI-DOI-S

26 JAN 73

MEMORANDUM THRU: VICE CHIEF OF STAFF, UNITED STATES ARMY

FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

1. Reference your memorandum of 8 February 1972, subject as above.

2. The 11 ACIP operations reported to you by OACSI memorandum, dated 20 October 1972, subject as above, remain in effect. No additional ACIP operations have been approved. A quarterly report of current operations is attached (TAB A).

1 Incl
as (CONFIDENTIAL)

WILLIAM E. POTTS
Major General, GS
ACofS for Intelligence

Regraded UNCLASSIFIED when separated from classified inclosures

143

CONFIDENTIAL

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE COMMAND
FORT HOLABIRD, MARYLAND 21219

15 JAN 1973

ICDISO-OC

SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

HQDA (DAMI-DOI-S)
WASH DC 20310

1. (U) References:

a. Letter, DAMI-DOI-S, 8 Mar 72, subject as above.

b. Letter, ICDISO-OC, 18 Apr 72, subject as above.

c. Letter, ICDISO-OC, 11 Oct 72, subject as above.

2. (U) In compliance with reference a, above, the ACIP quarterly report for the period 1 October - 31 December 1972 is forwarded herewith.

3. (U) Operational and administrative control measures outlined in reference c, above, remained in effect during the reporting period. There were no instances of acquisition of information on non-DoD affiliated personnel.

4. (C) Based on the immediate concern for the security of chemical and nuclear weapons, this Command is preparing plans in conjunction with US Army Materiel Command and HQ, US Army Air Defense Command to provide counter-intelligence support to these units and their sub-elements. In view of recent terrorist group actions, it is apparent that such groups will go to any extreme to achieve their ends. As some terrorist representatives have pointed out, they feel that such actions must have increasing world shock value in order to further their cause. The capture or explosive destruction of a nuclear weapon either in storage or in transit would be just such an act. Indications of intention may be developed through the ACIP. Planning for this kind of support in conjunction with other means available to USAINTC is being effected. It is expected that by the end of the next reporting quarter, more definitive information concerning initiation of ACIP in support of these two Commands will be established.

Classified by DISO, USAINTC
SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS. DECLASSIFIED ON 31 DEC 1979

DECLASSIFIED
SEP -5 1997
BY CDR USAINSCOM FT HPO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

[redacted]

ICDISO-OC
SUBJECT: Quarterly Reporting of Aggressive Counterintelligence Program (ACIP) Operations (U)

5. (C) With a view towards the probable requirement of expanding ACIP operational capability by USAINTC field elements, this Command has initiated a training program designed to improve the professionalism of personnel in the operational techniques and reporting in such operations. This training program should qualify additional personnel to participate in current and potential future operations.

FOR THE COMMANDER:

RAY W. CHAMBERS
LTC, MI
Acting Assistant Adjutant General

11 Incl
as

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY ODR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

2 145

[redacted]

[redacted]

1. CANAL LOOP: (OACSI Approval - 16 Feb 72)

a. Location: Edgewood Arsenal, Edgewood, MD

b. Confidential Source Utilization: Five sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: During the reporting period, experienced personnel were assigned in both liaison and source handling capacity, and the operational capabilities can be expected to improve. The Commanding Officer of Edgewood Arsenal has again expressed his desire for continuation of ACIP operations within his installation.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PA
AUTH Para 1-603 DOD 5200.1R

Classified by .....DISO USAINTC.....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC ....1979....

146

[redacted]

[redacted]

2. CANARY EFFORT: (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Information reflecting on the character and suitability of certain employees in the target areas was obtained.

e. Operational Status: During the period, both Case Officer and Liaison Officer were assigned to DIS. The transfer of the former diminished source contact appreciably. With the assignment of a case officer, information obtained during the period will be developed to its fullest extent. An experienced liaison officer is being assigned to this ACIP and will begin spotting and assessing potential sources to meet the desire of the Commanding Officer to achieve the greatest operational potential.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

[redacted]

Page 1645 of 3957

3. CANCER PORCH: ([redacted]SI Approval - 28 Dec 71)

a. Location: Defense Language Institute Southwest Branch, Fort Bliss, TX

b. Confidential Source Utilization: One such source was recruited during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: As indicated in previous reports, this facility is expected to cease operations on 30 June 1973. The prime reason for developing this single confidential source is his expected transfer at that time to another branch of the Institute.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

[redacted]

Page 1646 of 3957

4. CANDID FROLIC: (OACSI Approval - 21 Dec 71)

a. Location: Fort Ord, CA

b. Confidential Source Utilization: Regularly scheduled contacts were conducted with two such sources during the period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Identification of military personnel affiliated with the Vietnam Veterans Against the War; identification of military personnel associated with the proposed filming of an anti-war film on the Fort Ord reservation.

e. Operational Status: As the major US Army training facility on the West Coast, the installation continues to be the target for dissident elements.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

Page 1647 of 3957

CONF

5. CENTRAL TAXI: (OACSI Approval - 16 Feb 72)

a. Location: Headquarters, US Army Electronics Command, Fort Monmouth, NJ

b. Confidential Source Utilization: Three sources were contacted on a regular basis during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affilated Civilians: None

d. Useful Information Obtained Information indicating a potential security problem area was developed and passed to the serviced command.

e. Operational Status: Personnel turbulence during the period caused by transfers of operational personnel to DIS prevented the proper development of this ACIP. An experienced liaison officer was assigned during the period. This should result in the recruitment of additional sources needed to cover this complex target. The Commanding General has reiterated his desire to continue the operation.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

150

CONFIDENTIAL

[redacted]

6. GONDOLA STAR: (OACSI Approval - 17 Feb 72)

a. Location: Aberdeen Proving Ground, MD

b. Confidential Source Utilization: Two sources were contacted regularly during the period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The newly assigned liaison officer has begun the spotting and assessment process, which should result in expansion of coverage to the degree desired.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISO DSAI NTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF [redacted]
AUTOMATICALLY [redacted] TWO YEAR
INTERVALS [redacted] 31 DEC 1979

[redacted]

[redacted]

7. GONG SILK: (OACSI Approval - 16 Feb 72)

a. Location: Picatinny Arsenal, Dover, NJ

b. Confidential Source Utilization: Regular contact was maintained with three sources during the period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Two potential problem areas in the field of security were identified and reported to the serviced commander.

e. Operational Status: The commanders of the two serviced facilities have expressed their desires that the ACIP be continued and expanded. Efforts to establish sources in each target area have been hampered to date by the lack of experienced MI personnel.

DECLASSIFIED UNCLASSIFIED
SEP 5 1997
FOIA CASE # 1-03 DOD 5200.1R

Classified by ...DISO USAINTC.....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

152

[redacted]

CONFIDENTIAL

8. LANDLESS TIME: (OACSI Approval - 19 Jan 72)

a. Location: Philadelphia Facility, US Army Electronics Command

b. Confidential Source Utilization: One source was terminated due to lack of access; regular contact was maintained with the remaining three.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Identification of personnel with access to classified information who have character weaknesses or habits reflecting on suitability. This information has been brought to the attention of the supported commander.

e. Operational Status: Individual personnel activities are being closely monitored to determine any adverse effects on the morale and discipline of the work force. The supported commander desires that this ACIP be expanded to cover more areas in depth.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

CONFIDENTIAL

CONFIDENTIAL

9. LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute East Coast Branch
Anacostia Naval Annex, Washington, DC

b. Confidential Source Utilization: Conventional, rather than confidential sources, have been utilized to date in this ACIP.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: No information to indicate the existence of a hostile threat to the installation or a possible security hazard was developed during the reporting period.

e. Operational Status: The installation continues to offer a lucrative target to hostile intelligence, with students, ranging in rank from private to general, who undergo instructions for periods up to a year.

DOWNGRADED UNCLASSIFIED
ON SEP 5 1997
BY OSD/DOE, DAM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISCUSAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1977

CONFIDENTIAL

Page 1652 of 3957

~~CONFIDENTIAL~~

10. LENIENT CLOUD: (OACSI Approval - 16 Feb 72)

a. Location: US Army War College, Carlisle Barracks, PA

b. Confidential Source Utilization: Four sources were contacted on a regular basis during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Identification of four individuals possessing possible adverse suitability traits.

e. Operational Status: Attempts to develop additional information on the four individuals mentioned above is continuing and upon completion, this information will be furnished to the supported commander.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY ODR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

Classified by DISO USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

~~CONFIDENTIAL~~

[redacted]

11. LENTIL MONKEY: (OACSI Approval - 26 Oct 71)

a. Location: Defense Language Institute West Coast Branch, Presidio of Monterey, CA

b. Confidential Source Utilization: Contact was maintained with four sources during the reporting period. This represents an increase of one source.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Information was developed on what allegedly is a program of fradulent immigration from a Communist country. Additionally, classroom statements by an Army student identified his father as a Soviet-born key employee of another intelligence agency. In each case, A Summary of Information was prepared for transmission to the appropriate agency.

e. Operational Status: There is currently a source in each of four sensitive language departments. Sources have been alert for classroom discussion which would identify personnel who are in communication with relatives in countries considered hostile to the US. Additional sources are to be developed in the larger departments, which will allow more adequate monitoring for possible indicators of hostile intelligence influence.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DISC USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS DECLASSIFIED ON 31 DEC 1979

[redacted]

Page 1654 of 3957

THIS MUST REMAIN T O P D O C U M E N T

DOSSIER NO. ZF011946W
Vol 3 of 7 Vols

As of 18 Sep 85 (Date) all material included in this file conforms with DA policies currently in effect.

Delmar Smith (Signature) 18 Sep 85 (Date Signed)

Delmar Smith (Printed Name) GS5 (Grade)

Reviewed for Retention
Criteria UP AR 381-10
Reviewer [illegible] Date 4 Jan 93

THIS MUST REMAIN T O P D O C U M E N T

IA (HQ) Form 2214
(1 Sep 78)

Replaces MIIA Fm 315, 1 Jun 75, which may be used until supplies are exhausted.

157

[redacted] ICIP 1974 [redacted]

158

[redacted]

ICIP QUARTERLY REPORTS

INDEX

TAB A	21 Apr 72	Memo to USecArmy w/ 1st qtr rpt
TAB B	1 Aug 72	2nd qtr rpt, CY 72
TAB C	20 Oct 72	3rd qtr rpt, CY 72
TAB D	12 Feb 73	4th qtr rpt, CY 72
TAB E	23 Apr 73	1st qtr rpt, CY 73
TAB F	19 Jul 73	2nd qtr rpt, CY 73
TAB G	29 Oct 73	3rd qtr rpt, CY 73
TAB H	1 Feb 74	4th qtr rpt, CY 73
TAB I	19 Apr 74	1st qtr rpt, CY 74
TAB J	13 Aug 74	2nd qtr rpt, CY 74
TAB K	27 Sep 74	MFR, ICIP Brief for USecArmy
TAB L	29 Nov 74	3rd qtr rpt, CY 74
TAB M	4 Feb 75	Memo for USofA (response) to include 4th qtr rpt, CY 74

Page 1657 of 3957

~~SECRET~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

DAMI-ZA

04 FEB 1975

MEMORANDUM THRU: VICE CHIEF OF STAFF, UNITED STATES ARMY

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

1. (U) This is in response to your Memorandum on 17 January 1975 to the Vice Chief of Staff in regard to subject and serves as the Quarterly ICIP Report for the 2d Quarter, FY 2975.

2. (U) On 2 October 1974, I directed a review of the entire ICIP program with a view towards the elimination of those no longer considered of sufficient merit to warrant retention. The criteria used in evaluating each ICIP operation was: (a) The sensitivity of the installation/activity is such that some type of special counterintelligence support is required or (b) There is a known threat of sufficient magnitude to the installation/activity to warrant a need for some type of special counterintelligence support and (c) The information desired cannot be obtained except through the use of confidential sources.

3. (U) Based on this review and considering your 17 January guidance, I directed the termination of 12 ICIP operations at the following headquarters:

a. Hq, US Army Communications Command, Fort Huachuca, Arizona (CANAL ROPE).

b. Dugway Proving Ground, Utah (CANARY STONE).

c. US Army Air Defense Center, Fort Bliss, Texas (CANTINA ARCH).

d. Umatilla Army Depot Activity, Hermiston, Oregon (CANYON ROSTER).

e. US Army Mobility Equipment Research and Development Center, Fort Belvoir, Virginia (CENTAUR SALE).

Regraded CONFIDENTIAL when Separated from CLASSIFIED Inclosures

160

Classified by DAMI-ZA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2005

~~SECRET~~

SECRET

DAMI-ZA 04 FEB 1975

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

f. Hq, US Army Electronics Command, Fort Monmouth, New Jersey (CENTRAL TAXI).

g. US Army Management Systems Support Agency, The Pentagon, Washington, DC (CENTURY SQUAD).

h. US Army Electronics Proving Ground, Fort Huachuca, Arizona (GONDOLA FLAG).

i. Aberdeen Proving Ground, Aberdeen, Maryland (GONDOLA STAR).

j. Defense Language Institute East Coast, Washington Navy Yard, Washington, DC (LANYARD MOOD).

k. Picatinny Arsenal, Armament Command, Dover, New Jersey (LEND TONE).

l. US Army War College, Carlisle Barracks, Pennsylvania (LENIENT CLOUD).

4. (U) The remaining seven ICIPs are worthy of retention as they meet your criteria. Reviews of these seven operations are attached at Incl 1. Reviews of the 12 to be terminated are at Incl 2.

2 Incls
as

HAROLD R.
Major Gene
ACofS for I

Vol 4 of 7 Without correct Pg #

REGRADED UNCLASS
ON 5 SEP 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

161

SECRET

~~SECRET~~

ICIP operations recommended for continuation (7)

CANARY EFFORT

CANINE PLATE

CANVAS TAX

CENSUS TIME

CENTAVO KID

LENS HOLDER

LENTIL MONKEY

Regraded UNCLASSIFIED when separated from classified inclosures.

162

~~SECRET~~

Incl 1

~~SECRET~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOI-C

SUSPENSE:

DATE: 31 January 1975

ACTION REQUIRED: To respond to tasking from the USofA pertaining to ICIP.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. At the direction of the USofA quarterly reporting of ICIP has been furnished to him through the VCSA since February 1972. In a memorandum to the VCSA (RED TAB B), the VSofA suggests that in more than half of the ongoing operations, no useful information was developed. He directed a detailed review of the benefits derived through the program over the last two years.

b. On 29 January 1975, the ACSI directed the termination of 12 of the 19 ongoing operations. They will be terminated on a time phase basis with all 12 being terminated by 31 March 1975.

2. DISCUSSION: At RED TAB A is a memo through the VCSA to the USofA replying to the comments of USofA and providing the requested information pertaining to the program.

3. RECOMMENDATION: That the memo at RED TAB A be approved and signed.

(Continue on plain bond)

IMPLICATIONS — CINFO: YES ☐ NO ☐ | PRIM PROGS: YES ☐ NO ☐ | BUDGET: YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		3 Feb 75
			DIV		3 Feb 75
			DIR/DEP		3 Feb 75
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

MAJ EBERSOLE/56074/th

Record Copy

ACSI FORM 28, 13 Sep 71

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED

~~SECRET~~

~~SECRET~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

MIIA-ZA

MEMORANDUM FOR: MG AARON, ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE, DA

SUBJECT: Status of Internal Counterintelligence Program (ICIP) Operations

1. (U) References:

a. ACSI Memo, 7 Jan 75, subject: ICIP.

b. Under Secretary of the Army Memorandum, 17 Jan 75, subject: ICIP.

c. Letter, DAMI-DOI-S, 8 Mar 72, subject: Quarterly Reporting of ICIP Operations (U).

2. (U) In compliance with your oral instructions of 2 October 1974; your Memorandum of 7 January 1975; and guidance contained in the Memorandum of 17 January 1975 from the Under Secretary of the Army, we have completed a comprehensive review of the current active 19 ICIP operations.

3. (C) Our review was basically governed by the following factors: (1) The sensitivity of the installation/activity is such that some type of special counterintelligence support is required or (2) there is a known threat of sufficient magnitude to the installation/activity to warrant some type of special counterintelligence support and (3) the information desired cannot be obtained except through the use of Confidential Sources.

4. (C) Using the above criteria and your decision of 29 January, 12 of the 19 on-going operations are to be terminated. We believe that we can provide adequate support to the installations/activities concerned through a program of intensified liaison by the appropriate local USAINTA representative. The operations to be terminated are listed in an attached proposed Memorandum to the Under Secretary of the Army. These operations should be terminated on a time phased basis with all 12 to be terminated no later than 31 March 1975.

[redacted]
SECRET

164

Classified by AR 380-47 (ACSI-DA)
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2005

~~SECRET~~

~~SECRET~~

MIIA-ZA
SUBJECT: Status of Internal Counterintelligence Program (ICIP) Operations

Phasing will permit adequate liaison to be established by RO and FO in lieu of the operations and permit no degradation of necessary good will.

5. (U) The remaining seven operations to be retained are reviewed individually in our draft reply for Mr. Staudt.

William S. Wolf

WILLIAM S. WOLF
Colonel, MI
Commanding

1 Incl
Proposed draft
Memorandum

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FO1/PO
AUTH Para 1-603 DOD 5200.1R

~~SECRET~~

Page 1663 of 3957

CONFIDENTIAL

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

(U) ~~(C)~~ CANARY EFFORT:

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three confidential sources are currently being utilized.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Sensitive Character of the Mission that Necessitates an ICIP Operation: The mission of the elements within Fort Ritchie, which include the Telecommunications Directorate (TD), Alternate Joint Communications Center (AJCC), Site R, and Divisions organic to TD is critical sensitive. The Telecommunications Directorate provides the operation, maintenance, engineering, and installation of communication-electronic activities, facilities, systems, and networks comprising the AJCC serving the Alternate National Military Command Center (ANMCC) and other agencies as directed. This activity also provides direction and supervision to the operations division, the maintenance division and the communications services divisions which are included in the target list for the project. Because of the nature of the target areas and of the work force, a confidential source program is essential to provide adequate CI coverage to the project.

e. Benefits and Information Obtained Over the Last Two Years: Although the operation was initiated in 1958, the program was terminated in 1971 and was not revalidated until February 1972. Sources within the target area report information concerning both US Army personnel and Department of the Army civilian personnel assigned to Fort Ritchie and AJCC. The following are examples of information obtained:

(1) Suitability information concerning an Army NCO, specifically, indebtedness. The NCO was responsible for the issuance of passes, both temporary and permanent, to the AJCC. The surfacing of the indebtedness resulted in the reassignment of the individual to a less sensitive billet and further investigation was requested.

(2) A report personality change manifested by alcohol abuse concerning an Army NCO assigned to sensitive duties at the TD, AJCC, resulted in the monitoring of the NCO's activities to determine if an investigation is warranted.

(3) Suitability information, specifically, alleged drug abuse and irrational behavior, was provided on a DAC employed within the Office of the Comptroller. The report resulted in a request for a Suitability Investigation to be conducted by USAINTA.

(4) Adverse suitablity information, specifically, financial problems and irrational behavior was developed pertaining to an Army NCO assigned sensitive duties within the Record Communication Branch, TD. This resulted in a request for a Suitablity Investigation from USAINTA.

CONFIDENTIAL

~~CONFIDENTIAL~~

CANARY EFFORT:

(5) Adverse suitability information, specifically, promiscuity with officers and enlisted personnel at Fort Ritchie, pertaining to a female DAC employee of the ADP Service Division resulted in the monitoring of her activities by local authorities.

(6) Adverse suitability information, specifically, an abnormal interest in firearms, explosives and poisions, coupled with irrational behavior, was surfaced concerning an enlisted man assigned to the USACEEIA-CONUS, Automated Support Group. The result was the suspension of the individual's access to classified defense information pending a psychiatric evaluation of the individual.

(7) During the period 1 January 1974 through 31 December 1974 a total of 94 Agent Reports were submitted concerning 44 individuals assigned to Fort Ritchie occupying either sensitive positions and/or having security clearances. The Agent Reports forwarded adverse suitability information. It is estimated that approximately 50% of the useful information obtained through this operation would not have been available on a timely basis without the use of confidential sources.

f. Based on the above, and the fact that the type of activities conducted at Fort Ritchie are known to be of interest to hostile intelligence services, this operation has been selected for retention at this time.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1665 of 3957

~~CONFIDENTIAL~~

(U)~~(C)~~ CANINE PLATE:

a. Location: Seneca Army Depot, Romulus, NY

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Sensitive Character of the Mission that Necessitates an ICIP Operation: The mission of the Seneca Army Depot (SAD) is the operation of a supply depot for the receipt, storage, issue, maintenance, and disposal of missile and artillery weapons systems with a nuclear capability. Included in the items handled are ammunition, propellants, explosive components of guided missiles, special weapons materials, supplies, industrial production equipment (to include special tools), petroleum and chemical supplies, fire control test and measuring equipment, and other special weapons with a nuclear capability. SAD is also responsible for systems modification for AEC/DOD test firings. The Directorate for Special Weapons, which includes the Production Planning and Control Division, Supply Division, and Maintenance Division includes the most sensitive and critical areas of Seneca Army Depot, and is the Priority I target for the operation. Because of the sensitivity and criticality of the activities at this installation, a confidential source program is essential to provide adequate CI coverage to the depot and its activities.

e. Benefits and Information Obtained: This operation was administratively implemented in November 1973, but has not yet become operationally effective. The successful development of a viable source program has been hampered by personnel turbulence within the Army's Intelligence Agency, the remoteness of the target area, and the composition of the work force. The lack of significant information is viewed as a direct result of the absence of a firmly established confidential source program and reinforces the need to employ all possible means to deter and detect the efforts of hostile intelligence services to penetrate the activity or approach some of its key personnel. It is a known fact that hostile intelligence services have high priority collection objectives directed against activities such as those conducted at Seneca Army Depot. This is a matter of grave concern to the security of the Army, which is reinforced by the growing threat of nuclear theft and blackmail from terrorist groups.

f. Based on the above, it is considered absolutely necessary to maintain a counterintelligence "early warning" device such as the ICIP as an adjunct to the normal internal security program; therefore, this operation has been selected for retention at this time.

~~CONFIDENTIAL~~ 168

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

CONFIDENTIAL

(U) CANVAS TAX:

a. Location: Sierra Army Depot (SAD), Herlong, CA

b. Confidential Source Utilization: None

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Sensitive Character of the Mission that Necessitates an ICIP Operation: The mission of the Sierra Army Depot (SAD) is the operation of a supply depot for the receipt, storage, issue, maintenance, and disposal of missile and artillery weapons with a nuclear capability. Included in the items handled are ammunition, propellants, explosive components of guided missiles, special weapons materials, supplies, industrial production equipment, petroleum and chemical supplies, fire control test and measuring equipment, and other special weapons with a nuclear capability. SAD is also responsible for maintaining a capability for systems modification in support of the joint AEC/DOD test firing programs. Priority I targets are Exclusion Area One, Exclusion Area Two, and the Maintenance Area for Special Weapons. Because of the nature of the activities, the isolated location of the target areas and the composition of the work force, a confidential source program is essential to provide adequate CI coverage to the depot and its activities.

e. Benefits and Information Obtained: This operation was administratively implemented in April 1974, but has not yet become operationally effective. In the nine months of its existence, the successful development of a viable source program has been hampered by personnel turbulence within the Army's Intelligence Agency. Although the operation has surfaced no significant information to date, this is considered directly attributable to the lack of a firmly established confidential source program and does not rule out the need to employ all available means designed to deter and detect the efforts of hostile intelligence services to penetrate the activity or approach some of its key personnel. It is a known fact that hostile intelligence services have high priority collection objectives pertaining to activities such as those conducted at Sierra Army Depot. When this matter of grave concern to the security of the Army is coupled with the growing threat of nuclear theft and blackmail from terrorist groups, it is considered absolutely necessary to maintain a counterintelligence "early warning" device such as the ICIP as an adjunct to the normal internal security program.

f. Based on the above, this operation has been selected for retention at this time.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

169

CONFIDENTIAL

~~CONFIDENTIAL~~

(U) CENSUS TIME:

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC

b. Confidential Source Utilization: One source was used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Sensitive Character of the Mission that Necessitates an ICIP Operation: The mission of the elements of the Pentagon Telecommunication Center, which include the Operations Division, the Army Operations Center Division, Facilities Division, Supply Division, and Administrative Division is critical sensitive. The Operations Division provides electrical record communications cryptographic services for Department of the Army and communications support to the Department of Defense, Joint Chiefs of Staff, National Military Command Center, Department of State, White House, other government agencies in the Washington area, embassies of allied nations and NATO. Additionally, the Pentagon Telecommunications Center operates the Forrestal Building Telecommunications Center, the Hoffman Building Telecommunications Center, and telephone and teletype service, including secure means, in the Army Operations Center. Because of the nature of the target areas and the work force, a confidential source program is essential to provide adequate CI coverage to the project.

e. Benefits and Information Obtained: Although the operation was administratively activated in February 1974, it did not become operational until October 1974. The one source used in the operation is a recent recruitment and project control personnel have devoted their time to training and developing the source. This operation has produced no significant counterintelligence threat information to date because of the factors indicated. Based upon information available through other sources, it is known that the hostile intelligence services are extremely interested in computerized communications systems and on the type of communications and activities conducted by PTC. The lack of positive information acquired to date does not rule out the threat of hostile intelligence service efforts to penetrate the activity, and is viewed as an indication that confidential source program is essential to provide adequate CI coverage to the activity.

f. Based on the above, this operation has been selected for retention at this time.

170

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

(U) CENTAVO KID:

a. Location: Harry Diamond Laboratories (HDL), Washington, DC.

b. Confidential Source Utilization: Seven confidential sources are currently being utilized.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Sensitive Character of the Mission that Necessitates an ICIP Operation: The mission of the HDL includes critical sensitive research and development activities accomplished in support of the US Army. The most sensitive elements are the Branch Laboratory 240 which conducts research into the hardening of communications equipment against nuclear weapons radiation; Branch Laboratory 290 which conducts tests of nuclear warhead and missile systems to determine their ability to withstand nuclear weapons radiation; Branch Laboratory 510 and 640 which conduct joint research to develop countermeasures against various foreign weapons systems; Branch Laboratory 750 which manages the development and production of all fuzes produced by HDL; Branch Laboratories 610 and 620 which develop fuzes for use with nuclear warheads and Branch Laboratory 1000 which conducts development and testing of radiation hardened systems for Minutemen and Poseidon Missiles. Because of the sensitive research and development mission of HDL, and the dispersed location of the activities, a confidential source program is essential to provide adequate CI coverage to the activity.

e. Benefits and Information Obtained over the Last Two Years: Although the operation was administratively initiated in March 1973, it did not become operational until October 1974. The sources within the target area provide coverage on five of the above listed six target areas. The following examples illustrate the type of information obtained:

(1) The identification of a "loosetalk" problem at HDL's Woodbridge facility.

(2) Adverse suitability information, specifically, extra marital affairs and other related marital problems, coupled with an assault incident was surfaced which contributed to an on-going security investigation concerning a DAC at HDL.

(3) A security weakness was identified at the Woodbridge facility as various persons were entering the facility to hunt deer without any clearances or security checks of any kind.

(4) It is estimated that approximately 60% of the useful information obtained through this operation during the past three months would not have been available on a timely basis without the use of confidential sources.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1669 of 3957

CONFIDENTIAL

CENTAVO KID

f. Based on the above and the fact that the hostile intelligence services have a current high priority interest in the research and development activities of the type conducted at HDL, this operation has been selected for retention at this time.

REGRADED UNCLASSIFIED
ON
BY OSEP/CIA 5 (1997) FOI/PO
AUTH Para 1-603 DOD 5200.1R

CONFIDENTIAL

~~CONFIDENTIAL~~

(U)(C) LENS HOLDER:

a. Location: White Sands Missile Range (WSMR), NM

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Sensitive Character of the Mission that Necessitates an ICIP Operation: The mission of the White Sands Missile Range (WSMR) is to evaluate the Safeguard Missile System, missile vulnerability studies, and missile control systems, and perform pre-production tests and analyses of missile systems. Priority I targets of elements located at WSMR are the Missile Electronic Warfare Technical Area, National Range Operations Directorate, US Army Missile Test and Evaluation Directorate, and the US Army Safeguard Systems Evaluation Agency. These elements develop electronic countermeasure techniques to nullify vulnerabilities discovered in missile systems, conduct pre-production tests of rocket and guided missile systems, operate a nuclear effects facility, and operate National Range facilities for tests conducted at WSMR.

e. Benefits and Information Obtained: This operation was initiated administratively in August 1974. Not yet operational, this ICIP has no source assets and has produced no significant counterintelligence information to date. However, the nature of the activities and the work force at WSMR make it necessary that a confidential source program be developed to provide adequate CI coverage. The remoteness of the installation and the knowledge that the type of activities conducted there are current targets of hostile intelligence services make it necessary to provide the type of "early warning" protection offered by the ICIP.

f. Based on the above, this operation has been selected for retention at this time.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1671 of 3957

SECRET

(S) LENTIL MONKEY:

a. (U) Location: Defense Language Institute (DLI), Presidio of Monterey, CA

b. (C) Confidential Source Utilization: Four confidential sources were utilized during the period.

c. (U) Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. (U) Sensitive Character of the Mission that Necessitates an ICIP Operation: The mission of DLI is to train DOD intelligence and communications security specialists in every major foreign language. Military attaches and employees of CIA, FBI, and other federal agencies are also trained at DLI, making it an extremely enticing target for hostile intelligence service operatives. The majority of the faculty of DLI have foreign backgrounds and many possibly have had contact with foreign intelligence agencies in their native countries. Many of the instructors who are subject to hostage factors, and may or may not have had previous contact with a hostile intelligence service, frequently travel to their native countries in Eastern Europe. Because of the unique nature of this activity and the sensitivity of the intelligence personnel who are students there, a confidential source program is essential to provide adequate CI coverage to the project.

e. (S) Benefits and Information Obtained over the Last Two Years: Although initiated in 1968, the operation was dormant for most of 1971. Revalidated in October 1971, this operation and the sources employed have produced voluminous information and leads indicative of hostile intelligence modus operandi aimed at contact with students or faculty. The following are examples of information obtained:

(1) b1

(2) Another indicator is the frequent attempt made by foreign-born instructors to induce "pen-pal" contact between DLI students and persons living in Soviet-bloc countries. This is a known spotting technique of hostile intelligence services.

(3) Numerous reports have been surfaced of adverse suitability information involving drug abuse or immoral conduct on the part of students which have triggered investigations to determine their suitability for sensitive assignments.

SECRET

Page 1672 of 3957

~~SECRET~~

(U)

~~(S)~~ LENTIL MONKEY

(4) An incident in which two Soviet citizens visited DLI and moved about unescorted caused new visitor control regulations to be published and put into effect.

(5) Students from DLI on field trips sponsored by the Arabic Language Department were exposed to anti-US propaganda at the Arabic Trade Mission in San Francisco.

(6) Sources reported several instances on questionable activities and curricula in the Arabic Language Department which involved the use of politically contentious materials in classroom drills.

(7) An ICIP source reported information which alerted another agency to a possible breach in the security of its intelligence operations and possibly helped avoid some embarrassment in relations with the Middle East.

(8) It is estimated that approximately 70% of the useful information obtained in this operation would not have been available on a timely basis without the use of confidential sources.

f. (U) Based on the above, and due to the unique mission of DLI, this operation has been selected for retention at this time.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

~~SECRET~~

Page 1673 of 3957

~~CONFIDENTIAL~~

ICIP Operations Recommended for Termination (12)

CANAL ROPE
CANARY STONE
CANTINA ARCH
CANYON ROSTER
CENTAUR SALE
CENTRAL TAXI
CENTURY SQUAD
GONDOLA FLAG
GONDOLA STAR
LANYARD MOOD
LEND TONE
LENIENT CLOUD

Regraded UNCLASSIFIED when separated from classified inclosures.

176

Encl 2

~~CONFIDENTIAL~~

[redacted]

(W)(C) CANAL ROPE: (OACSI Approval - 17 Dec 73)

a. Location: Headquarters, US Army Communications Command (USACC), and 11th Signal Group, Fort Huachuca, AZ.

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Initial assessment information on two prospective sources.

e. Operational Status: The two sources previously recruited in this operation were terminated during the last reporting period. Although two prospective sources have been spotted, they are still undergoing assessment and have not been recruited. One prospective source is in the 11th Signal Group and the other is in the Headquarters, USACC. Information was reported on an NCO assigned to the Communications Electronics Engineering Installation Agency (CEEIA), USACC, alleging possible foreign business interests. USACC has initiated a limited investigation on the NCO to clarify the allegation. On 17 Dec 74 the PLO presented the Quarterly Briefing to CPT Richard Milligan, Assistant Director of Security, USACC, who indicated that the supported commands were satisfied with the progress of the ICIP.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

[redacted]

~~CONFIDENTIAL~~

(U) CANARY STONE: (OACSI Approval - 18 Jul 73)

a. Location: Dugway Proving Ground, (DPG), UT

b. Confidential Source Utilization: Two confidential sources were utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Assessment information obtained on two potential confidential sources.

e. Operational Status: On 21 November 1974, COL Adalbert E. Toepel Jr., Commander, DPG, was presented the Quarterly Briefing by the PLO. MAJ Trevor E. Bissey, Commander, San Francisco Field Office, 525th MI Group, and Mr. Clinton E. Bair, Intelligence Officer, DPG, also attended the briefing. No immediate threat to DPG was surfaced during the reporting period. A possible item of long term interest was reported involving foreign correspondence and/or contacts by DPG scientific personnel. COL Toepel expressed satisfaction at the progress of CANARY STONE and was appreciative of MI support rendered to DPG, particularly the conduct of security guard training preparatory to a AMC inspection in January 1975. Source spotting, recruitment, and assessment has been hampered by an impending reduction of civilian employees and a proposed reorganization of DPG directorates which will likely result in shifts of personnel. A reduction in force is scheduled for January 1975 and approximately 160 civilian employees, primarily research and scientific staff, will be discharged or reassigned to other duties.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED ON SEP 5 1997 BY CDR USAINSCOM FOI/PO AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1676 of 3957

~~CONFIDENTIAL~~

(U) CANTINA ARCH: (OACSI Approval - 12 Dec 74)

a. Location: US Army Air Defense Center, Fort Bliss (USAADCENFB), Ft Bliss, TX

b. Confidential Source Utilization: Four confidential sources were utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Suitability information was reported on one DAC employee of the Directorate of Combat Developments who reportedly has a drinking problem. The unidentified individual reported previously as selling used clothing in Mexico and suspected of bribing Mexican border officials has been tentatively identified as an NCO assigned to the Air Defense School. A limited investigation is to be conducted on the NCO to determine the legality and extent of his activities.

e. Operational Status: One of the four confidential sources used in the operation was terminated when he was reassigned from Fort Bliss. The PCO for the operation retired at the end of November 1974. Recruitment of additional sources has been hampered somewhat by personnel turbulence at the installation, but this situation is expected to stabilize in early 1975. On 16 December 1974, LTC Robert Davenport, Director of Security, USAADCENFT, Ft Bliss, was given the Quarterly Briefing on CANTINA ARCH. LTC Davenport stated that he was pleased with the progress of the ICIP and stated that he was requesting limited investigations on Ft Bliss personnel on whom information had been recently surfaced.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1677 of 3957

~~CONFIDENTIAL~~

CANYON ROSTER: (OACSI Approval - 8 Mar 74)

a. Location: Umatilla Army Depot Activity (UMDA), Hermiston, Oregon

b. Confidential Source Utilization: Two confidential sources were utilized during this period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Some investigative data was obtained on prospective sources.

e. Operational Status: One confidential source was terminated during the period and two confidential sources were recruited during the period. Firm liaison and operational rapport has been established with federal and local law enforcement agencies in the area. Five prospective sources are presently under initial assessment. Of the five, three are in the guard force of the Security Branch. On 23 December 1974, the PLO presented the Quarterly Progress Briefing to LTC Daniel W. Doty, Commander, Umatilla Depot Activity. The briefing consisted of a review of MI activities, performed in support of the installation's security program and the status of the ICIP. LTC Doty indicated that he was generally well satisfied with the program and the support rendered.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1678 of 3957

~~CONFIDENTIAL~~

(U) ~~(a)~~ CENTAUR SALE: (OACSI Approval - 14 Dec 73)

a. Location: US Army Mobility Equipment Research and Development Center (USAMERDC), Fort Belvoir, VA

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Travel plans were learned for one USAMERDC civilian employee who will travel to the USSR in the Spring of 1975. A reported SAEDA attempt involving an officer of the Camouflage Division, USAMERDC in Oct 74 has led to an internal security measure in which the PLO will give informal SAEDA lectures to management personnel of USAMERDC in an effort to improve the security posture. The PLO will in the future accompany USAMERDC security inspection teams as they make weekly inspections of USAMERDC activities. This will not only increase the visibility of the PLO at USAMERDC, but will alsc enable the PLO to spot and assess additional personnel in the more sensitive areas of USAMERDC for possible use in the ICIP.

e. Operational Status: The series of informal SAEDA lectures and the accompanyment of the security inspection teams described above have been coordinated with the supported command and the security officer to start in January 1975. On 10 December 1974, the PLO presented the Quarterly Progress Briefing to Mr. Leslie L. Askew, USAMERDC Security Officer. From the period 5 September through 5 November 1974, the PLO was on special duty with the OACSI, DA, and was unable to participate actively in the ICIP.

f. Recommendation: Based upon results achieved to date we feel we can continue to provide the support necessary without the use of confidential sources. Based on the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1679 of 3957

~~CONFIDENTIAL~~

(U) CENTRAL TAXI: (OACSI Approval - 16 Feb 72)

a. Location: Headquarters, US Army Electronics Command (ECOM), Fort Monmouth, New Jersey

b. Confidential Source Utilization: Five confidential sources were utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: On 23 October 1974, a bomb threat was received which caused evacuation of the new ECOM office building. During the evacuation some classified material was left unsecured and unattended. The ECOM Security Office is insuring that classified material is secured during future evacuations and that fire marshals and bomb squads remain on all floors during an evacuation. A source also reported that an unsecured fire exit door in the east wing of the new ECOM office building allowed free access to a fire tower and all floors above. The Security Officer was notified who in turn notified the Provost Marshal's Office (PMO) who will insure that the door is secured in the future. A discharged enlisted man used his expired building pass to enter the Hexagon Building, Ft Monmouth, in early Dec 74. The information was passed to the Security Office who coordinated with the PMO to correct such deficiencies during the out-processing of reassigned/separated personnel. A source reported an increase in use of narcotics among military personnel employed at ECOM. The information was provided to CID which assumed investigative responsibility. An ECOM civilian employee received a telephonic threat against his life during the week of 24 Oct 74. The PLO provided the information to the local CID which initiated an investigation.

e. Operational Status: Thirteen conventional sources are used to provide coverage of the ECOM target areas in addition to the five confidential sources used. Efforts are being made to recruit two additional sources in the Directorate of Management Information Systems (DMIS), ECOM. On 9 January 1975, the PLO presented the Quarterly Progress Briefing to COL John Sanderson, Security Officer, ECOM. MAJ Nicholas F. Quintarelli, Commander, Fort Monmouth Field Office, 902d MI Group, also attended the briefing. COL Sanderson indicated at the briefing that the command was extremely well pleased with the support being provided by this ICIP.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1680 of 3957

(U) CENTURY SQUAD: (OACSI Approval - 3 Oct 73)

a. Location: US Army Management Systems Support Agency (USAMSSA), The Pentagon, Washington, DC

b. Confidential Source Utilization: One confidential source was used during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: Only one confidential source has been recruited for this ICIP. The source has been assigned for much of the time to the 2300-0700 hour shift when there has been only a small number of other persons present. Thus the situation has not been conducive to a volume of reporting. The source will be terminated early in 1975 when he transfers to a new assignment. The PLO and PCO presently are making a re-evaluation of this ICIP which will lead to a recommendation for continuation or termination. On 18 December 1974, the PLO presented a Quarterly Progress Briefing to Mr. John R. Bjork, Security Manager, USAMSSA.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Page 1681 of 3957

(U) GONDOLA STAR: (OACSI Approval - 17 Feb 72) (Revalidated 30 Oct 74)

a. Location: Aberdeen Proving Ground (APG), MD

b. Confidential Source Utilization: Seven confidential sources were used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: A source reported allegations that a civilian employee of Edgewood Arsenal was possibly engaged in an illicit affair with another Edgewood employee. The Commander was briefed.

e. Operational Status: One confidential source was terminated on 9 Oct 74. During the reporting period, limited progress was made in increasing ICIP support to the serviced activities. The PLO's duties not directly related to the ICIP limited the acquisition of ICIP sources needed to increase the ICIP coverage to the desired level. However, two prospective sources are under assessment and their recruitment is planned for the next quarter. On 18 December 1974, the Quarterly Progress Briefing was given to COL Alvin D. Ungerleider, Commander, APG, and Mr. Harry A. Mencke, Installation Intelligence Officer, APG. On 19 December 1974, the Quarterly Progress Briefing was presented by the PLO to COL Kenneth L. Stahl, Commander, Edgewood Arsenal, APG, and MAJ Walter W. Stansberry, Chief of Security, Edgewood Arsenal.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PC
AUTH Para 1-603 DOD 5200.1R

CONFIDENTIAL

Page 1682 of 3957

~~CONFIDENTIAL~~

(U) GONDOLA FLAG: (OACSI Approval - 22 Apr 74)

a. Location: US Army Electronic Proving Ground (USAPEG), Fort Huachuca, AZ

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: At present, three prospective confidential sources are under initial assessment. Personnel turbulence has hampered significant progress in this ICIP. The PLO was transferred during the last reporting period. The PLO will be transferred on a PCS overseas during the next reporting period. On 20 December 1974, the Quarterly Briefing was presented to Mr. Henry O. Dupes, Director of Security, USAPEG, Ft Huachuca, AZ. The Director of Security expressed satisfaction with the progress of the ICIP.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY OSR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1683 of 3957

(U) LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute East Coast (DLIEC), Washington Navy Yard, Washington, DC

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Approximately half of the faculty of DLIEC which is being transferred to DLI West Coast have departed for that installation. Classes and all attendant activities have been greatly reduced in preparation of the phaseout of DLIEC in Jun 75.

e. Operational Status: On 12 December 1974, the PLO presented the Quarterly Progress Briefing on the ICIP to CPT Richard W. Pederson, Security Officer, DLIEC. The Security Officer stated that the supported command was pleased with the MI support provided by the ICIP and full cooperation would be provided for the PLO in the continued conduct of the ICIP.

f. Recommendation: The Defense Language Institute, East Coast (DLIEC), will cease operations when its present cycle of students graduate this summer. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Page 1684 of 3957

(U) LEND TONE: (OACSI Approval - 16 Feb 72)

a. Location: Picatinny Arsenal (PA), Armament Command, US Army Materiel Command, Dover, NJ

b. Confidential Source Utilization: Three confidential sources were utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: A civilian employee identified earlier as being a possible security risk due to a reported episode of erratic and irrational behavior was removed from the employee rolls at Picatinny after an October 1974 report by a source that he behaved irrationally during a visit to the Installation's US Army Health Clinic.

e. Operational Status: The PCO assigned to this ICIP is being released from active duty in January 1975. An officer of the 902d MI Group Headquarters is assuming the PCO duties on an interim basis pending assignment of a PCO. Source recruitment efforts in the future will be concentrated on attempting to recruit sources who are single and have more extensive social contact in the Picatinny Arsenal and thus are better attuned to the activities of the Arsenal personnel. On 30 December 1974, the Quarterly Progress Briefing was presented by the PLO to MAJ George Carpenter, Chief, Security Office, PA. MAJ Carpenter at the briefing expressed the desire of the command that the ICIP be continued at that location.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

(U) LENIENT CLOUD: (OACSI Approval - 16 Feb 72)

a. Location: US Army War College (USAWC), Carlisle Barracks, PA

b. Confidential Source Utilization: Three confidential sources were used during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: A suitability investigation which was started in the previous period is still in progress and a subject interview plus a polygraph examination has been conducted on the original subject, an enlisted man assigned to the USAWC staff. The suitability investigation, which involved allegations of aberrant sexual activity, has expanded to include several leads implicating three officers assigned or recently assigned to USAWC. The Commandant, USAWC, has requested suitability investigations on all personnel implicated in the allegations. A female civilian applicant applying to be rehired at USAWC has become the subject of a loyalty/suitability investigation triggered by information from sources.

e. Operational Status: COL Albert N. Stubblebine III, Commander, 902d MI Group, visited USAWC for an orientation and courtesy call on the Commandant. An ICIP briefing was presented on 6 Jan 75 to LTC Richard H. Gray, Deputy Secretary for Logistics, USAWC, upon his selection as ICIP Coordinator, succeeding COL David T. Teberg. No formal Quarterly Progress Briefing was given MG DeWitt C. Smith, Jr, Commandant, USAEC, at his specific request. The PLO briefed MG Smith six times during the quarter on specific progress made in the special suitability investigations in progress as described in d, above. Because of the frequency of these briefings, MG Smith stated that a formal quarterly briefing was unnecessary. MG Smith indicated continued satisfaction with the ICIP and the support being provided by it.

f. Recommendation: The installation and activities are such in this case that we feel we can provide the support necessary without the use of confidential sources. Based upon the above, recommend the ICIP be terminated.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

188

Page 1686 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE UNDER SECRETARY
WASHINGTON, D.C. 20310

17 January 1975

MEMORANDUM FOR: VICE CHIEF OF STAFF, U.S. ARMY 21 Jan

SUBJECT: Internal Counterintelligence Program (ICIP)

I have received and reviewed the latest quarterly report of ICIP operations during 1974 as requested. In 1972 the Under Secretary authorized a trial run of this subject program. Judging from this report, the program has grown considerably and includes installations that I did not appreciate were considered sensitive. A cursory review of the data presented suggests that in more than half the cases, no useful information was obtained.

It would appear to me appropriate to review the results of this experiment to date in order to establish that the program is in fact of such a value that it should be continued in the future.

I would therefore appreciate a detailed report documenting all of the benefits, information, etc., that have been obtained through this program over the last two years. It would also be helpful to have a statement for each listed installation of the sensitive character of the mission that necessitates an ICIP operation. Finally, I would appreciate an indication of your subjective judgment as to how many of the issues that arose from these ICIP efforts would not have otherwise come to our attention.

HRStaudt

Herman R. Staudt
Under Secretary of the Army

Inclosure
Memo, 29 Nov 74,
Subj: ICIP Operations

REGRADED FOR OFFICIAL USE ONLY
WHEN SEPARATED FROM
CLASSIFIED INCLOSURES

189

189

~~CONFIDENTIAL~~

90(21Jan75)

~~TOP IDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, D.C. 20310

DEC 3 8 20 AM '74
OFFICE SECRETARY OF THE ARMY

29 November 1974

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations (U)

1. (U) Reference is made to memorandum, Under Secretary of the Army, dated 8 February 1972, subject as above.

2. (U) ~~(C)~~ During the third quarter of CY 1974, the ICIP at Edgewood Arsenal Maryland (CANAL LOOP) was combined with the Aberdeen Proving Ground ICIP (GONDOLA STAR). The nickname GONDOLA STAR was retained.

3. (U) ~~(C)~~ With the subsidence of anti-military activity at Fort Lewis, Washington and in the absence of a specific on-post threat, the Commanding General, 9th Infantry Division requested that the Fort Lewis ICIP (CENTAUR RACE) be terminated. This ICIP was inactivated on 22 Aug 74. During the same time frame, LENS HOLDER, a new ICIP developed at White Sands Missile Range was approved on 7 Aug 74. With the implementation of this ICIP, the total number of active ICIP operations at the close of the quarter was 19. Brief status reports are attached.

4. (U) ~~(C)~~ After briefing you on 25 September 1974 on the status of this program, the Assistant Chief of Staff for Intelligence personally reviewed and revalidated each on-going operation. Each operation will be revalidated on an annual basis hereafter. Additionally, MG Aaron has initiated a systematic review of all source dossiers to insure that all sources possess sufficient maturity and stability to enable them to function efficiently and effectively in ICIP operations.

1 Incl
as ~~(CONFIDENTIAL)~~

WALTER T. KERWIN, JR.
General, United States Army
Vice Chief of Staff

Classified by DAMI
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 2004

190
193

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

MAJ Ebersole/56074

~~CONFIDENTIAL~~

CLASSIFIED

ACTION SHEET

CONTROL NUMBER

SUBJECT	OFFICE SYMBOL	SUSPENSE
Internal Counterintelligence Program (ICIP)	DAMI-DOI-C	
	DATE: 20 November 1974	

ACTION REQUIRED

To obtain approval of the quarterly ICIP report.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND: By memorandum, dated 8 February 1972 (GREEN TAB B), the Under Secretary of the Army requested the Vice Chief of Staff (VCSA), US Army, to provide quarterly reports on all ICIP operations.

2. DISCUSSION: Inclosure 1 to GREEN TAB A is a memorandum for the VCSA's signature forwarding the quarterly report for the quarter ending 30 September 1974 to the Under Secretary of the Army. GREEN TAB A forwards to the VCSA the memorandum for the Under Secretary of the Army.

3. RECOMMENDATION: That the memorandum to the VCSA at GREEN TAB A be approved and signed by the ACSI.

(Continue on plain bond)

IMPLICATIONS CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR	KWH	20 NOV 74/26 NW
			DIV		20 Nov 74
			DIR MC		20 Nov 74
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

MAJ EBERSOLE/56074/th Richard A. Ebersole 191

C/Branch Record Copy

ACSI FORM 28, 13 Sep 71

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

CLASSIFIED

[redacted]

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

REPLY TO ATTENTION OF: DAMI-DOI-C

29 NOV 1974

MEMORANDUM FOR: VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above.

2. At the request of the Under Secretary of the Army, on 25 September 1974, I briefed him on status of this program. At that time, he expressed reservations about operational control within the program and its recent rapid growth. He wanted assurance that the program was carefully monitored.

3. On 4 October 1974, I personally reviewed and revalidated each operation and have arranged for a systematic review of all source dossiers.

4. Recommend your approval and signature of the attached memorandum which transmits the report required by the cited reference.

5. Coordination: None required.

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

1 Incl
as

29 NOV 1974

APPROVED - VCSA

JETHRO J. DAVIS
Colonel, GS
Assistant to the Director
of the Army Staff

Remove Classified When Separated From Classified Inclosures

192 MAJ Ebersole/56074

[redacted]

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, D.C. 20310

29 November 1974

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations (U)

1. (U) Reference is made to memorandum, Under Secretary of the Army, dated 8 February 1972, subject as above.

2. (U) During the third quarter of CY 1974, the ICIP at Edgewood Arsenal Maryland (CANAL LOOP) was combined with the Aberdeen Proving Ground ICIP (GONDOLA STAR). The nickname GONDOLA STAR was retained.

3. (U) With the subsidence of anti-military activity at Fort Lewis, Washington and in the absence of a specific on-post threat, the Commanding General, 9th Infantry Division requested that the Fort Lewis ICIP (CENTAUR RACE) be terminated. This ICIP was inactivated on 22 Aug 74. During the same time frame, LENS HOLDER, a new ICIP developed at White Sands Missile Range was approved on 7 Aug 74. With the implementation of this ICIP, the total number of active ICIP operations at the close of the quarter was 19. Brief status reports are attached.

4. (U) After briefing you on 25 September 1974 on the status of this program, the Assistant Chief of Staff for Intelligence personally reviewed and revalidated each on-going operation. Each operation will be revalidated on an annual basis hereafter. Additionally, MG Aaron has initiated a systematic review of all source dossiers to insure that all sources possess sufficient maturity and stability to enable them to function efficiently and effectively in ICIP operations.

1 Incl
as (CONFIDENTIAL)

WALTER T. KERWIN, JR.
General, United States Army
Vice Chief of Staff

Classified by DAMI
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 2004

193

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

MAJ Ebersole/56074

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

11 OCT

MIIA-SO

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOI-C)
WASH DC 20310

1. (U) Several significant changes occurred in individual Internal Counterintelligence Program (ICIP) operations during the third quarter of CY 1974. Among these was the combination of the ICIP at Edgewood Arsenal, Maryland (CANAL LOOP), with the Aberdeen Proving Ground ICIP (GONDOLA STAR) on 17 July 1974. The nickname GONDOLA STAR was retained for the resulting consolidated ICIP which will realize some savings in administrative requirements and permit a more effective utilization of available manpower.

2. (U) The Commanding General, 9th Infantry Division, and Headquarters, Fort Lewis, Washington, requested that the Fort Lewis ICIP be terminated due to the subsiding of the level of anti-military activities at that post and the absence of a specific on-post threat. With the concurrence of the Commanding General, FORSCOM, the ICIP was inactivated on 22 August 1974. The White Sands Missile Range ICIP, which had been requested in the previous quarter, was approved on 7 August 1974. Spotting and assessment for potential sources continues. With the implementation of the White Sands Missile Range ICIP, the total number of active ICIP operations at the close of the quarter is 19.

3. (U) Since the 1 July 1974 organization of the US Army Intelligence Agency, the 902d MI Group and the 525th MI Group have both experienced a reduction in personnel authorizations at all levels to include some Resident Offices which were initially established for the purpose of supporting an approved ICIP project. The reductions are impacting on some areas, especially isolated installations where servicing by both the Project Liaison Officer (PLO) and Project Case Officer (PCO) threatens to escalate TDY costs. In an effort to find a solution, the 525th MI Group has consolidated the functions of the PLO and the PCO by having the PLO perform duties for both. This measure has been put into

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

194

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Exempt

~~CONFIDENTIAL~~

[redacted]

MIIA-SO
SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

effect at Sierra Army Depot, Dugway Proving Ground, and Umatilla Army Depot. The 902d MI Group has experienced difficulty in maintaining PLOs full-time at Seneca Army Depot and Picatinny Arsenal. During the reporting period, PLOs at Carlisle Barracks, Fort Ritchie, and Fort Monmouth all spent a considerable amount of time on TDY and in support of other counterintelligence duties. Local Field Office Commanders are making efforts to assign their personnel to duties according to assigned priorities, but the current shortages are slowing somewhat on-going operations and hampering the development of the newly established ICIPs.

4. (U) Currently an in-depth review of each ICIP is being made with an objective of determining the effectiveness of each operation. The necessity of continuing or recommending termination of each ICIP and possible improvements which can be made are also goals of this revalidation program.

5. (U) Brief status reports for each of the active 19 ICIP operations are attached as inclosures.

FOR THE COMMANDER:

E. L. Stephens

19 Incl
as

E. L. STEPHENS
Chief
Intelligence Division

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

195

2

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

MIIA-SO

11 OCT 1974

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOI-C)
WASH DC 20310

1. (U) Several significant changes occurred in individual Internal Counterintelligence Program (ICIP) operations during the third quarter of CY 1974. Among these was the combination of the ICIP at Edgewood Arsenal, Maryland (CANAL LOOP), with the Aberdeen Proving Ground ICIP (GONDOLA STAR) on 17 July 1974. The nickname GONDOLA STAR was retained for the resulting consolidated ICIP which will realize some savings in administrative requirements and permit a more effective utilization of available manpower.

2. (U) The Commanding General, 9th Infantry Division, and Headquarters, Fort Lewis, Washington, requested that the Fort Lewis ICIP be terminated due to the subsiding of the level of anti-military activities at that post and the absence of a specific on-post threat. With the concurrence of the Commanding General, FORSCOM, the ICIP was inactivated on 22 August 1974. The White Sands Missile Range ICIP, which had been requested in the previous quarter, was approved on 7 August 1974. Spotting and assessment for potential sources continues. With the implementation of the White Sands Missile Range ICIP, the total number of active ICIP operations at the close of the quarter is 19.

3. (U) Since the 1 July 1974 organization of the US Army Intelligence Agency, the 902d MI Group and the 525th MI Group have both experienced a reduction in personnel authorizations at all levels to include some Resident Offices which were initially established for the purpose of supporting an approved ICIP project. The reductions are impacting on some areas, especially isolated installations where servicing by both the Project Liaison Officer (PLO) and Project Case Officer (PCO) threatens to escalate TDY costs. In an effort to find a solution, the 525th MI Group has consolidated the functions of the PLO and the PCO by having the PLO perform duties for both. This measure has been put into

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

196

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Graduate

[redacted]

MIIA-SO
SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

effect at Sierra Army Depot, Dugway Proving Ground, and Umatilla Army Depot. The 902d MI Group has experienced difficulty in maintaining PLOs full-time at Seneca Army Depot and Picatinny Arsenal. During the reporting period, PLOs at Carlisle Barracks, Fort Ritchie, and Fort Monmouth all spent a considerable amount of time on TDY and in support of other counterintelligence duties. Local Field Office Commanders are making efforts to assign their personnel to duties according to assigned priorities, but the current shortages are slowing somewhat on-going operations and hampering the development of the newly established ICIPs.

4. (U) Currently an in-depth review of each ICIP is being made with an objective of determining the effectiveness of each operation. The necessity of continuing or recommending termination of each ICIP and possible improvements which can be made are also goals of this revalidation program.

5. (U) Brief status reports for each of the active 19 ICIP operations are attached as inclosures.

FOR THE COMMANDER:

19 Incl
as

E. L. STEPHENS
Chief
Intelligence Division

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CSA MSG DACSM-701/PO
AUTH Para 1-603 DOD 5200.1R

[redacted]

197

2

[redacted]

1 (U) CANAL ROPE: (OACSI Approval - 17 Dec 73)

a. Location: Headquarters, US Army Communications Command and 11th Signal Group, Fort Huachuca, AZ.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Investigative data and assessment information on newly recruited sources.

e. Operational Status: One confidential source in the 11th Signal Group Crypto Facility who had been recruited in April 1974 was terminated when he lost his placement and access. He also is near the completion of his federal service. A second confidential source recruited in May 1974 in the Communications Electronics Engineering Installation Agency (CEEIA), Hq, US Army Communications Command (USACC) was terminated when continued assessment and evaluation revealed previously unknown personal and professional problems. Spotting and assessing actions are now under way to recruit new confidential sources for the operation. The CANAL ROPE PLO presented a Quarterly Progress Report on the ICIP to Mr John Maiorana, Chief, Physical Security, USACC, Ft Huachuca, on 27 September 1974. The security official indicated to the PLO that USACC was satisfied with the ICIP.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY OSD/WHS/DOM/FOI/PO
AUTH Para 1-603 DOD 5200.1R

198

[redacted]

[redacted]

2 (U) CANARY EFFORT: (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three sources were used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Three potential confidential sources are currently under assessment. Adverse suitability information alleging moral misconduct on the part of a civilian employee with a SECRET clearance was reported. The Deputy Chief of Staff, Intelligence and Security, Fort Ritchie, and the Provost Marshal have been notified and are monitoring the employee's activities. An enlisted man with a TOP SECRET clearance and assigned to the Automatic Message Processing Systems (AMPS) Branch, Telecommunications Directorate, Site "R", for temporary duty, displayed an abnormal interest in firearms, explosives, and poisons. He also displayed somewhat abnormal behavior traits. The individual's access has been suspended temporarily pending a psychiatric evaluation.

e. Operational Status: Twenty-two official sources and 14 liaison sources are contacted on a frequent basis in addition to the three confidential sources. The PIO presented the Quarterly Progress Report to the supported command on 12 September 1974. The following were present at the briefing: COL Harold G. deMoya, Commander, Fort Ritchie; LTC Arlyn R. Madsen, Director, Telecommunications, Fort Ritchie; Mr. Joseph J. Carroll, Chief, Intelligence and Security, US Army Communications Command-CONUS and HQ, Fort Ritchie; CPT Lawrence N. Brogan, Commander, Fort Ritchie Field Office, 902d MI Group; and CW2 Benjamin Struchen, HQ, 902d MI Group.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

199

[redacted]

3. (C) CANARY STONE: (OACSI Approval - 18 Jul 73)

a. Location: Dugway Proving Ground, (DPG), UT

b. Confidential Source Utilization: Two confidential sources were utilized during the period.

c. Information Obtained Off-post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Assessment information and investigative data used for potential confidential sources. Minor suitability information on the drinking habits of three DPG employees was reported. The Installation Security Officer has been appraised of the information and will continue to monitor the behavior of the employees in coming weeks.

e. Operational Status: Two confidential sources were recruited during the reporting period and are being provided training and orientation. On 9 September 1974, a new PLO/PCO was assigned to the ICIP and the Dugway Proving Ground Resident Office. The new PLO/PCO has assumed control of both the newly recruited confidential sources used in the operation and has been engaged in thorough orientation of his new duties. On 29 August 1974, LTC Andrew J. Armstrong, Acting Commander, DPG, was briefed by the former PLO in the presence of MAJ Trevor E. Bissey, Commander, San Francisco Field Office, 525th MI Group, and Mr. Clinton E. Bair, Intelligence Officer, Security Div, DPG. LTC Armstrong provided the initial ICIP briefing to the new DPG Commander, COL Adalbert F. Toepel, Jr., on 9 September 1974. The ICIP PLO and LTC Henry F. Kale, Director of Security, DPG, will provide a more detailed briefing to the new Commander at a later date.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

200

4. CANINE PLATE: (OACSI Approval - 18 Sep 73)

a. Location: Seneca Army Depot, Romulus, NY

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: Investigative data on prospective sources.

e. Operational Status: Coverage of the Directorate for Special Weapons (DSW) presently is maintained by use of two conventional sources. Two additional prospective sources, both of whom are assigned to the military police guard force, are presently under assessment. Prolonged absence of the PLO during this period due to leave and TDY travel to other locations hampered effective development and recruitment of new sources. The PLO has identified a total of four individuals for possible use as conventional sources in support of the operation. It is the goal of the Fort Monmouth Field Office Commander to recruit an additional three or four sources by the end of the calendar year. COL Light, Seneca Army Depot Commander, has instructed the PLO to use extreme care in the recruitment of sources and expressed his desire that the ICIP be developed very slowly. No Quarterly Progress Briefing was given during the period since there were no significant items of information reported. The PLO was on extended TDY for most of the month of September.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM-F01/PO
AUTH Para 1-603 DOD 5200.1R

SEP 5 1997

201

5. (U) CANYON ROSTER: (OACSI Approval - 8 Mar 74)

a. Location: Umatilla Army Depot Activity (UMDA), Hermiston, Oregon

b. Confidential Source Utilization: One confidential source was utilized during this period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Information received on the possible theft and a sale of weapons from UMDA has resulted in all weapons being placed in an area under twenty-four hour guard. A construction project has been started to build a centralized weapons storage area. As a result of a request for aerial photographs of UMDA being received by the depot, procedures have been established whereby all questionable requests for information will be routed through the PLO of the ICIP.

e. Operational Status: One confidential source was recruited during the reporting period. Seven other potential sources, four of whom are guards on various shifts at UMDA, are also under assessment and preliminary investigation. On 17 September 1974, the PLO briefed the Commander, UMDA, LTC Daniel W. Doty on the progress of the ICIP during the quarter. The briefing consisted of a review of MI activities directed toward improving the security of UMDA. LTC Doty indicated he was generally well satisfied with the program and the support rendered. It became evident during the quarter that UMDA's mission will be one of a long-term storage of conventional and toxic munitions. Although the work force is still unstable, target areas within the UMDA organizational structure have been identified and potential sources within each area are now under assessment. Liaison contacts with other Federal agencies and civilian law enforcement agencies are being developed as part of an early warning net around UMDA.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPA
AUTHORITY OF DEPSECDEF

6. (U) CANVAS TAX: (OACSI Approval - 8 Mar 74)

a. Location: Sierra Army Depot (SIAD), Herlong, CA

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: Investigative data on prospective confidential sources.

e. Operational Status: Overall progress in this ICIP has been extremely slow due to the non-availability of a PLO. The PLO assigned in June 1974 which was reported in the previous Quarterly Report was not continued on station. A decision was made to combine the PLO and Project Case Officer (PCO) functions in this ICIP. Continued development of the operation can be expected as soon as a PLO/PCO is on station. On 15 August 1974, the Quarterly Briefing was presented to the supported command. Those in attendance were: COL Robert Hawlk, CDR, SIAD; LTC Bernard Render, Dep CDR, SIAD; MAJ John Jolley, PM/Security Officer; SIAD; 1LT Wayne Heringer, Intelligence Officer, SIAD; and Mr. Anthony Tornabene, Asst Intelligence Officer, SIAD. LTC Clifford Fry, USAINTA Liaison Officer to HQ, Army Materiel Command, also attended the briefing. COL Hawlk, SIAD Commander, expressed his support for the concept of the operation and added that support would be provided the SIAD Resident Office when it was established.

REGRADED UNCLASSIFIED
ON SEP - 5 19
BY ODS/INSCOM/F01/PO
AUTH Para 1-603 DOD 5200.1R

203

[redacted]

7. (U) CANTINA ARCH: (OACSI Approval - 12 Dec 73)

a. Location: US Army Air Defense Center and Fort Bliss (USAADCENFT), TX

b. Confidential Source Utilization: Four confidential sources were utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Information was reported on a person assigned to Fort Bliss with a security clearance who resides in Mexico and was allegedly dealing in gold and silver. The report was provided to the Directorate of Security (DSEC) and to the Criminal Investigation Division (CID) for further investigation. As a result of this report, the supported command now requires that all personnel holding a security clearance and residing in Mexico report this fact, along with their address. The DSEC now maintains a roster of all such personnel.

e. Operational Status: The prospective confidential source in the Emergency Operations Center who was under assessment during the last reporting period was recruited on 4 September 1974. The US Army Communications Command Agency Fort Bliss Telecommunications Center presently is being covered through the liaison efforts of the Project Liaison Officer (PLO), but efforts are being made to recruit a confidential source there in the future. On 20 September 1974, the ICIP PLO presented a Quarterly Status Report on CANTINA ARCH to CPT James E. Stevens, Acting DSEC, USAADCENFT, Ft Bliss. Speaking for the Commander, the Acting DSEC indicated that the operation seems to be progressing in a satisfactory manner. He had no other comments, recommendations or expressed problem areas. A new DSEC will be appointed in the near future and will be briefed on the operation after he assumes his duties.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

204

[redacted]

8. (U) CENSUS TIME: (OACSI Approval - 5 Feb 74)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC

b. Confidential Source Utilization: One source was used during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: Investigative leads for possible confidential sources.

e. Operational Status: As part of his training, the one confidential source used in this ICIP was given test EEI and tasked to provide names of other potential sources. Three other potential sources, all in the Operations Division, PTC, are currently under assessment. If these sources are successfully recruited, the depth of coverage of the target area will be improved considerably. The PLO provided the Quarterly Progress Briefing on 26 August 1974 to COL Joseph T. Adinaro, Commander, PTC, and Mr. D. E. Thompson, Deputy Commander, PTC. Both the Commander and the Deputy Commander, PTC, indicated satisfaction with the support rendered by the ICIP and the progress of its development to date.

UNCLASSIFIED
ON SEP 5 1997
BY C SER F01/PO
AUTH 00.1R

205

[redacted]

(U)

9. ~~(S)~~ CENTAUR SALE: (OACSI Approval - 14 Dec 73)

a. Location: US Army Mobility Equipment Research and Development Center (MERDC), Fort Belvoir, VA

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Investigative data on prospective sources.

e. Operational Status: This ICIP coverage to date has been made by conventional sources who have access to the target areas and liaison contacts. Efforts are being made by the Pentagon CI Force/National Capital Region Field Office to revitalize this ICIP. To provide a wider target coverage of MERDC, three potential confidential sources are presently under assessment. The PLO presented the Quarterly Progress Briefing to Mr. Leslie L. Askew, Security Manager, MERDC, on 28 August 1974. The Commander and the MERDC staff continue to provide support for the ICIP and render all possible assistance for its continued development.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

[redacted]

206

[redacted]

10. (U) CENTAVO KID: (OACSI Approval - 18 Oct 73)

a. Location: Harry Diamond Laboratories, Washington, DC

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Investigative data on potential sources.

e. Operational Status: The Pentagon Counterintelligence Force/ National Capital Region Field Office (PCF/NCR FO), 902d MI Group, which is charged with the conduct of this ICIP is engaged in an intensive review and revitalization program for the operation. At present, two individuals who are employed in the Harry Diamond Laboratories, one in the Engineering/Reserve Support Division, and one in the Relocation/ Planning Group are under assessment as potential confidential sources. The PLO presented the Quarterly Progress Briefing on 23 August 1974 to COL D. W. Einsel, Jr., Commander, Harry Diamond Laboratories, and Mr. Joseph Schnieder, Security Manager. Both the Commander and the Security Manager continue to support the ICIP strongly and provide cooperation necessary for its development.

DECLASSIFIED UNCLASSIFIED
ON SEP 5 1997
UNDER USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

[redacted]

11. (U) CENTRAL TAXI: (OACSI Approval - 16 Feb 72)

a. Location: Headquarters, US Army Electronics Command (ECOM), Fort Monmouth, New Jersey

b. Confidential Source Utilization: Five confidential sources were utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: A source reported that a civilian employee at Fort Monmouth was stealing US Government property. The information was passed to the Fort Monmouth CID for further investigation. Another source reported that an employee in the ECOM Directorate of Research, Development, and Engineering was planning non-official travel to Finland and the Soviet Union. Further details are being sought on the lead. A civilian physicist in the Electronics Technology and Devices Laboratory at ECOM received unsolicited correspondence from an organization calling itself the Arab Projects and Development, Beirut, Lebanon. The employee promptly notified the proper security authorities and requested permission to respond to the letter. He was granted permission by the US Army Materiel Command, answered the initial letter and received a reply in September 1974. Investigation to date has revealed little information concerning Arab Projects and Development but the assets in the ICIP will continue to monitor future activity.

e. Operational Status: In addition to the five confidential sources being contacted regularly in this ICIP, thirteen conventional sources provide additional coverage of ECOM target areas. Among four employees presently being assessed as possible sources, one has been dropped from further consideration due to refusal to cooperate in the program. There are three remaining under active consideration. The PLO presented the Quarterly Progress Briefing on 30 September 1974 to COL John Sanderson, Security Officer, ECOM, and ICIP Project Coordinator for ECOM. COL Sanderson indicated command satisfaction with the type of information and support rendered by this ICIP.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

208

12. (U) CENTURY SQUAD: (OACSI Approval - 3 Oct 73)

a. Location: US Army Management Systems Support Agency (USAMSSA), The Pentagon, Washington, DC

b. Confidential Source Utilization: One confidential source was utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: Only one confidential source has been recruited to date in this operation. The PCO has been devoting most of the meeting periods to further training and testing of this source. In addition to training, the source is being tasked to provide names and leads for additional possible sources. Two other employees of the Operations Division, USAMSSA, are being evaluated as potential sources. The Quarterly Briefing of the supported command was presented by the PLO on 18 September 1974 to Mr. John R. Bjork, Security Manager, USAMSSA. The Director and his security staff continue to support the operation fully and have offered every assistance to aid in its development.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOIA/PO
AUTH Para 1-603 DOD 5200.1R

Page 1707 of 3957

13 (U) GONDOLA FLAG: (OACSI Approval - 22 Apr 74)

a. Location: US Army Electronic Proving Ground (USAPEG), Fort Huachuca, AZ

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: Additional investigative data on a prospective confidential source.

e. Operational Status: The prospective source, located in the Electromagnetic Branch, USAEPG, is in the final stages of assessment and recruitment is expected during the next reporting period. Efforts to spot and recruit sources in this comparatively new ICIP were somewhat hampered by the transfer of the PLO during the period. On 27 September 1974, the PLO gave the Quarterly Progress Report to Mr. Henry O. Dupes, Director of Security, USAEPG, Ft Huachuca, AZ, who stated that the Commander, USAEPG, was satisfied with the progress of the ICIP to date.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

210

14(U) GONDOLA STAR: (OACSI Approval - 17 Feb 72)

a. Location: Aberdeen Proving Ground (APG), MD

b. Confidential Source Utilization: Eight confidential sources were used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: A report of an employee who travelled to Poland with his two sons triggered a request for an investigation by the supported command of the employee's foreign travel and extent of his foreign connections when it was learned that he plans to send his eldest son to Poland on some type of foreign exchange program. Another employee planned travel to Czechoslovakia in Aug 74, but postponed his trip to 1975 when he was hospitalized. The supported command does not desire an investigation immediately, but has requested continued monitoring by the ICIP. A man and wife physicist team have had their access to classified information suspended while an investigation is conducted concerning their alleged loose moral conduct andabuse of alcohol. A confidential source reported that a cipher lock installed on a door to a Data Processing Office of the US Army Test and Evaluation Command (TECOM), APG, had been altered so the door could be opened without using the combination. Investigation revealed that the lock had been installed and made operational to check for possible defects and subsequently disconnected. The lock was disconnected pending installation of a telephone at the door for use by persons not having the combination in order to call for escort. The telephone has now been installed and the cipher lock has been re-connected.

e. Operational Status: During the reporting period, limited progress was made in increasing ICIP support to the serviced activities since duties not directly related to the ICIP required the greatest portion of the PLO's time. One confidential source was terminated due to loss of placement and access. One confidential source with placement in Edgewood Arsenal was recruited. Three other potential sources are still under assessment. On 25 September 1974, COL Alvin D. Ungerleider, newly assigned Commander, APG, was given both the initial ICIP Briefing and the Quarterly Progress Briefing. Mr. Harry A. Mencke, Installation Intelligence Officer (IIO), APG, was present for both briefings. The PLO gave a Quarterly Progress Briefing on 26 September 1974 to COL Kenneth L. Stahl, Commander, Edgewood Arsenal, APG, and MAJ Walter W. Stansberry, Chief of Security, Edgewood Arsenal.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

211

15 (U) GONG SILK: (OACSI Approval - 16 Feb 72)

a. Location: Picatinny Arsenal (PA), Armament Command, US Army Materiel Command, Dover, NJ

b. Confidential Source Utilization: Three confidential sources were used during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: A source reported that a PA employee frequently used a substance which appeared to be a narcotic during duty hours, then left his work area to sleep in parked cars. The information was passed to the PA security officials with a recommendation that a limited investigation be conducted. Another PA employee of the Ammunition Development and Engineering Directorate (ADED) was reported to be under the care of a psychiatrist. Investigation revealed that the PA Civilian Personnel Office and the employee's supervisors were aware of the problem. Although the employee continues to have access to classified defense information, his workload has been significantly reduced and all of his activities at ADED are closely supervised. A confidential source reported that combinations on adjacent security containers in the Nuclear Development and Engineering Directorate were set in numerical sequence, a practice in contravention of security regulations. Security officials were briefed on the weakness and have taken corrective action.

e. Operational Status: A new PIO has assumed duties who has devoted much of his efforts acquiring area knowledge, establishing source rapport and acquiring on-the-job experience. Due to a personnel shortage, the PIO no longer is able to spend his full time with the supported command, but the commander of the Fort Hamilton Resident Office performs the PIO duty on a TDY basis. This will serve to make spotting and assessing of future sources difficult. On 20 September 1974, the PIO presented the Quarterly Progress Briefing to MAJ George Carpenter, Chief, Security Office, PA. MAJ Carpenter indicated during the briefing that the command was satisfied with the service provided by the ICIP.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

16 (U) (C) LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute, East Coast (DLIEC), Anacostia Naval Annex, Washington, DC

b. Confidential Source Utilization: None

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: Investigative data on a potential confidential source.

e. Operational Status: As reported previously, DLIEC is being phased out during Fiscal Year 1975 in preparation for its move to DLIWC, Presidio of Monterey, CA. For that reason, a concerted effort is not being made to recruit large numbers of sources, although at present one potential source is being assessed. The move to the Presidio of Monterey will be completed by 1 Jul 75. DLIEC security records have been shipped to DLIWC. The PIO presented the Quarterly Progress Briefing in the ICIP to CPT Richard W. Pederson, Security Officer, DLIEC, on 16 September 1974. The Commandant and the Security Manager continue to provide cooperation and no problems exist at this time.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Page 1711 of 3957

17. (U) LENIENT CLOUD: (OACSI Approval - 16 Feb 72)

a. Location: US Army War College (USAWC), Carlisle Barracks, PA

b. Confidential Source Utilization: Three confidential sources were used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: Numerous reports were made on USAWC personnel during the period, primarily on suitability, but ranging from drug abuse to aberrant sexual activity. Five military policemen were apprehended for narcotics abuse; their security clearances were suspended and they were removed from sensitive duties. Of the total of 13 suitability cases reported during the period, security clearances were suspended for 6; investigations have been requested for 4; 1 individual was dismissed from USAWC; 1 has been reassigned, and the activities of the one remaining are being monitored. With the addition of the US Army Military History Research Collection to USAWC, both the ICIP PLO and the Ft Ritchie Field Office personnel have provided security support and assistance in the form of a Counter-intelligence Survey and identification of security weaknesses and deficiencies.

e. Operational Status: The PLO served as Acting USAWC Security Manager during a three-week absence of the incumbent and has now established at least one after duty hours CI inspection per week with the approval of COL D. T. Teberg, ICIP Coordinator. On 5 August 1974, MG DeWitt C. Smith, Jr., Commandant, USAWC, was provided his initial ICIP briefing. Following that briefing, MG Smith requested that he be briefed on significant developments of the operation at least monthly rather than quarterly. MG Smith was given a second briefing on 30 Aug 74. The PLO presented an initial ICIP briefing to COL William M. Whitesel, Deputy Commanding Officer, Carlisle Barracks, on 3 September 1974

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM ATTN: IAPO
AUTH Para 1-603 DOD 5200.1R

Page 1712 of 3957

(U)

18. ~~(S)~~ LENS HOLDER: (OACSI Approval - 7 Aug 74)

a. Location: White Sands Missile Range (WSMR), NM

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable

d. Useful Information Obtained: Initial spotting and assessment actions are taking place.

e. Operational Status: During the processing of applicants for MI, the PLO has identified two potential sources for this ICIP, which is the most recently implemented operation. The ICIP PLO briefed MG Robert J. Proudfoot, Commanding General, WSMR, on the implementation of the ICIP on 16 September 1974. MG Proudfoot verbally approved the operation which had been requested by his predecessor, MG Sweeney. MG Proudfoot stated that he desired a progress briefing on the ICIP in two or three months. LTC Carl I. Davis, Chief of Security, WSMR; and Mr. William F. Arket, Chief, Intelligence Div, WSMR, also attended the briefing.

REGRADED UNCLASSIFIED
ON 14661 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

215

[redacted]

(U)

19. ~~(C)~~ LENTIL MONKEY: (OACSI Approval - 26 Oct 71)

a. Location: Defense Language Institute West Coast (DLIWC), Presidio of Monterey, CA

b. Confidential Source Utilization: Nine confidential sources were utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: The Czech "Pen-Pal" incident and the visit of a Polish national with his brother, a DLIWC instructor, reported in the last period, are still under investigation. Information concerning a new "pen-pal" relationship was reported, this one involved a US Air Force student. The airman exchanged several letters with a Polish citizen and sent him money for the purchase of Polish magazines. The Polish citizen commented in his letters that he believes the letters are being checked by Polish officials, since one was received in an opened condition. Information on this incident has been passed to the Air Force. Information surfaced that an instructor of the Polish Language Department has a radio transmitter at his residence is presently being investigated. Another report that unauthorized radio transmissions were being heard in the Fort Ord area is being evaluated by the National Security Agency (NSA). Two Soviet citizens, allegedly language instructors for the Soviet Government, visited DLIWC on a State Department sponsored trip. The State Department did not provide an escort and the visitors were able to visit the Russian Language Department unescorted. The DLIWC Security Officer has taken steps to prevent a recurrence of this type of incident and especially to insure that all visitors are properly escorted. Suitability information concerning student personnel continued to be reported and was passed to the appropriate authorities. Information received from another government investigative agency and amplified by the ICIP sources indicates that the Arabic Trade Mission located in San Francisco is gathering data on DLIWC Arabic students. During a class visit to the Arabic Trade Mission, DLIWC Arabic students were required to sign a guest register, listing their names and addresses. The reason for the register was allegedly so that additional printed information could be sent to the students. The students were also given anti-Israel propaganda.

e. Operational Status: Five confidential sources were terminated during the period due to graduation. Reduction of case officer personnel on the project to one full-time and one part-time case officer may make it necessary to limit the number of confidential sources handled to five.

REGRADED UNCLASSIFIED
ON 26 SEP 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

216

[redacted]

[redacted]

At present, four confidential sources are active; two potential sources, including one instructor, are under assessment. In the future, confidential sources will be recruited on a staggered basis, with no more than two sources recruited in any one quarter. This will prevent the loss of several sources at one time due to graduation. The PIO presented the Quarterly Progress Report on 19 Sep 74 to LTC Max Newman, Secretary, DLIWC; MAJ Richard Erickson, Security Officer, DLIWC; and CPT Edward N. Janecki, Commander, Fort Ord Field Office, 525th MI Group. LTC Newman expressed appreciation for information furnished through the project and requested that briefing be planned for mid-October 1974 for the new incoming Director, DLIWC, COL Koenig.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

217

[redacted]

~~SECRET~~

DAMI-DOI-C 27 September 1974

MEMORANDUM FOR THE RECORD

SUBJECT: ICIP Briefing for Under Secretary of the Army (U)

1. (U) ~~(C)~~ On 25 September 1974 MG Aaron briefed Mr. Herman Staudt, on the ICIP. Mr. Staudt expressed reservations about operational control within the program and concern about the sudden rapid growth. He wanted assurances that the program was carefully monitored precluding the possibility for embarrassment.

2. (U) ~~(C)~~ General Aaron assigned the following tasks to USAINTA through Mr. Leslie Hime, the USAINTA representative at the meeting.

a. Prepare all the operations plans for review; General Aaron will personally re-validate each plan.

b. Prepare source dossiers for review. General Aaron wants to be able to personally be assured that all sources are of such maturity and stability that they would not cause any embarrassment to the Army.

3. (U) ~~(C)~~ General Aaron will personally validate and approve all future operations plans and will assume command and control of the program. Only essential plans will be approved and permitted to continue. General Aaron did not consider the operation at the War College to be essential.

4. (U) Operations plans and dossiers will be reviewed on 4 October 1974.

RICHARD EBERSOLE
Major, GS

Regraded ~~Confidential~~ When Separated From Classified Enclosures.

REGRADED UNCLASSIFIED ON SEP 5 1997 BY CDR USAINSCOM F01/PO AUTH Para 1-603 DOD 5200.1R

218

~~SECRET~~

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) Operations

OFFICE SYMBOL: DAMI-DOI-C

SUSPENSE:

DATE: 6 August 1974

ACTION REQUIRED: To obtain approval of the quarterly ICIP report.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By memorandum, dated 8 February 1972 (ORANGE TAB B), the Under Secretary of the Army requested the Vice Chief of Staff (VCSA), US Army, provide quarterly reports on all (ICIP) operations.

b. This is the nineth such quarterly report.

c. The quarterly report of current operations for the quarter ending 31 March 1974 is at (ORANGE TAB C).

30 Jun 74

2. DISCUSSION:

a. Inclosure 1 to ORANGE TAB A is a memorandum for the VCSA's signature forwarding the quarterly report to the Under Secretary of the Army.

b. ORANGE TAB A forwards to the VCSA the memorandum and ICIP Quarterly Report.

3. RECOMMENDATION: That the memorandum to the VCSA at ORANGE TAB A be approved and signed by the ACSI.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		6 Aug 74
			DIV		6 Aug 74
			DIR		8 Aug 74
			EX		
			ACSI		
			DISPATCHED (DTG)		
SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET					

ACTION OFFICER *(Name, grade, phone and signature)*
MAJ PIGNATO/77017/th — MAJ P C Pignato 219

CI Branch
Record Copy

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

REPLY TO ATTENTION OF: DAMI-DOI-C

21 AUG 1974

MEMORANDUM FOR: VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above.

2. Recommend your approval and signature of the attached memorandum which transmits the report required by the cited reference.

3. Coordination: None required.

1 Incl
as

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

21 AUG 1974

APPROVED - VCSA

JETHRO J. DAVIS
LTC, GS
Assistant to the Director
of the Army Staff

Regraded UNCLASSIFIED when separated from classified inclosures

MAJ Pignato/77017

220

~~CONFIDENTIAL~~

DAMI-DOI-C

MEMORANDUM FOR: VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above.

2. Recommend your approval and signature of the attached memorandum which transmits the report required by the cited reference.

3. Coordination: None required.

1 Incl
as

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

Regraded UNCLASSIFIED when
separated from classified
inclosure

MAJ Pignato/77017

221

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations (U)

1. (U) Reference is made to memorandum, Under Secretary of the Army, dated 8 February 1972, subject as above.

2. (U) Progress in the second quarter of CY 1974 in the ICIP was characterized by a sizeable increase in the number of Confidential Sources utilized in the various ICIPs. Thirty-six Confidential Sources have been recruited, an increase from 27 in the preceding quarter. One request for an ICIP was received during the period which requested ICIP coverage at the White Sands Missile Range, White Sands, New Mexico. Brief status reports are attached.

3. (U) As Army reorganization results in some shifts of facilities to other locations, the consolidation of ICIP operations continues in the interest of more efficient management and administration. The ICIP LANDLESS TIME (U), which formerly supported the Philadelphia Facility of the US Army Electronics Command, has been consolidated with the ICIP CENTRAL TAXI (U), which supports Electronics Command at Fort Monmouth, New Jersey. A similar revised plan is being written in which the ICIP CANAL LOOP (U) at Edgewood Arsenal, Maryland, will be combined with the Aberdeen Proving Ground ICIP GONDOLA STAR (U). Including these consolidations, there were 19 ICIP operations active at the close of the period. The White Sands Missile Range ICIP, for which implementation is expected early in the next quarter, will bring this total to 20.

4. (U) As I mentioned to you in my memorandum of 30 April 74, the primary value of ICIP operations is in their potential for early warning and detecting internal security weakness and security threats to the supported command. Inasmuch as these operations are a form of intensified security watchfulness, negative reports in themselves are frequently of value to a commander in planning for security requirements of a given installation or activity.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

1 Incl
as

FRED C. WEYAND
General, United States Army
Vice Chief of Staff

Classified by DAMI-DO
222
2
31 December 2004

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

MIIA-OP-O

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOI-C)
WASH DC 20310

1. (U)(C) Progress in the second quarter of CY 1974 in the ICIP was characterized by a sizeable increase in the number of Confidential Sources utilized in the various ICIPs. Thirty-six Confidential Sources have been recruited, an increase from 27 in the preceding quarter. One request for an ICJP was received during the period which requested ICIP coverage at the White Sands Missile Range, White Sands, New Mexico.

2. (U)(C) As Army reorganization results in some shifts of facilities to other locations, the consolidation of ICIP operations continues in the interest of more efficient management and administration. The ICIP LANDLESS TIME (U), which formerly supported the Philadelphia Facility of the US Army Electronics Command, has been consolidated with the ICIP CENTRAL TAXI (U), which supports Electronics Command at Fort Monmouth, New Jersey. A similar revised plan is being written in which the ICIP CANAL LOOP (U) at Edgewood Arsenal, Maryland, will be combined with the Aberdeen Proving Ground ICIP GONDOLA STAR (U). Including these consolidations, there were 19 ICIP operations active at the close of the period. The White Sands Missile Range ICIP, for which implementation is expected early in the next quarter, will bring this total to 20.

3. (U)(C) Significant progress in the operations at Sierra and Umatilla Army Depots is expected during the coming quarter. The Project Liaison Officer arrived at Sierra Army Depot on 19 June 1974. Two prospective sources, spotted during TDY trips to the installation by personnel from the San Francisco Field Office, are presently under assessment. A similar situation exists at the Umatilla Army Depot at Hermiston, Oregon. The Project Liaison Officer became operational at that facility on 30 June 1974, at the close of the quarter. TDY trips pending the assignment and arrival of the PLO have resulted in having 19 civilian

Cdr USA Intel Agcy

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

223

Indef

MIIA-OP-O
SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

employees of the Umatilla Depot under assessment as potential sources by the close of the reporting period.

4. (U) Brief status reports for each of the active 19 ICIP operations are attached as inclosures.

FOR THE COMMANDER:

19 Incl
as

EDWARD H. BORT
Colonel, MI
Chief, Operations Division

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Cdr USA Intel Agency

224
2

Indiv 2

1. (U) ~~(C)~~ CANAL ROPE: (OACSI Approval - 17 Dec 73)

a. Location: Headquarters, US Army Communications Command and 11th Signal Group, Fort Huachuca, AZ.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Investigative data on potential sources.

e. Operational Status: One confidential source was recruited in the 11th Signal Group Crypto Facility on 17 April 1974, and a second confidential source was recruited in the Communications Electronics Engineering Installation Agency (CEEIA), Headquarters, US Army Communications Command (USACC), on 20 May 1-74. Two additional sources in USACC are under assessment for possible recruitment in the next quarter. One CIRL surfaced by the ICIP is under assessment for possible exploitation as an OFCO. The CANAL ROPE PLO briefed Mr. R. H. Milligan, Office of the Assistant Chief of Staff for Intelligence and Security, USACC, on 28 May 74, on the status of the ICIP. Mr. Milligan stated that USACC was pleased with the support being provided by this ICIP.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Cdr USA Intel Cyber

2

225

2. (U) ~~(C)~~ CANARY EFFORT: (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD.

b. Confidential Source Utilization: Three sources were used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Information developed on 15 US Army personnel involved in drug abuse-related incidents was passed to the ICIP Coordinator. Adverse suitability information developed on a soldier assigned to the Operations Company, Fort Ritchie. The soldier, whose clearance was suspended, was transferred to Kimbrough Army Hospital, Fort Meade, for psychiatric evaluation on 28 May 1974. Alleged moral misconduct on the part of a WAC was reported to the ICIP Coordinator. The supported command is monitoring the activities of the WAC to determine if an investigation is warranted. Information obtained on alleged threats against the lives of three Military Police investigators was provided the Fort Ritchie Commander and the ICIP Coordinator. The US Army Criminal Investigation Department Command (USACIDC) is conducting an investigation.

e. Operational Status: In addition to the confidential sources used, three potential new sources are under assessment. Twenty-one conventional sources and thirteen liaison sources are contacted on a regular basis. The Quarterly Progress Briefing, scheduled for 15 June 1974, was postponed until July 1974 because the Fort Ritchie Commander was not available.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Cdr USA Intel Agcy

22b Indef

(24)

3. ~~(C)~~ CANARY STONE: (OACSI Approval - 18 Jul 73)

a. Location: Dugway Proving Ground, UT.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Investigative data on potential sources.

e. Operational Status: Efforts continue to recruit confidential sources; at present eleven individuals are being assessed. An initial recruitment approach was made to one prospect during the period, but due to personal circumstances of the individual, recruitment could not be accomplished. Two of the CIRLs have been processed to the point where recruitment can be attempted in the next quarter. On 3 Jun 74, the PLO briefed COL Robert A. Shade, Commander, Dugway Proving Ground, on the status of the operation. The briefing was also attended by COL Eric H. Vieler, Commander, 115th MI Group, LTC Henry F. Kale, Security Officer, Dugway Proving Ground, and the SAIC, Fort Douglas Resident Office, 115th MI Group. COL Shade expressed his satisfaction with the progress of the ICIP. COL Shade retires on 1 Jul 74. LTC Andrew J. Armonstrong, who will serve as Acting Commander pending assignment of a new commander, will be briefed by LTC Kale and the CANARY STONE PLO on the ICIP early in the next quarter.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Colr, USA Intel Agcy

Indef

221

4. ~~(C)~~ (U) CANINE PLATE: (OACSI Approval - 18 Sep 73)

a. Location: Seneca Army Depot, Romulus, NY.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Investigative data on prospective sources.

e. Operational Status: Two conventional sources were recruited during the period and were given security training and general EEI. Two additional individuals are being assessed as potential sources; both have access to the Directorate for Special Weapons. The PLO presented the Quarterly Progress Briefing to COL Allen H. Light, Jr., Commander, Seneca Army Depot, on 21 Jun 74. The Commander expressed his satisfaction with the progress of the ICIP and reiterated his previous desires that the ICIP be conducted in such a way to not cause any embarrassment to the Army, specifically, he has cautioned the PLO to exercise care in the recruitment of any sources used in the operation. He expressed his confidence in the conduct of the ICIP thus far.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USA INTEL AGCY
AUTH Para 1-605 DOD 5200.1R

Cdr, USA Intel Agcy

DECLASSIFY ON: Indef

228

5. (U) CANTINA ARCH: (OACSI Approval - 12 Dec 73)

a. Location: US Army Air Defense Center and Fort Bliss (USAADCENFB), TX.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Investigative data on potential sources.

e. Operational Status: Three confidential sources were successfully recruited during the period. Two of the sources are in the Office of the Deputy Commandant for Combat and Training Developments and the third is in the Ballistic Missile Defense Department, both of which are on the prime targets list of the ICIP. An approach plan is being devised for a prospective source in the Emergency Operations Center. Two other individuals currently under assessment work in the Ballistic Missile Defense Department and the Telecommunications Center. The ICIP PLO briefed COL George M. Hamscher, Director of Security, USAADCENFB, on the status of CANTINA ARCH on 14 Jun 74. COL Hamscher has indicated a keen interest in the progress of the ICIP and is satisfied with the successful recruitment of sources during this period.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intel Agcy

229

6. ~~(S)~~ CANVAS TAX: (OACSI Approval - 8 Mar 74)

a. Location: Sierra Army Depot (SIAD), Herlong, CA.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Investigative data on prospective confidential sources.

e. Operational Status: The project has been delayed in its initial stages due to non-availability of a Project Liaison Officer. Pending arrival of the PLO, San Francisco Field Office personnel established liaison with the Commander of SIAD and his staff and also initiated spotting and assessment actions for potential confidential sources. At present, two individuals are under assessment and preliminary investigations are being conducted on them. The PLO arrived on station on 19 Jun 74 and considerable operational progress is expected during the next quarter.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intel Cgy

Incl 2

230

[redacted]

7. (U) ~~(C)~~ CANYON ROSTER: (OACSI Approval - 8 Mar 74)

a. Location: Umatilla Army Depot Activity, Hermiston, Oregon.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Investigative data on potential conventional and confidential sources.

e. Operational Status: Despite the absence of an established Resident Office at Umatilla or a PLO at the supported activity for the reporting period, considerable progress was made in establishing liaison contacts and spotting and assessing potential confidential sources. This has been accomplished by personnel from the Fort Lewis Field Office performing TDY trips to the Umatilla Army Depot. At present nineteen civilian employees of the Depot are under assessment. One CIRL has been approved for recruitment and a Lead Development Report has been submitted on a second one. The Commander, Fort Lewis Field Office, contacted LTC Harold Echols, Commander, Umatilla Army Depot, on 11 Jun 74, to arrange for the first Quarterly Progress Briefing. The Commander stated he desired a briefing later after the new PLO had sufficient time to become established. The PLO became operational on 30 Jun 74.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intel Agcy

DECLASSIFY ON: Indef

231

8. ~~(S)~~ (W) CENSUS TIME: (OACSI Approval - 5 Feb 74)

a. Location: Pentagon Telecommunications Center.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Investigative data on prospective sources.

e. Operational Status: One confidential source, assigned to the Operations Division, Pentagon Telecommunications Center (PTC), was recruited during the reporting period. This source is being trained by the PCO and appears to have excellent potential for covering the target. Two other individuals, assigned as Communications Relay Operators, are being assessed as potential confidential sources. Recruitment of either one or both of these sources will improve the coverage of the target area. The PTC Director is appreciative of the progress being made in the ICIP and his staff of security officials are completely cooperative.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Chf, USA Intel Agcy

Indiv

232

9. ~~(C)~~ (U) CENTAUR RACE: (OACSI Approval - 30 Jul 73)

a. Location: Ninth Infantry Division and Fort Lewis, WA.

b. Confidential Source Utilization: Three confidential sources were utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: A confidential source reported that a soldier assigned to the 9th AG Company, Fort Lewis, Washington, exhibited signs of affluence beyond the normal financial capacity of a soldier in his grade. A limited investigation is being conducted. No significant counter-intelligence information was developed during the period, and all indications are that anti-military/dissident activity has subsided to a low level.

e. Operational Status: Spotting and assessment of potential sources continues to be emphasized in an effort to improve the ICIP coverage. Three confidential sources were recruited during this period. In addition to these, twenty conventional sources are used, as well as six official liaison sources. Nine individuals currently are under assessment for use as conventional or confidential sources. The Fort Lewis Field Office Commander presented a quarterly progress briefing on 21 Jun 74 to BG McFadden, Asst Division Commander, 9th Infantry Division, Fort Lewis. COL Kenneth Koch, Chief of Staff, and LTC Roy Davis, AC of S, G2, 9th Inf Div, were also in attendance. The 9th Infantry Division Asst Commander and the AC of S, G2, are preparing to recommend to the Division Commander that CENTAUR RACE be terminated because of a lack of specific, identifiable targets.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intel Agcy

Indcl 2

233

10. (U) CENTAUR SALE: (OACSI Approval - 14 Dec 73)

a. Location: US Army Mobility Equipment Research and Development Center, Fort Belvoir, VA.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Investigative data on prospective sources.

e. Operational Status: Two conventional sources presently are being used in CENTAUR SALE who have access to all target areas. Three other individuals are in various stages of assessment as potential sources; two of the prospects are in the Countermine/Counterintrusion Department, the third is in the System Engineering & Computer Support Office, Computer Division. The PLO provided the Quarterly Progress Briefing on the ICIP to Mr. Leslie L. Askew, Security Officer, US Army Mobility Equipment Research and Development Center (MERDC), on 6 Jun 74. During the briefing, Special Agent Shawn M. Sandlin was introduced to Mr. Askew as the New PLO for the operation effective 1 Jul 74.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM-F01/PO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intel Agcy

Indef 3

234

11. (U) CENTAVO KID: (OACSI Approval - 18 Oct 73)

a. Location: Harry Diamond Laboratories, Washington, D.C.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: Not applicable.

d. Useful Information Obtained: Investigative data on potential sources.

e. Operational Status: A new PLO was appointed effective 14 Jun 74 due to the PCS of the present PLO. A series of thefts have occurred at the Adelphi, Maryland, Harry Diamond Laboratories (HDL) facility. The PLO provided some assistance to the Security Office and the Federal Bureau of Investigation (FBI) during its investigation. The results of the FBI investigation of the prime suspect were negative and no further action has been taken. Two individuals who are employed in the facilities are under assessment as potential confidential sources. The quarterly ICIP Progress Briefing was presented on 7 Jun 74 to the ICIP Coordinator and Security Officer, Mr. Alfred F. Schneder, and Mr. James H. Yeick, Asst Security Officer, HDL. The briefing was presented by the former PLO who introduced the new PLO to the HDL security staff at the time.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intel Agcy

Indef 2

235

12. (U) CENTRAL TAXI: (OACSI Approval - 16 Feb 72)

a. Location: Headquarters, US Army Electronics Command (ECOM), Fort Monmouth, New Jersey.

b. Confidential Source Utilization: One additional source was recruited, bringing the total utilized to five.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) An ECOM civilian employee regularly engages in foreign travel. This information was brought to the attention of the ICIP Coordinator purely as a matter of interest since the employee is not in violation of existing regulations and none of the travel has been made to a Soviet bloc country.

(2) Another ECOM employee was arrested on 3 May 74 on a federal misdemeanor for her part in alleged forgery of US Government checks by the US Secret Service in Newark, New Jersey. The federal authorities released the employee because of her cooperation and set bail at $1,000. The information was passed to the ICIP Coordinator who informed the Provost Marshal's O-fice and the CID. Removal of the individual's security clearance is pending.

e. Operational Status: A revised Operations Plan was submitted during the period which consolidated ICIP LANDLESS TIME with CENTRAL TAXI. The consolidation resulted from the closing of the ECOM Philadelphia Facility and its subsequent transfer to ECOM, Fort Monmouth, NJ. A new PLO assumed duties in May 74. In addition to the five confidential sources used in the ICIP, ten conventional sources are being used, and one prospective sources is under assessment. Target coverage by conventional sources has been expanded to cover the Avionics Laboratory, Comptroller Office, and the Directorate of Procurement and Production. The Fort Monmouth Field Office Commander presented the Quarterly Progress Report Briefing to LTC Richard O. Aamot, Chief, Security Officer, ECOM, on 4 June 1974. LTC Aamot stated that he is most pleased with the continuing progress and effectiveness of CENTRAL TAXI and the security support being provided to ECOM by the ICIP. All priority targets are covered by conventional sources or by confidential sources.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intelligence

DECLASSIFY ON: Indef 236

13. (U) CENTURY SQUAD: (OACSI Approval - 3 Oct 73)

a. Location: US Army Management Systems Support Agency (USAMSSA), the Pentagon, Washington, D.C.

b. Confidential Source Utilization: One confidential source was utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: The confidential source has been provided with training instruction during this period. Source works during non-duty hours and surfaced no information of a counterintelligence interest during the reporting period. Two additional individuals currently under assessment as prospective sources, are expected to be recruited during the next period. Both are in the Operations Division, USAMSSA; one is a Computer Operator, the other is a Computer Technician. Recruitment of either of these prospects will provide coverage of the primary target during regular duty hours.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intel Agcy

Incl 2

237

14. (U) (S) GONDOLA FLAG: (OACSI Approval - 22 Apr 74)

a. Location: US Army Electronic Proving Ground (USAEPG), Fort Huachuca, AZ.

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Limited investigative data on a potential source.

e. Operational Status: Initial implementation efforts in this ICIP to date have been expended in establishing liaison contacts at USAEPG and conducting spotting and assessments of individuals who have placement and access in one of the prime target areas. One employee in the Electromagnetic Branch, USAEPG, is currently under assessment. Acquisition of several conventional sources is expected in the next quarter. The Commander, USAEPG, COL E. D. Downing, was provided the implementation briefing on GONDOLA FLAG on 7 May 74.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intel Agcy

DECLASSIFY ON: Indef 2

238

15. (U) GONDOLA STAR: (OACSI Approval - 17 Feb 72)

a. Location: Aberdeen Proving Ground (APG), MD.

b. Confidential Source Utilization: Two sources were used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) A confidential source reported the possibility that classified information may have been compromised by having been published in an unclassified publication. A follow-up report established that the information was not classified.

(2) A conventional source reported that a civilian employee of the Behavioral Research Directorate, Human Engineering Laboratory (HEL), Aberdeen Proving Ground, had some foreign professional contacts made in the line of duty. No unusual activity was reported; however, the situation is being monitored for unusual activity or interests.

(3) A confidential source surfaced the possibility that APG contractors were receiving unauthorized information pertaining to contracts being processed by the APG Procurement Directorate. Subsequent checks with APG authorities disclosed that the information being disclosed was not only authorized, but it was in fact required to be disseminated by regulation.

e. Operational Status: Three conventional sources are presently under assessment as potential new sources to expand and improve the target coverage in this ICIP. the PLO has established several worthwhile contacts in the Ballistics Research Laboratory (BRL) and make the presence of MI better known in this key target facility. No basic change in priority for ICIP coverage occurred in this current quarter, but coverage of the US Army Materiel Systems Analysis Agency (AMSAA) will receive greater emphasis in the next quarter. On 20 Jun 74, COL Walter R. Harris, Commander, APG, and Mr. Harry A. Mencke, Installation Intelligence Officer (IIO), APG, were given the Quarterly Progress Briefing on GONDOLA STAR. Both the APG Commander and the APG IIO expressed strong and continuing interest in the ICIP and pledged their full support and cooperation.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Cdr, USA Intel Agcy

239

(U)

16. ~~(C)~~ GONG SILK: (OACSI Approval - 16 Feb 72)

a. Location: Picatinny Arsenal (PA), Dover, NJ.

b. Confidential Source Utilization: Three confidential sources were used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: A confidential source reported suitability information concerning two PA employees who were allegedly emotionally unstable and had bad tempers. Security officials at PA took appropriate action following the incidents. Another source reported that two employees at PA were engaged in selling stolen merchandise. Initial information, in the form of hearsay, was too fragmentary; attempts are being made to obtain further details. As part of the effort to respond to EEI on Extremist Threat Against the US Army, PA Security Office records were examined to identify PA employees born in Arabian countries. Biographical data on four such employees was submitted in Agent Reports which were placed in appropriate dossiers of the individuals. The files search revealed nothing indicating connections with any known extremist activity.

e. Operational Status: In addition to the three confidential sources, 11 conventional sources are being met on a regular basis. Spotting and assessing activities, held in abeyance during April and May until PA employees had received Reduction in Force (RIF) notices, has now been resumed. In the course of the RIF 418 positions were deleted, and 1,700 employees were affected. The PA Security Office has been changing its manual document security procedures to the Controlled Accountable Document Inventory System (CADIS), a computerized system of accountability. The 109th MI Group Security Assistance Program representative and the PLO provided considerable assistance to PA in its preparation for CADIS. On 3 Jun 74, the Quarterly Progress Briefing was presented by the PLO to MAJ George A. Carpenter, Chief, Security Office, PA, and Mr. John R. Greffe, Asst Chief of the PA Security Office.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DA AR 380-5

Cdr, USA Intel Agy

Incl 2

Page 1738 of 3957

17. (U) LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute, East Coast Branch (DLIEC), Anacostia Naval Annex, Washington, D.C.

b. Confidential Source Utilization: None. Coverage is provided by conventional sources.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Local Agency Checks and additional biographic information was submitted on eight instructors of Arabic origin. The information is submitted in response to requirements of a USAINTC program concerning extremist threats against the Army.

e. Operational Status: DLIEC will begin movement to the Presidio of Monterey, CA, in July 1974. Permanent instructors are being offered an opportunity to relocate if they so desire; however, there has been no movement schedule established. Classes in session will continue at DLIEC until they graduate, attenuating the move over the next year. The move will be completed by 1 Jul 75. Information pertaining to instructors of DLIEC will be transferred to the PLO of the ICIP at DLIEC as the instructors transfer to the new location. On 3 Jun 74, the PLO briefed LTC Matthew T. Hendrickson, Commandant, DLIEC, providing the Quarterly Progress Briefing. No problems exist at this time and the Commandant expressed his satisfaction with the ICIP.

DECLASSIFIED UNCLASSIFIED
BY OSD/ USAINSCOM 97-01/PO
AUTH Para 1-603 DOD 5200.1R
SEP 5 1997

Cdr, USA Intel Agency

241

18. (U) LENIENT CLOUD: (OACSI Approval - 16 Feb 72)

a. Location: US Army War College (USAWC), Carlisle Barracks, PA.

b. Confidential Source Utilization: Three sources used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: The investigation concerning the financial activities of the captain reported during the last quarter has been completed except for a subject interview. The officer was assigned to less sensitive duties on 6 May 74 and will be transferred to Indiantown Gap Military Reservation in Jul 74. A limited investigation was conducted on a soldier assigned to Carlisle Barracks for reported use of narcotics.

e. Operational Status: In addition to the three confidential sources used in the operation, 35 conventional sources are contacted on a recurring basis. Target research provided to the Security Manager, USAWC, was sufficient justification for assignment of two full-time Military Police sentinels in Root Hall, an aid toward accomplishing a completely restricted access to the USAWC. Research is continuing on the best ways of restricting movement within Root Hall, to include surveys of electronic and mechanical equipment. Use of such equipment and reconfiguration of Root Hall is planned for Fiscal Year 1975. The PLO assisted in the preparation of security directives relative to the USAWC Military Research Program (MRP) in which student officers travel to foreign countries to obtain information for their thesis. The PLO also coordinated with elements of the 902d MI Group concerning MRP travellers in respect to Army Regulation 381-15. The PLO gave a Quarterly Progress Briefing to MG Franklin M. Davis, Jr., Commandant, USAWC, on 7 Jun 74. MG Davis indicated that he was very enthusiastic with the support received from LENIENT CLOUD and also that he expected the in-coming USAWC Commandant, MG DeWitt Clinton Smith, would be as receptive toward continuation of the ICIP.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Chief, USA Intel Agency

242

19. (U) LENTIL MONKEY: (OACSI Approval 26 Oct 71)

a. Location: Defense Language Institute West Coast (DLIWC), Presidio of Monterey, CA.

b. Confidential Source Utilization: Nine sources were utilized during the period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: A confidential source reported a May 74 incident involving an approach made to Czech language students on a picnic to engage in a pen-pal relationship with residents of Czechoslovokia. Details of this latest incident and previous incidents are being further investigated by the 902d MI Group and coordinated with the Federal Bureau of Investigation. An instructor in the Polish Language Department was visited by his brother, a Polish national, who also attended a picnic with students and instructors of the Polish Language Department. Further inquiries are underway with other Federal Agencies concerning the visitor. Verbal information given to the DLIWC Security Office concerning the homosexual activities of a student was used as a partial basis for separation action. Sources provided valuable background and biographic data on DLIWC instructors born in foreign countries which now have Communist Governments. This information is used to update target data files on instructors who might be potential targets of hostile intelligence.

e. Operational Status: Eleven conventional sources are currently used in the ICIP. During the quarter, five confidential sources were recruited while four were terminated because of their graduation. Source Lead and Development Reports have been prepared on two prospective sources and an additional seven new leads are undergoing initial investigation. The new recruitment efforts are being directed at Priority II Language Departments since present sources are located in Priority I language areas. The ICIP PLO presented the Quarterly Progress Briefing on 14 Jun 74 to COL John F. Hook, Commandant, DLIWC, MAJ Richard Erickson, Security Officer, DLIWC, and Mr. James R. Green, Asst Security Officer, DLIWC. COL Hook expressed his appreciation for the briefing and stated that he believed the Operation was achieving its objectives and had improved the security posture of DLIWC.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/RO
AUTH Para 1-603 DOD 5200.1R

CG, USA Intel Agcy

243

~~SECRET~~

ACTION SHEET

TROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) Operations

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 19 April 1974

ACTION REQUIRED: To obtain approval of the quarterly ICIP report.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By memorandum, dated 8 February 1972 (ORANGE TAB B), the Under Secretary of the Army requested the Vice Chief of Staff (VCSA), US Army, provide quarterly reports on all (ICIP) operations.

b. This is the eighth such quarterly report.

c. The quarterly report of current operations for the quarter ending 31 March 1974 is at (ORANGE TAB C).

2. DISCUSSION:

a. Inclosure 1 to ORANGE TAB A is a memorandum for the VCSA's signature forwarding the quarterly report to the Under Secretary of the Army.

b. ORANGE TAB A forwards to the VCSA the memorandum and ICIP Quarterly Report.

3. RECOMMENDATION: That the memorandum to the VCSA at ORANGE TAB A be approved and signed by the ACSI.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		23 APR 74
			DIV		23 APR 74
			DIR		23 APR 74
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

LTC STROM/77017

SPECIAL ACTIONS BR
RECORDS COPY

~~SECRET~~

ACSI FORM 28, 13 Sep 71

REGRADED
WHEN SEPARATED FROM CLASSIFIED
DOCUMENT

~~SECRET~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

REPLY TO ATTENTION OF: DAMI-DOI-S

26 APR 1974

MEMORANDUM FOR: VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above (Inclosure 2).

2. Recommend your approval and signature of the memorandum at Inclosure 1 which transmits the report required by the cited reference.

3. Coordination: None required.

2 Incl
as

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

30 APR 1974

APPROVED - VCSA

MICHAEL F. SPIGELMIRE
Major, GS
Assistant Secretary of
the General Staff

Regraded UNCLASSIFIED when separated from classified inclosures.

245

~~SECRET~~

LTC STROM/77017/jl

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, D.C. 20310

30 April 1974

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations (U)

1. (U) Reference is made to memorandum, Under Secretary of the Army, dated 8 February 1972, subject as above.

2. (U) The seventeen Internal Counterintelligence Program (ICIP) Operations reported by memorandum to you last quarter remain active. Three new operations submitted during the quarter covered by this report have been reviewed at DA and approved for implementation. The list of current operations and narrative summary for the quarter ending 31 March 1974 are attached. Adjustments to ICIP operations will be made in the next quarterly report to conform with Army reorganization.

3. (C) The primary value of ICIP operations is in their potential for early warning and detecting internal security weakness and security threats to the supported command. Inasmuch as these operations are a form of intensified security watchfulness, negative reports in themselves are frequently of value to a commander in planning for security requirements of a given installation or activity.

2 Incl
as

FRED C. WEYAND
General, United States Army
Vice Chief of Staff

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DAMI-DO
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 1980

246

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

CURRENT ICIP OPERATIONS

LOCATION	ICIP NICKNAME	DATE APPROVED	CONVENTIONAL SOURCES	CONFIDENTIAL SOURCES
Edgewood Arsenal, Maryland	CANAL LOOP	16 Feb 72	0	5
Fort Huachuca, Arizona	CANAL ROPE	17 Dec 73	0	0
Fort Ritchie, Maryland	CANARY EFFORT	16 Feb 72	18	3
Dugway Proving Ground, Utah	CANARY STONE	18 Jul 73	0	0
Seneca Army Depot, New York	CANINE PLATE	18 Sep 73	0	0
Fort Bliss, Texas	CANTINA ARCH	12 Dec 73	0	0
Sierra Army Depot, Herlong, CA	CANVAS TAX	8 Mar 74	0	0
Umatilla Army Depot, Hermiston, OR	CANYON ROSTER	8 Mar 74	0	0
Telecom Center, Pentagon	CENSUS TIME	5 Feb 74	0	0
Fort Lewis, Washington	CENTAUR RACE	30 Jul 73	26	0
Fort Belvoir, Virginia	CENTAUR SALE	14 Dec 73	0	0
Harry Diamond Lab, Washington, DC	CENTAVO KID	18 Oct 73	0	0
Fort Monmouth, New Jersey	CENTRAL TAXI	16 Feb 72	9	4

Classified by DAMI-ISC
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 1980

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

CURRENT ICIP OPERATIONS (cont)

LOCATION		ICIP NICKNAME	DATE APPROVED	CONVENTIONAL SOURCES	CONFIDENTIAL SOURCES
Mgmt Sys Spt Agency, Pentagon		CENTURY SQUAD	3 Oct 73	0	1
Aberdeen Proving Grounds, Maryland		GONDOLA STAR	16 Feb 72	0	2
Picatinny Arsenal, New Jersey		GONG SILK	16 Feb 72	11	2
Electronics Command, Philadelphia, PA		LANDLESS TIME	19 Jan 72	0	1
Defense Language Institute Washington, DC		LANYARD MOOD	22 Dec 71	1	0
Army War College, Carlisle Barracks, PA		LENIENT CLOUD	16 Feb 72	2	4
Defense Language Institute Presidio of Monterey, CA		LENTIL MONKEY	26 Oct 71	11	4
TOTALS	20	20		78	26

* Conventional sources are those on-post sources which are met overtly and from which information of a counterintelligence nature is elicited.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

ICIP Narrative Summary

There were no instances in which information on non-affiliated civilians was collected off post.

Progress in the development of information of counterintelligence value is slow. All significant reporting during the quarter has come about through the use of confidential sources with critical placement and access; however, to date, only 10 of the 20 ICIPs have confidential sources of information. Guidance has been provided the Intelligence field units to upgrade their efforts in the recruitment of confidential sources. The USAINTC has placed increased efforts on the use of conventional source contact by the Army counterintelligence units servicing installations not employing formal ICIPs. This effort may provide indications that such ICIP operations are warranted on the posts or installations. Emphasis on acquiring such conventional installation sources has been placed at Forts Rucker, Sheridan, Sill, Polk, Sam Houston, and McClellan.

Information of counterintelligence value developed during the 1st quarter of CY 74 came from six of the 20 counterintelligence programs in operation. The significant information was concerned primarily with adverse suitability and weaknesses in security practices. Typical of the information developed is that uncovered in the following two operations. Operation CANARY EFFORT developed information of adverse suitability on an Army captain, who eventually offered to resign from the Army and similar information on a Military Police investigator who subsequently was reassigned less sensitive duties. Adverse suitability information considered of lesser significance was reported on 17 other individuals assigned to the Communications Command, Ft. Ritichie, Md. Thirteen of these US Army personnel were involved in drug related activity. Operation CENTRAL TAXI revealed information concerning a highly placed employee in contact with foreign export companies, some of which are located within the Soviet Bloc. Poor security practices in several other instances at the Electronics Command have been brought to the attention of the Chief of Security, Ft. Monmouth.

Progress has been made in simplifying the procedural steps which must be followed to implement an ICIP operation. The establishment of an umbrella or basic OPLAN which precludes the preparation of lengthy separate plans at the unit level was approved by OACSI. This action was considered appropriate as all ICIP plans have sufficient common elements to permit utilization of a single basic plan. Operations plans will, in the future, be "fleshed out" by appropriate detailed annexes. This procedural change will significantly reduce the time from requestor to the time when the approved plan can be implemented.

The Army reorganization has caused two ICIPs to be combined with existing ICIPs. At the end of the reporting period, there was a total of 20 operations including one pending approval. It is planned that two additional

Page 1747 of 3957

ICIP plans will be submitted for approval during the second quarter 1974.

Supported commanders continue to express their support for the program and their satisfaction with the results. The ICIP operations will be continued for their original stated purposes.

250

Page 1748 of 3957

~~CONFIDENTIAL~~

CURRENT ICIP OPERATIONS

LOCATION	ICIP NICKNAME	DATE APPROVED	*CONVENTIONAL SOURCES	CONFIDENTI SOURCES
Edgewood Arsenal, Maryland	CANAL LOOP	16 Feb 72	0	5
Fort Huachuca, Arizona	CANAL ROPE	17 Dec 73	0	0
Fort Ritchie, Maryland	CANARY EFFORT	16 Feb 72	18	3
Dugway Proving Ground, Utah	CANARY STONE	18 Jul 73	0	0
Seneca Army Depot, New York	CANINE PLATE	18 Sep 73	0	0
Fort Bliss, Texas	CANTINA ARCH	12 Dec 73	0	0
Sierra Army Depot, Herlong, CA	CANVAS TAX	8 Mar 74	0	0
Umatilla Army Depot, Hermiston, OR	CANYON ROSTER	8 Mar 74	0	0
Telecom Center, Pentagon	CENSUS TIME	5 Feb 74	0	0
Fort Lewis, Washington	CENTAUR RACE	30 Jul 73	26	0
Fort Belvoir, Virginia	CENTAUR SALE	14 Dec 73	0	0
Harry Diamond Lab, Washington, DC	CENTAVO KID	18 Oct 73	0	0
Fort Monmouth, New Jersey	CENTRAL TAXI	16 Feb 72	9	4

Classified by DAMI-DO
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 1980

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R
251

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

CURRENT ICIP OPERATIONS (cont)

LOCATION	ICIP NICKNAME	DATE APPROVED	CONVENTIONAL SOURCES	CONFIDENTIAL SOURCES
Mgmt Sys Spt Agency, Pentagon	CENTURY SQUAD	3 Oct 73	0	1
Aberdeen Proving Grounds, Maryland	GONDOLA STAR	16 Feb 72	0	2
Picatinny Arsenal, New Jersey	GONG SILK	16 Feb 72	11	2
Electronics Command, Philadelphia, PA	LANDLESS TIME	19 Jan 72	0	1
Defense Language Institute Washington, DC	LANYARD MOOD	22 Dec 71	1	0
Army War College, Carlisle Barracks, PA	LENIENT CLOUD	16 Feb 72	2	4
Defense Language Institute Presidio of Monterey, CA	LENTIL MONKEY	26 Oct 71	11	4
TOTALS 20	20		78	26

* Conventional sources are those on-post sources which are met overtly and from which information of a counterintelligence nature is elicited.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM-OJI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

ICIP Narrative Summary

There were no instances in which information on non-affiliated civilians was collected off post.

Progress in the development of information of counterintelligence value is slow. All significant reporting during the quarter has come about through the use of confidential sources with critical placement and access; however, to date, only 10 of the 20 ICIPs have confidential sources of information. Guidance has been provided the Intelligence field units to upgrade their efforts in the recruitment of confidential sources. The USAINTC has placed increased efforts on the use of conventional source contact by the Army counterintelligence units servicing installations not employing formal ICIPs. This effort may provide indications that such ICIP operations are warranted on the posts or installations. Emphasis on acquiring such conventional installation sources has been placed at Forts Rucker, Sheridan, Sill, Polk, Sam Houston, and McClellan.

Information of counterintelligence value developed during the 1st quarter of CY 74 came from six of the 20 counterintelligence programs in operation. The significant information was concerned primarily with adverse suitability and weaknesses in security practices. Typical of the information developed is that uncovered in the following two operations. Operation CANARY EFFORT developed information of adverse suitability on an Army captain, who eventually offered to resign from the Army and similar information on a Military Police investigator who subsequently was reassigned less sensitive duties. Adverse suitability information considered of lesser significance was reported on 17 other individuals assigned to the Communications Command, Ft. Ritichie, Md. Thirteen of these US Army personnel were involved in drug related activity. Operation CENTRAL TAXI revealed information concerning a highly placed employee in contact with foreign export companies, some of which are located within the Soviet Bloc. Poor security practices in several other instances at the Electronics Command have been brought to the attention of the Chief of Security, Ft. Monmouth.

Progress has been made in simplifying the procedural steps which must be followed to implement an ICIP operation. The establishment of an umbrella or basic OPLAN which precludes the preparation of lengthy separate plans at the unit level was approved by OACSI. This action was considered appropriate as all ICIP plans have sufficient common elements to permit utilization of a single basic plan. Operations plans will, in the future, be "fleshed out" by appropriate detailed annexes. This procedural change will significantly reduce the time from requestor to the time when the approved plan can be implemented.

The Army reorganization has caused two ICIPs to be combined with existing ICIPs. At the end of the reporting period, there was a total of 20 operations including one pending approval. It is planned that two additional

Page 1751 of 3957

ICIP plans will be submitted for approval during the second quarter 1974.

Supported commanders continue to express their support for the program and their satisfaction with the results. The ICIP operations will be continued for their original stated purposes.

254

Page 1752 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U S ARMY INTELLIGENCE COMMAND
FORT MEADE, MARYLAND 20755

10 APR 1974

ICDO-OP

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOI-S)
WASH DC 20310

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

1. (C) Progress in the ICIP continued during the first quarter of CY 1974. The accession rate dropped from six requests in the previous quarter to three for the reported quarter. However, additional requests are anticipated during the next reporting period. In addition, Installation Source Programs are being established at appropriate locations and may result in changes to ICIP operations if significant information is developed. These operations have been established at Forts Rucker, Sheridan, Polk, Sill, Sam Houston and McClellan.

2. (C) Much of the credit for the significant information developed can be attributed to the increased use of Conventional Sources to supplement the coverage provided by Confidential Sources. A large percentage of the sources mentioned as being under assessment in the inclosures will be initially recruited as Conventional Sources controlled by the Project Liaison Officers. When their training has progressed to the point where their reliability is established and their production becomes substantial, they can be transferred to confidential status under the control of Project Case Officers. This approach is expected to increase the quantity and quality of production in established operations. A monthly operational status report system was initiated during the quarter which will provide a continuing overview to insure that each operation is productive in relation to the manhours and funds expended and is not being continued merely for the sake of having an operation on the books.

3. (C) Difficulties are being experienced in the implementation of the approved operations at Sierra and Umatilla Army Depots. Their isolated locations require that a Project Liaison Officer be stationed at each. Two volunteer CWOs were found among the assets of the 115th MI Group, but OPO disapproved their contemplated assignment because both were nearing 20 years service and were not to be retained on duty. Emergency requisitions are at MI Branch, and a candidate for Sierra has been nominated

~~CONFIDENTIAL~~

255

Classified by Cdr USAINTC
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

ICDO-OP
SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

to arrive o/a 15 June 1974. The status of the Umatilla fill is not known. In the meantime, the MI presence is manifested by regular TDY visits to each installation. Individual inclosures were therefore not prepared on these installations.

4. (U) The inclosures on CANAL LOOP and LANDLESS TIME are submitted for the last time. These operations are being absorbed into GONDOLA STAR and CENTRAL TAXI as a result to Army reorganization. In the case of CANAL LOOP, administration and management will be simplified. At the end of the reporting period, there was a net gain of two for a total of 19 operations, including the Electronic Proving Ground, Fort Huachuca, which is pending approval. There are two known gains during the second quarter of CY 74, not including any operations which will be generated as a result of the proposed letter by the CG, US Army Communications Command - CONUS, which is addressed in the CANARY EFFORT inclosure.

FOR THE COMMANDER:

18 Incl
as

JESSE D. JOY, JR.
Colonel, GS
Deputy Chief of Staff, Operations

REGRADED UNCLASSIFIED
ON SEP 5 1997
IAW DOD 5200.1R

256

~~CONFIDENTIAL~~
~~USAINSCOM~~

1. (U) CANAL LOOP: (OACSI Approval - 16 Feb 72)

a. Location: Edgewood Arsenal, Edgewood, MD

b. Confidential Source Utilization: Five sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: Sources provided additional leads on b6 USAR officer, which will be utilized in the limited investigation now underway.

e. Operational Status: Three additional sources are under assessment, and emphasis was placed on increasing contact with official sources during the reporting period. A study of targets covered under this operation was made by the Installation Intelligence Officer, Aberdeen Proving Ground, the Chief of Security, Edgewood, and the Project Liaison Officer. It was agreed that all current targets have the highest priority under the ICIP. A reviewed OPLAN is being prepared to consolidate the operations at Edgewood and Aberdeen. This will relieve the administrative burden of reporting on two separate operations, and is logical since the two posts are considered as a single entity.

Gordon A STAR
in the AP6 opn.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ...Cdr USAINSCOM...
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY ...2...
DECLASSIFY ON ...Exempt...

257

~~CONFIDENTIAL~~

Incl 1

~~CONFIDENTIAL~~

2. (U) CANAL ROPE: (OACSI Approval - 17 Dec 73)

a. Location: Headquarters, US Army Communications Command and 11th Signal Group, Ft Huachuca, AZ

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: Not applicable

d. Useful Information Obtained: Investigative data on potential sources.

e. Operational Status: The recruitment of two sources in the 11th Signal Gp Crypto Facility, the primary concern of the ACofS, Intelligence and Security, will be accomplished upon the receipt of NAC results. A source is under assessment in the Communications-Electronics Engineering Installation Agency. COL Vega, the ACofS, IS, is pleased with the support rendered to date.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPO
AUTH Para 1-603 DOD 5200.1R

Classified by ...Cdr USAINSCOM.....
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2.....
DECLASSIFY ON ...Graduate.....

258

~~CONFIDENTIAL~~

Incl 2

~~CONFIDENTIAL~~

3. (U) CANARY EFFORT: (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three sources were used during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Adverse suitability information was developed on a Military Police investigator and resulted in his relief from investigative duties and assignment to less sensitive duties. A request for an investigation was forwarded to USAINTC. Similar information was developed on a US Army Captain being considered for sensitive duties in the Alternate Joint Communications Center (AJCC). Prior to the submission of a request for investigation to USAINTC, the officer became involved with law enforcement agencies and, after counseling, offered to resign from the Army. Information on drug abuse related incidents involving 13 US Army personnel was developed, and passed to the ICIP Coordinator. This is a decrease in the number of incidents from the previous quarter, and the Post Commander and ICIP Coordinator credit the ICIP operation and increased liaison between the Project Liaison Officer and the Provost Marshal with contributing to the decrease. The CG and C/S of US Army Communications Command-CONUS were also given an ICIP briefing during the period. BG Redman advised that he had been made aware of the achievements of the ICIP at Fort Ritchie and was planning to request coverage of sensitive installations within his command. Additional details are contained in the attached Quarterly Progress Report (ANNEX A).

e. Operational Status: In addition to the Confidential Sources, contact was maintained with 18 casual and nine liaison sources during the period. The favorable attitude of the Commander and the ICIP Coordinator are reflected in attachment.

1 Incl
as

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ..... CdrUSAINTC .....
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2 .....
DECLASSIFY ON ..... Indefinite .....

259

~~CONFIDENTIAL~~

Incl 3

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
Fort Ritchie Field Office
109th Military Intelligence Group
Fort Ritchie, Maryland 21719

ICGP-B-FR

29 March 1974

QUARTERLY PROGRESS REPORT NUMBER 2

Period January 1974 thru March 1974

"WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED"

SUBJECT: Operation CANARY EFFORT (U)

1. (U) CIRCUMSTANCES:

a. On 25 February 1974, the US Army Intelligence Command (USAINTC) Internal Counterintelligence Program (ICIP) Briefing was presented to BG Albert Redman, Jr., Commander, US Army Communications Command - CONUS and Mr. Kenneth L. Alexander, DAC, GS-14, Chief of Staff, US Army Communications Command - CONUS, Fort Ritchie. The aforementioned briefing, presented by the Project Liaison Officer (PLO), Operation CANARY EFFORT, was enthusiastically received by BG Redman and Mr. Alexander. Both BG Redman and Mr. Alexander were knowledgeable that an ICIP was in effect at Fort Ritchie and indicated that the ICIP had received many laudable comments. BG Redman indicated a desire to have the ICIP program expanded to include sensitive installations within his command. The following personnel were in attendance at the aforementioned briefing:

BG Albert Redman, Jr., Commander, US Army Communications Command - CONUS, Fort Ritchie.

Mr. Kenneth L. Alexander, DAC, GS-14, Chief of Staff, US Army Communications Command - CONUS, Fort Ritchie.

Mr. Joseph J. Carroll, DAC, GS-14, Assistant Chief of Staff, Intelligence and Security, US Army Communications Command - CONUS and Headquarters, Fort Ritchie.

MAJ Robert L. Brooks, MI, Commander, Fort Ritchie Field Office, 109th Military Intelligence Group, Fort Ritchie.

b. A formal briefing, per se, was not presented during the reporting period of 15 October 1973 to 15 December 1973. The Quarterly Progress Briefing presented on 29 March 1974, included the aforementioned period as well as the period of January 1974 thru March 1974. The Quarterly Progress Briefing was presented on 29 March 1974 at the request of COL James A. Manning, Commander, Fort Ritchie, as COL Manning felt the briefing should be presented at the end of the reporting period

260

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Cdr., 109th MI Group
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 4
DECLASSIFY ON cannot be determined

~~CONFIDENTIAL~~

IOGP-B-FR
SUBJECT: Operation CANARY EFFORT (U) 29 March 1974

as opposed to 15 March 1974, as stipulated by existing USAINTC regulations. Although the formal briefing was presented on 29 March 1974, continual/constant liaison was maintained with appropriate individuals briefed on the ICIP prior to the formal briefing. The following briefed personnel were present on 29 March 1974, at which time the Quarterly Progress Briefing was presented:

COL James A. Manning, b6 Armor, Commander, Fort Ritchie.

COL Harold G. de Moya, b6 Infantry, Deputy Commander, Fort Ritchie.

LTC Arlyn R. Madsen, b6 Signal Corps, Director, Telecommunications Directorate, Fort Ritchie.

Mr. Joseph J. Carroll, DAC, GS-14, Assistant Chief of Staff, Intelligence and Security, US Army Communications Command - CONUS and Headquarters, Fort Ritchie. Mr. Carroll is the ICIP Coordinator, Operation CANARY EFFORT.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. During reporting period, Spotting and Assessment for Confidential Sources with placement and access continued.

b. Daily liaison was maintained with the Assistant Chief of Staff, Intelligence and Security, US Army Communications Command - CONUS and Headquarters, Fort Ritchie and/or a briefed member of the aforementioned office.

c. Periodic, if not daily, liaison was maintained with 16 individuals assigned key positions within the Fort Ritchie military community. Aforementioned individuals, considered Casual/Official Sources, include the Director, Telecommunications Directorate, the Provost Marshal, Military Police Investigations, Company Commanders, and other appropriate personnel.

d. Periodic/continual liaison was maintained with appropriate federal, state and local agencies.

e. During reporting period a total of 31 Agent Reports were submitted concerning 19 individuals assigned to Fort Ritchie occupying either sensitive positions and/or having security clearances. The aforementioned Agent Reports forwarded adverse suitability information.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

261

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICGP-B-FR
SUBJECT: Operation CANARY EFFORT (U) 29 March 1974

f. On 4 January 1974, a draft letter was prepared for the Assistant Chief of Staff, Intelligence and Security, US Army Communications Command - CONUS and Headquarters, Fort Ritchie, to be used by the aforementioned individual/office in requesting expansion of the ICIP within the US Army Communications Command - CONUS. The aforementioned letter (draft) was well received and appropriate staffing was initiated. On 26 March 1974, COL Antonio Vega, GS, Assistant Chief of Staff, Intelligence and Security, US Army Communications Command, Fort Huachuca, Arizona, discussed proposed ICIP expansion with Mr. Carroll and indicated strong interest in the proposal. COL Vega reportedly informed Mr. Carroll that the letter from Fort Ritchie would be enthusiastically received at Fort Huachuca and that COL Vega would recommend that the request for ICIP expansion be approved and forwarded, in the form of a formal request, to the Office of the Assistant Chief of Staff for Intelligence, Department of the Army. Mr. Carroll indicated to undersigned PLO that the aforementioned letter would leave Fort Ritchie by 8 April 1974.

g. Upon termination of the Quarterly Progress Briefing, 29 March 1974, COL Manning and Mr. Carroll expressed their appreciation and enthusiasm for the ICIP at Fort Ritchie. Comments for accomplishments rendered during the reporting period were laudatory, to say the least. COL Manning indicated his desire to continue the ICIP at Fort Ritchie as he believed it's contribution toward enhancing the security posture of Fort Ritchie and the Alternate Joint Communications Center (AJCC) was invaluable. Both COL Manning and Mr. Carroll desired that the existing ICIP at Fort Ritchie continue "uninterrupted" despite any reorganizational changes anticipated by USAINTC. Mr. Carroll stated that he did not desire to see any personnel changes in as far as the PLO was concerned as he was "immensily satisfied" with the present PLO both professionally and personally. Mr. Carroll added, that for the first time since his assignment to Fort Ritchie in 1971, he was totally satisfied with the ICIP in it's entirety.

h. COL Manning and Mr. Carroll further expressed their appreciation of SAEDA briefings presented to a total of 583 personnel, both military and civilian, on 28 March 1974, by the PLO.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

a. As previously stated, a total of 31 Agent Reports (DA Form 341) were submitted concerning 19 individuals, US Army personnel, assigned to the US Army Communications Command - CONUS and Fort Ritchie. Aforementioned Agent Reports, submitted by the PLO, forwarded adverse suitability information. Of the aforementioned 31 Agent Reports, a total of 15 Agent Reports were submitted concerning 13 US Army personnel involved in drug abuse related incidents. A total of 17 Agent Reports concerning five US Army personnel were submitted in regard to adverse suitability information.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1760 of 3957

~~CONFIDENTIAL~~

ICGP-B-FR
SUBJECT: Operation CANARY EFFORT (U) 29 March 1974

b. On 4 February 1974, PLO was notified of an alleged threat on the life of the Commander, 572d Military Police Company (Security), Fort Ritchie. The threat, in form of an alleged $10,000 "contract", was allegedly sponsored by either De Mau Mau or the Black Liberation Army. Contact was effected with appropriate military and civilian agencies and reported information was forwarded in form of a Spot Report as well as a follow-up Agent Report. Both COL Manning and Mr. Carroll expressed appreciation for the timely and effective manner in which the aforementioned incident was handled by the PLO.

c. In yet another case, adverse suitability information was surfaced concerning a former Military Police Investigator assigned to Fort Ritchie. The aforementioned individual was relieved of MPI duties and assigned less sensitive duties. Adverse suitability information was gleaned from official records and Official Sources and brought to the attention of Mr. Carroll. Mr. Carroll, in turn, requested an investigation of the individual from USAINTC.

d. In still another instance, adverse suitability information was surfaced concerning a US Army Captain who was being considered for a sensitive position both at Fort Ritchie and the AJCC. Adverse suitability information was gleaned from official records and Official Sources and brought to the attention of both COL Manning and Mr. Carroll. Prior to an investigation being requested by Mr. Carroll, the individual concerned again became involved with law enforcement agencies and, after counselling by COL Manning, offered to resign from the US Army. The aforementioned incident was particularly delicate as the individual concerned was a graduate of the US Military Academy and possessed a distinguished combat record in the Republic of Vietnam. COL Manning and Mr. Carroll both expressed complete satisfaction in the manner in which the PLO brought the adverse suitability information to their attention and concurred with PLO in recommendations offered.

e. While drug abuse, per se, is not within the investigative purview of USAINTC, the issue does involve suitability of the individuals concerned to hold security clearances and occupy sensitive positions. Upon recient of adverse information, immediate action was taken to notify the ICIP Coordinator, Operation CANARY EFFORT, Mr. Joseph J. Carroll; the Commander, Fort Ritchie; and the Director, Telecommunications Directorate, if applicable. In addition to the aforementioned, action was taken to disseminate information, criminal in nature, to the appropriate military and civilian authorities. COL Manning and Mr. Carroll both expressed satisfaction in the decrease of drug abuse related incidents during reporting period and voiced belief that the marked decrease was largely due to the enhanced liaison between the PLO and the Office of the Provost Marshal.

263

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICGP-B-FR
SUBJECT: Operation CANARY EFFORT (U) 29 March 1974

f. Information concerning both military and civilian personnel assigned to US Army Communications Command - CONUS and Fort Ritchie, and on whom Agent Reports have been submitted, by both the PLO and Project Case Officer (PCO), are duly reflected in Monthly Status Reports (MSR) for the months of February and March 1974. Paragraphs 2.e. and 3.a. of this report contain statistics concerning Agents Reports submitted only by the PLO.

g. Covert Sources within the CANARY EFFORT target area continue to report adverse suitability information concerning both US Army and Department of the Army personnel assigned to Fort Ritchie and the AJCC.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS:

a. It is strongly recommended that, in the event personnel changes are anticipated in the forthcoming reorganization, appropriate and responsible USAINTC personnel effect contact with COL Manning and/or Mr. Carroll prior to initiating such changes. If nothing else, the aforementioned recommended action should be accomplished as a "matter of courtesy".

b. PLO and PCO continue to enjoy an excellent professional and personal working relationship. PLO and PCO indeed work and function as a team. PLO continues to enjoy an excellent professional and personal working relationship with his counterparts, liaison contacts, and Casual/ Official Sources.

c. It is envisioned that,once the Fort Ritchie Field Office increases it's personnel strength, and once the administrative requirements levied on the PLO either diminish or stabilize, the PLO will become increasingly effective/productive and be permitted to support the supported commander in the manner intented by the ICIP, i. e. in the "true spirit" of the program. The ultimate goal of the ICIP and, hence, the PLO, is to afford the Commander, Fort Ritchie, with coverage desired, i. e., enhancement of the security posture of Fort Ritchie and the AJCC by means not locally available the Commander.

Gary L Peisen

GARY L. PEISEN
CW4, USA
Project Liaison Officer

REGRADED UNCLASSIFIED
SEP 5 1997
ON
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

264

~~CONFIDENTIAL~~

Page 1762 of 3957

[redacted]

4. (U) CANARY STONE: (OACSI Approval - 18 Jul 73)

a. Location: Dugway Proving Ground, UT

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: Not applicable

d. Useful Information Obtained: Investigative data on potential sources.

e. Operational Status: Deseret Test Center, the original organization, has been disestablished and the functions assumed by Dugway, necessitating a realignment of targets. The Project Liaison Officer has established excellent liaison with the Commander and Security Officer. As of the end of the reporting period, 12 potential sources with proper placement were under assessment. Production is expected during the next quarter.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ...Cdr USAINSCOM...
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY ...3...
DECLASSIFY ON ...Indefinite...

[redacted]

265

Incl 4

~~CONFIDENTIAL~~

(U) CANINE PLATE: (OACSI Approval - 18 Sep 73)

a. Location: Seneca Army Depot, Romulus, NY

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Limited investigative data on prospective sources.

e. Operational Status: This operation has been developing slowly at the specific desires of the commander. He has directed that no on-post record or file checks be conducted on potential sources for fear that they or the operation will be compromised. However, he has suggested that any prospective source approached who is in doubt of the Project Liaison Officer's bona fides be instructed to telephone him privately. Four potential sources have been identified and subjected to police and FBI checks, and will be recruited when favorable assessment is concluded.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ..... Cdr USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON ..... Indefinite

266

~~CONFIDENTIAL~~

Incl 5

~~CONFIDENTIAL~~

6. (U) CANTINA ARCH: (OACSI Approval - 12 Dec 73)

a. Location: US Army Air Defense Center and Ft Bliss, TX

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: Not applicable

d. Useful Information Obtained: Investigative data on potential sources.

e. Operational Status: Complete cooperation is being received from the DSEC, who is the ICIP Coordinator. Two sources are ready for recruitment and five are under assessment. Two were assessed and rejected because of suitability information developed. Production can be expected during the second quarter of CY 74. The DSEC is being kept abreast of developments and is satisfied with the progress to date.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Cdr USAINTC

267

~~CONFIDENTIAL~~

Incl 6

7. (U) CENSUS TIME: (OACSI Approval - 5 Feb 74)

a. Location: Pentagon Telecommunications Center

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: Not applicable

d. Useful Information Obtained: Investigative data on prospective sources.

e. Operational Status: This operation has not been completely implemented due to the lack of recruited sources. Two are currently under assessment and, if acceptable or amenable to recruitment, should begin to provide information during the coming quarter. The Director and his security officials continue to be completely cooperative and appreciative of the development of the operation.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ODRUSAINTC
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

268

Incl 7

[redacted]

8. (U) CENTAUR RACE: (OACSI Approval - 30 Jul 73)

a. Location: Ninth Infantry Division and Fort Lewis, WA

b. Confidential Source Utilization: None

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: A conventional source reported activity ~~by~~ on behalf the wife of SP4 b6 courtmartialed on 17 Jan 74 for illegal distribution of literature on post. (Agent Report attached at ANNEX A.) There were two instances of distribution of such literature on the post during the period reported on. The FBI continues to provide information on military personnel who engage in anti-military activity off-post.

e. Operational Status: b6 transferred to Leavenworth and then released from confinement and the service during the period, is allegedly returning to or already in Tacoma, WA. He is expected to continue his anti-military activities, but the FBI is in a position to provide continuing coverage. Both b6 and b6 are expected to assist b6 in his activities. Security officials at Fort Lewis indicate that this minor activity has no apparent affect on troop morale or efficiency. This is confirmed by contacts with 26 conventional sources during the period. Eighteen additional individuals are under assessment for use as either confidential or conventional sources. The civilian deputy to the G2 advised the CI Div, DCSI, FORSCOM, that he was pleased with what was being provided.

1 Incl
as

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ...Cdr USAINSC...
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF E[redacted]
EXEMPTION CATEGORY 2
DECLASSIFY ON ...Exempt...

[redacted] 269

Incl 8

AGENT REPORT

For use of this form, see FM 30-17(C); AR 381-130; the proponent agency is the Office of the Assistant Chief of Staff for Intelligence.

1. NAME OF SUBJECT OR TITLE OF INCIDENT	2. DATE SUBMITTED
ANTI-MILITARY/DISSIDENT ACTIVITIES Company A, 3/39th Inf, 9th Inf Div Fort Lewis, Washington	31 January 1974
	3. CONTROL SYMBOL OR FILE NUMBER

4. REPORT OF FINDINGS

(CASUAL SOURCE) On 31 January 1974, PFC b6 Company A, 3/39th Infantry, 9th Infantry Division, Fort Lewis, Washington, was interviewed by the undersigned, at the Fort Lewis Field Office, 115th Military Intelligence Group, Fort Lewis, regarding SUBJECT, and stated substantially as follows:

Two of b6 's friends, PVT b6 and PFC b6 b6, both members of the 3/39th Infantry, collected approximately $175.00 from Source's platoon on 31 January 1974. The money was collected for b6 's wife. A substantial number of persons in Company A, 3/39th Infantry are highly disgruntled with the US Army for the stiff sentence b6 received as a result of his recent court-martial at Fort Lewis.

AGENT'S NOTES: b6, a former member of Company A, 3/39th Infantry, Fort Lewis, was given a Special Court-Martial on 16 January 1974, for the unauthorized distribution of literature at Fort Lewis, Washington.

270

[redacted]

5. TYPED NAME AND ORGANIZATION OF SPECIAL AGENT	6. SIGNATURE OF SPECIAL AGENT
ROBERT T. JENKINS, 115th MI Gp (LE)	Robert T. Jenkins

DA FORM 1 APR 52 341 REPLACES WD AGO FORM 341, 1 JUN 47, WHICH MAY BE USED. ☆ GPO: 1970 390-807/248

[redacted]

9. (U) ~~(C)~~ CENTAUR SALE: (OACSI Approval - 14 Dec 73)

a. Location: US Army Mobility Equipment Research and Development Center, Ft Belvoir, VA

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: Not applicable

d. Useful Information Obtained: SSG [b6], mentioned in the previous report, went AWOL and was dropped from the rolls as a deserter. He was not reported as a Knowledgeable AWOL. A contractor employee was caught taking unauthorized photographs on post. Examination of the developed photos indicated nothing of security interest, and MERDC authorities plan no further action.

e. Operational Status: The relationship with MERDC security officials continues to be excellent. The Project Liaison Officer (PLO) has been hampered by having to function in the same capacity at Harry Diamond Laboratories (HDL). However, he has identified 10 prospective sources and appropriate checks are being conducted. A separate PLO will be assigned to HDL and will allow the CENTAUR SALE PLO to function full-time.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ..... Ads USAMTC .....
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY ..... 2 .....
DECLASSIFY ON ..... Indefinite .....

271

[redacted]

Inc 19

~~CONFIDENTIAL~~

10. (W) (C) CENTAVO KID: (OACSI Approval - 18 Oct 73)

a. Location: Harry Diamond Laboratories, Washington, DC

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: Not applicable

d. Useful Information Obtained: Agent Reports on an Israeli-born employee which satisfy requirements in a USAINTC program concerning extremist threats against the Army.

e. Operational Status: This operation has been somewhat hampered by the reluctance of the Security Officer to cooperate with the Project Liaison Officer (PLO). The PLO has been also required to function in that capacity for CENTAUR SALE. A separate PLO for CENTAVO KID has been assigned and documented with a security badge. By working with the more receptive Assistant Security Officer, who is expected to take over from his chief when the latter retires this year, it is hoped that progress will be made. The staff in the Personnel Office cooperate fully, so that identification and selection of potential sources should begin shortly.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM 1701/PO
AUTH Para 1-603 DOD 5200.1R

Classified by Cdr USAINTC
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

272

~~CONFIDENTIAL~~

Inc 1 10

[redacted]

11. (U) CENTRAL TAXI: (OACSI Approval - 16 Feb 72)

a. Location: Headquarters, US Army Electronics Command, Ft Monmouth, NJ

b. Confidential Source Utilization: One additional source was recruited, bringing the total utilized to four.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained:

(1) A civilian employee continues to drink to excess; the matter will be discussed with his supervisor by the ICIP Coordinator.

(2) Another employee is in contact with foreign export companies, but the fact that some are in the Soviet Bloc has heretofore been unknown to ECOM officials. The coordinator has asked that sources be tasked to provide additional details.

(3) A civilian guard detailed to control access to a sensitive area has been absent from his post, allowing personnel to come and go with identification not checked. He has been transferred to other duties.

(4) A GS 15 scientist discussed SECRET information in a GSA cafeteria while on TDY. He will be counseled on proper security procedures, since he will soon host a visiting Japanese student and may inadvertently release unauthorized information. (See ANNEX A)

e. Operational Status: In addition to the confidential sources listed above, nine conventional sources were used during the period, two of whom contributed information on the guard and the talkative scientist. ECOM staff members continue to express appreciation for the information surfaced by the operation. LTC Richard O. Aamot, Chief, Security Office, and ICIP Coordinator, has announced his intention of expressing in writing his appreciation to personnel involved in the ICIP for their contributions to the security of ECOM. Additional details are contained in attached Quarterly Progress Report.

1 Incl
as

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

213

Classified by CDR USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

Incl 11

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
FORT MONMOUTH FIELD OFFICE
109TH MILITARY INTELLIGENCE GROUP
P. O. BOX 176, EATONTOWN, NEW JERSEY 07724

QUARTERLY PROGRESS REPORT NUMBER 16

Period: 10 December 1973 to 1 March 1974

WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED — 7 MAR 1974

SUBJECT: CENTRAL TAXI (U)

1. (U) CIRCUMSTANCES:

On 4 March 1974, Quarterly Progress Report Number 16 was presented orally to LTC Richard O. Aamot, Chief, Security Office, US Army Electronics Command (ECOM), Fort Monmouth, New Jersey, in LTC Aamot's office; no others were present.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. The prospective confidential source mentioned in Quarterly Progress Report Number 15 (IC-B-075) was recruited by the PCO on 10 January 1974. (See CR-001-109-MON, Subject: IC-B-075, dated 16 January 1974).

b. The name of the program has been changed from the Counterintelligence Screening Program (CISP) to the Internal Counterintelligence Program (ICIP).

c. Emphasis continues on spotting, assessing and recruiting conventional sources. During the reporting period, the PLO recruited six additional conventional sources. A total of nine conventional sources have been recruited since November 1973, when the new conventional source program was implemented. The PLO is in the process of spotting and assessing four new conventional sources.

d. The PLO has been alerted by DA that he will be transferred to USAREUR. Hopefully, a new PLO will be on station prior to the undersigned's departure.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

a. On 9 January 1974, it was reported that Sherman Ray SHIELDS (see Quarterly Progress Report Number 15) continued to consume alcoholic beverages to excess. (CR-011-109-MON, Subject: IC-B-072, dated 15 January 1974).

b. On 9 January 1974, it was reported that b6 DAC, GS-12, b6 Electronics Devices Branch, Components Section, Production Engineering Division, Directorate of Research, Development and Engineering, ECOM, Fort Monmouth, New Jersey, was involved in foreign business transactions, to include transactions emanating from Soviet Bloc countries. (CR-011-109-MON, Subject: IC-B-072, dated 15 January 1974). Subsequent investigation re-

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

274

~~CONFIDENTIAL~~

CLASSIFIED BY: CDR USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS; NOT AUTOMATICALLY DECLASSIFIED

vealed that b6 had indicated on HIS latest Statement of Personal History that HE was involved in foreign business transactions, but failed to note HIS dealings with Soviet Bloc countries. Noteworthy is the fact that HIS mother, father and spouse were all born in Poland.

c. On 1 March 1974, information was received that John Randolph DICKERSON, Sr., DAC, GS-4, b6 a US Government Security Guard employed by ECOM was not carrying out HIS duties in a proper manner. DICKERSON had been observed for over a two-year period at HIS normal post at the entrance/exits to the Hexagon cafeteria. During this period, DICKERSON, who was supposed to be checking personnel for proper identification and clearance, was seen sleeping, wiping tables, working in the kitchen and operating the cafeteria cash register. (Agent Reports prepared by Jerome A. Britton, 109th MI Group, regarding DICKERSON, dated 1 March 1974.)

d. On 1 March 1974, information was received that b6 DAC, GS-15, b6 Chief, Laser Technical Area, Combat Surveillance & Target Acquisition Laboratory (CSTA), ECOM, Fort Monmouth, New Jersey, had taken a TDY trip to the Washington, D.C. area during the past 30 days. While in the Washington area, b6 accompanied by several others, went to an AMC cafeteria and began discussing sensitive SECRET information. It is unknown if uncleared personnel were able to listen to b6 's conversation. (Agent Reports prepared by Special Agent Jerome A. Britton, 109th MI Group, regarding b6 , dated 1 March 1974).

e. Information regarding b6 (see Quarterly Progress Report Number 15) was passed to the Fort Monmouth Resident Agency, USACIDC, for possible exploitation.

4. (U) ~~(C)~~ COMMENTS, REMARKS AND RECOMMENDATIONS:

a. Reference paragraphs 2a and 2c above: LTC Aamot expressed deep satisfaction with CENTRAL TAXI's progress, and urged that personnel involved in the program continue their aggressiveness.

b. Reference paragraph 3a above: LTC Aamot will talk to SHIELDS' supervisor.

c. Reference paragraph 3b above: LTC Aamot requested additional information regarding b6 as it is developed. Aamot already has briefed the ECOM Chief of Staff on b6 and would be most appreciative if we can surface additional details.

d. Reference paragraph 3c above: LTC Aamot advised the PLO that DICKERSON will be relieved from HIS post and transferred to another position with decreased responsibilities.

275

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

CONFIDENTIAL

e. Reference paragraph 3d above: LTC Aamot contacted the Director of the CSTA Laboratory and informed him that b6 had been overheard discussing SECRET information in an unauthorized area. Aamot will confront b6 with the same information, without being specific so as not to compromise our source. The Agent Report on b6 could be of more importance than superficially indicated because b6 is sponsoring a Japanese exchange scientist who only is cleared for access to CONFIDENTIAL material, and b6 is capable of inadvertently passing SECRET data to the Japanese scientist. The verbal counseling by Aamot should negate such an eventuality and result in increased security awareness on b6 's part.

f. Reference paragraphs 2c and 3c and 3d above: The Agent Reports on b6 b6 and DICKERSON were especially significant because they represent the first reporting by conventional sources since implementation of the conventional source program in November 1973. This data was obtained on just the second contact with the sources and indicates a very promising future for the overall program.

g. CENTRAL TAXI target coverage is presently as follows:

(1) Research, Development and Engineering Directorate: Confidential Sources IC-B-072 and IC-B-073.

(2) Directorate of Product Assurance: Confidential Source IC-B-074.

(3) Maintenance Directorate: Conventional Sources b7(d) and b7(d)

(4) Combat Surveillance and Target Acquisition Laboratory: Confidential Source IC-B-075 and Conventional Source b7(d).

(5) Electronics Technology and Devices Laboratory: Conventional Source b7(d)

(6) Electronic Warfare Laboratory: Conventional Sources b7(d), b7(d) and b7(d).

(7) Research and Development Technical Support Activity: Conventional Source b7(d).

(8) Directorate of Management Information Systems: Confidential Source IC-B-058, upon his transfer from ECOM/Philadelphia to Fort Monmouth.

(9) Communications/Automatic Data Processing Laboratory: Conventional Source b7(d).

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

276

CONFIDENTIAL

~~CONFIDENTIAL~~

h. Future plans relative to new target areas are to recruit sources in the following ECOM activities which are presently void of source coverage: Avionics Laboratory; Directorate of Procurement and Production; Directorate of Materiel Management, upon its relocation from Philadelphia to Fort Monmouth; Comptroller; and Directorate of Plans, Training and Force Development.

i. A total of 11 CENTRAL TAXI Agent Reports, consisting of 19 leads were prepared by the PCO and PLO during the reporting period.

JEROME A. BRITTON
CW3, USA
PLO, CENTRAL TAXI

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1775 of 3957

~~CONFIDENTIAL~~

12. (U) ~~(C)~~ CENTURY SQUAD: (OACSI Approval - 3 Oct 73)

a. Location: US Army Management Systems Support Agency, The Pentagon

b. Confidential Source Utilization: One source was recruited during the period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status: The source is still in the training phase, but can be expected to begin satisfying EEI during the next reporting period. Twenty-one prospective sources have been subjected to file reviews, LACs, NACs and assessment, and can be activated as required. The Director and the Security Manager continue to provide the cooperation necessary in the development of this operation. During the quarterly briefing, the Director stated that sensitive information discussed in his office was becoming common knowledge within the agency and felt that this information was either released by someone without authorization or that his office was technically monitored. He requested that a technical inspection of his office be provided, and was assured that an inspection would be conducted in the near future. A complete inspection was completed on 5 Apr 74 with negative results.

DECLASSIFIED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by Cdr. USAINTC
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

278

~~CONFIDENTIAL~~

Incl 12

[redacted]

13. (U) ~~(C)~~ GONDOLA STAR: (OACSI Approval - 17 Feb 72)

a. Location: Aberdeen Proving Ground, MD

b. Confidential Source Utilization: Two sources were used during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Investigative data on potential sources.

e. Operational Status: A review of installation targets indicates that the highest priority should be given the Ballistics Research Laboratory (BRL). One of the above sources is assigned to BRL, and three conventional sources are now under assessment to expand the coverage. Two additional conventional sources are under assessment in other target activities. The Project Liaison Officer has been assisting in preparation of the Sensitive Activity Vulnerability Estimate (SAVE) at Aberdeen since February. This has given him an opportunity to make additional useful contacts and identify areas such as BRL which need additional source coverage.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ..... Cdr USAINSCOM .....
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY ..... 2 .....
DECLASSIFY ON ..... Indefinite .....

279

Incl 13

[redacted]

(U)

14. ~~(C)~~ GONG SILK: (OACSI Approval - 16 Feb 72)

a. Location: Picatinny Arsenal, Dover, NJ

b. Confidential Source Utilization: One source was terminated during the period, leaving a total of two.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: As a result of information provided by a source, the Commander and Security Officer were made aware of excessive absenteeism by a GS 11 Engineer. The employee's absence and irrational behavior were known to the Civilian Personnel Office but not staffed. As a result, procedures have been changed so that such information will be reported to the Security Officer. Another engineer, a GS 12, allegedly takes bets from fellow employees in excess of $100 and "lays them off" with unidentified individuals off-post. Another engineer, a GS 11, is offering photographic equipment for sale to fellow employees at about 60% of cost, most of it admittedly "hot." This information, which could conceivably be exploited by HOIS came to the source as a target of opportunity. The ICIP Coordinator has requested further information be developed before requests for investigation are submitted to USAINTC.

e. Operational Status: Eleven of the 12 potential conventional sources mentioned in the previous quarterly report have been contacted, and 10 were amenable to recruitment. The 11th was agreeable, but did not consider that he had the proper placement. He identified the building in his directorate which was the location of the most sensitive activities, and recommended two individuals as possible sources. He has been briefed on the necessity of remaining silent about the operation. The Project Liaison Officer has been requested to assist in future SAEDA lectures, and expects to acquire additional potential sources from among the "walk-ins" who normally surface after such lectures. The Commander has taken an interest in the operation and requested the expanded coverage which will be provided by the use of conventional sources. Termination of the source was necessitated because of a RIF which reduced him from a GS 11 to a GS 7, affecting his production as a source. He was also transferred to a less sensitive area, ending his placement.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by Cdr USAINTC
EXEMPT FROM GENERAL [illegible] CATION
SCHEDULE OF [illegible] 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

[redacted]

280

15. (U) LANDLESS TIME: (OACSI Approval - 19 Jan 72)

a. Location: Philadelphia Facility, US Army Electronics Command

b. Confidential Source Utilization: One source was contacted during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: None.

e. Operational Status: The source was met in New Jersey and stated that he was to be officially transferred to Ft Monmouth on 11 Mar. From a practical standpoint, this signifies the demise of LANDLESS TIME. A revised CENTRAL TAXI OPLAN will include the functions transferred from Philadelphia to Ft Monmouth, and will identify the Management Information Services Branch, to which this source is assigned, as a target area. This source will be carried during the next reporting period under CENTRAL TAXI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by Cdr USAINTC
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

[redacted]

(4)

16. [redacted] LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute, East Coast Branch
Anacostia Naval Annex, Washington, DC

b. Confidential Source Utilization: None; coverage is provided by conventional sources.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Agent Reports on eight Arabian instructors which satisfies requirements of a USAINTC program concerning extremist threats against the Army.

e. Operational Status: During the reporting period, word was received that the headquarters and school would begin a move to the Presidio of Monterey, CA, after 1 July. However, all classes which are in session on that date will continue here until graduation. It will therefore be necessary to continue this operation until the move by attrition is completed, while LENTIL MONKEY will increase coverage accordingly.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by Cdr USAINTC
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON indefinite

[redacted] 282

Incl 16

17. (U) ~~(C)~~ LENIENT CLOUD: (OACSI Approval - 16 Feb 72)

a. Location: US Army War College, Carlisle Barracks, PA

b. Confidential Source Utilization: Four sources used during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: The limited investigation on the captain displaying unexplained affluence is not yet complete. A Hungarian-born NCO was identified as not having completely accounted for foreign visits and relatives. The requested investigation has been completed and is being returned to AWC. The questionable areas appear to have been satisfactorily resolved.

e. Operational Status: The CG, AWC continues to express his complete satisfaction with the operation. Conventional Sources continue to provide information to supplement that provided by the Confidential Sources. The new Deputy CG was briefed during the period and expressed reservations concerning the operation. It can only be hoped that the Commandant's enthusiasm for the operation will serve to overcome this attitude.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAIRSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

C: Cdr USAIRSCOM
I: ...ION
S: ...
E: ...
DECL: ...Declassify...

283

Inc 17

~~CONFIDENTIAL~~

18. (U) ~~(C)~~ LENTIL MONKEY: (OACSI Approval - 26 Oct 71)

a. Location: Defense Language Institute West Coast Branch
Presidio of Monterey, CA

b. Confidential Source Utilization: Four sources were utilized during the period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained: Another incident involving pen-pals in Czechoslovakia was surfaced, although it took place during the summer of 1973. It involved unidentified ethnic Czechs at the SOKOL Hall in San Mateo, CA and two unidentified WAC members of the Army Security Agency who graduated in Sep 73. ODCSI, USAREUR has been requested to pass this information to ASA security authorities in USAREUR and provide the identity of the perpetrators and the names of the Czech pen-pals. Five individuals involved in the illegal use of drugs were identified and appropriate notifications made. One of these was alleged to have admitted using heroin.

e. Operational Status: The Commandant, Defense Language Institute, was present for the quarterly briefing and was extremely receptive to the program. He expects to move his staff to the West Coast by Sep 74. There are 11 conventional sources employed, and eight additional students have been identified as probable confidential sources. Both the Commandant and Security Officer have expressed appreciation for the enhancement of the installation's security posture as a result of the ICIP and attendant CI support.

REGRADED UNCLASSIFIED
ON SEP 5, 1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

Classified by Gar USAINTC
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Originating

~~CONFIDENTIAL~~ 284
283A

Incl 18

~~SECRET~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) Operations

OFFICE SYMBOL: DAMI-DOI-S

SUSPENSE:

DATE: 28 January 1974

ACTION REQUIRED: To obtain approval of the quarterly ICIP report.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. By memorandum dated 8 February 1972 (YELLOW TAB B) the Under Secretary of the Army requested the Vice Chief of Staff (VCSA), US Army, provide quarterly reports on all (ICIP) operations.

b. This is the seventh such quarterly report.

c. USAINTC input is at YELLOW TAB C.

2. DISCUSSION:

a. At the direction of the VCSA, 2 November 1973, the term Internal Counterintelligence Program (ICIP) replaced the term Aggressive Counterintelligence Program, (ACIP).

b. YELLOW TAB A forwards to the VCSA the ICIP Quarterly Report ending 31 December 1973 for the Under Secretary of the Army.

3. RECOMMENDATION: That the memorandum to the VCSA at YELLOW TAB A be approved and signed.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		29 JAN 74
			DIV		30 JAN 74
			DIR		31 JAN 74
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

LTC STROM/77017

SPECIAL ACTIONS BR
RECORDS COPY

ACSI FORM 28, 13 Sep 71

~~SECRET~~

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~SECRET~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

DAMI-DOI-S

01 FEB 1974

MEMORANDUM FOR: VICE CHIEF OF STAFF, UNITED STATES ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations

1. Reference Under Secretary of the Army memorandum, dated 8 February 1972, subject as above (Inclosure 2).

2. Recommend your approval and signature of the memorandum at Inclosure 1 which transmits the report required by the cited reference.

3. Coordination: None required.

WD
2 Incl
1. Memo for USofA w/attachment (~~CONFIDENTIAL~~)
2. Memo for VCSA, 8 Feb 72 (~~SECRET~~)

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

15 Feb 74

APPROVED - VCSA. (Memo to USofA hand carried).

MICHAEL [illegible]
Major, GS
Assistant Secretary of the General Staff

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM F01/PO AUTH Para 1-603 DOD 5200.1R

File in

285

~~Regraded unclassified when separated from Classified Inclosures~~

~~SECRET~~

CS 350.09 (1 Feb 74)

~~CONFIDENTIAL~~

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations (U)

1. (U) Reference is made to memorandum, Under Secretary of the Army, dated 8 February 1972, subject as above.

2. (U) The eleven Internal Counterintelligence Program (ICIP) operations reported by memorandum to you last quarter remain active. Six new operations submitted during the last quarter have been reviewed at DA and approved for implementation. The report of current operations for the quarter ending 31 December 1973 is attached.

3. (U) The primary value of ICIP operations is in their potential for early warning and detecting internal security weaknesses and security threats to the supported command. Inasmuch as these operations are a form of intensified security watchfulness, negative reports in themselves are frequently of value to a commander in planning for security requirements of a given installation or activity.

1 Incl
as (CONFIDENTIAL)

FRED C. WEYAND
General, United States Army
Vice Chief of Staff

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DAMI-DO
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 1979

286

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

CURRENT ICIP OPERATIONS

LOCATION	ICIP NICKNAME	DATE APPROVED	NUMBER CONFIDENTIAL SOURCES
Edgewood Arsenal, Maryland	CANAL LOOP	16 Feb 72	5
Fort Huachuca, Arizona	CANAL ROPE	17 Dec 73	0
Fort Ritchie, Maryland	CANARY EFFORT	16 Feb 72	3
Dugway Proving Ground, Utah	CANARY STONE	18 Jul 73	0
Seneca Army Depot, New York	CANINE PLATE	18 Sep 73	0
Fort Bliss, Texas	CANTINA ARCH	12 Dec 73	0
Fort Lewis, Washington	CENTAUR RACE	30 Jul 73	0
Fort Belvoir, Virginia	CENTAUR SALE	14 Dec 73	0
Harry Diamond Lab, Washington, DC	CENTAVO KID	18 Oct 73	0
Fort Monmouth, New Jersey	CENTRAL TAXI	16 Feb 72	3
USAMSSA, Pentagon	CENTURY SQUAD	3 Oct 73	0
Aberdeen Proving Grounds, Maryland	GONDOLA STAR	16 Feb 72	2
Picatinny Arsenal, New Jersey	GONG SILK	16 Feb 72	3
Electronics Command, Philadelphia, Pennsylvania	LANDLESS TIME	19 Jan 72	1

Classified by [illegible]
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 1979

287

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY USAINSCOM FOIPA
Auth Para 4-102 DOD 5200.1R

~~CONFIDENTIAL~~

CURRENT ICIP OPERATIONS (cont)

LOCATION	ICIP NICKNAME	DATE APPROVED	NUMBER CONFIDENTIAL SOURCES
Defense Language Institute Washington, DC	LANYARD MOOD	22 Dec 71	0
Army War College, Carlisle Barracks, Pennsylvania	LENIENT CLOUD	16 Feb 72	4
Defense Language Institute Presidio of Monterey, California	LENTIL MONKEY	26 Oct 71	4
TOTALS 17	17		25

Off-post Information: There were no instances in which information on non-affiliated civilians was collected off post.

Information Obtained:

a. During the second quarter FY 74 the ICIP operations have received increased emphasis from the Intelligence Command and the supported commanders. The 17 operations, six of which are newly implemented, have been received with enthusiasm from the supported commands. None of the operations during this quarter indicated the existance of a hostile threat.

b. Approximately 30 reports emanating from the ongoing operations and passed to the supported commanders concern personnel suitability and incidents.

Continuance of Operations: The 17 ICIP operations are being continued for their original stated purpose.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR SAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

288

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE COMMAND
FORT MEADE, MARYLAND 20755

9 JAN 1974

ICDO-OP

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOI-S)
WASH DC 20310

1. (U) There has been positive improvement in the Internal Counterintelligence Program (ICIP) during the second quarter FY 1974. The positive improvement has resulted from Command emphasis placed on making the individual operations viable and productive. The briefings conducted by the Intelligence Command and the Group Commanders' visits have contributed immeasurably to understanding, acceptance and cooperation in the ICIP by the supported Commanders and their staffs. With this impetus and assignment of aggressive Project Liaison and Contact Officers, the operations are beginning to produce the counterintelligence information that meet and satisfy the objectives of this program. Criminal and security information gleaned as an adjunct of the program activity have been furnished the appropriate Army authorities for their action.

2. (U) During the reporting period, there have been six additional ICIP operations approved of which three were implemented and the other three are scheduled for implementation during January 1974. This brings the total number of operations to 17 for the program.

3. (U) In addition to Quarterly Status report, Progress Reports are inclosed for in depth information concerning the individual operations. These reports not only reflect the progress accomplished during the reporting period, but the positive attitude that now prevails at all levels.

Classified by DCSOPS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS. DECLASSIFIED ON 31 DEC 1979

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

289

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

09 JAN 1974

ICDO-OP
SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

This aggressive attitude is expected to result in increased productivity with each quarter. Equally important, the ICIP is expected to continue to project a favorable image of counterintelligence through professional accomplishments and service to the supported commands.

FOR THE COMMANDER:

JESSE D. JOY, JR.
Colonel, GS
Deputy Chief of Staff, Operations

32 Incl
1-17. Quarterly Status Rpts
18-32. Quarterly Progress Rpts

REGRADED UNCLASSIFIED
ON SEP -5
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

290

~~CONFIDENTIAL~~

Page 1789 of 3957

~~CONFIDENTIAL~~

1. (U) ~~(S)~~ CANAL LOOP: (OACSI Approval - 16 Feb 72)

a. Location: Edgewood Arsenal, Edgewood, MD

b. Confidential Source Utilization: Five sources were utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: Two Agent Reports dated 13 Dec 73, subject: b6 submitted.

e. Operational Status: The assignment of a replacement Project Liaison Officer will enhance the planned recruitment of additional sources both here and at Aberdeen Proving Ground.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC

1919

291

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

2. (U) ~~(C)~~ CANAL ROPE: (OACSI Approval - 17 Dec 73)

a. Location: Headquarters, US Army Communications Command and 11th Signal Group, Ft Huachuca, AZ

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: Not applicable.

d. Useful Information Obtained: Not applicable.

e. Operational Status: Implementation by the field element directed on 21 December 1973 is expected to be actioned in January 1974.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ..... DCSOPS USAINTC .....
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS DECLASSIFIED AFTER 1979

~~CONFIDENTIAL~~

Incl 2

~~CONFIDENTIAL~~

3. (U) ~~CONFIDENTIAL~~ CANARY EFFORT: (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three Confidential Sources were utilized during the reporting period. Additionally, one Conventional Source has been coded and was utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: Twenty-two Agent Reports were submitted pertaining to incidents and adverse suitability information regarding US Army personnel assigned to the US Army Communications Command - CONUS and Fort Ritchie. Several individuals were identified as being involved in drug abuse or drug abuse incidents. Appropriate Fort Ritchie staff personnel and CID were notified. Activities of these individuals will be monitored for development of specific suitability information, since the majority have access to the Alternate Joint Communications Center. A senior NCO assigned to communications was identified as being in debt.

e. Operational Status: An experienced Project Liaison Officer was assigned the operation on 15 October 1973 and is now well established. The Fort Ritchie commander expressed his gratitude at the accomplishments rendered during the reporting period. The Commanding General, US Army Communications Command - CONUS has expressed his desire that the operation continue in effect to enhance the security of his command.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC

1974

~~CONFIDENTIAL~~ 293

~~CONFIDENTIAL~~

4. (U) CANARY STONE: (OACSI Approval - 18 Jul 73)

a. Location: Deseret Test Center, Dugway Proving Ground, UT

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: Not applicable.

d. Useful Information Obtained: Not applicable

e. Operational Status: With the arrival of the Project Liaison Officer on station on 1 December 1973, and the finalization of the Intraservice Support Agreement, this operation can be expected to become operational during the coming quarter.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ...DCSOPS USAINTC...

~~CONFIDENTIAL~~

294

~~CONFIDENTIAL~~

5. (U) CANINE PLATE: (OACSI Approval - 18 Sep 73)

a. Location: Seneca Army Depot, Romulus, NY

b. Confidential Source Utilization: None utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: Not applicable.

e. Operational Status: The Commander was briefed on the implementation of the operation on 17 November 1973. Sources are expected to be recruited and reporting during the third quarter of FY 74.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM I-04/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
1979

~~CONFIDENTIAL~~ 295

Inc 15

6. (U) CANTINA ARCH: (OACSI Approval - 12 Dec 73)

a. Location: US Army Air Defense Center and Fort Bliss, TX

b. Confidential Source Utilization: Not applicable

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: Not applicable.

e. Operational Status: Implementation by the field element directed on 21 December is expected to be accomplished in January 1974.

REGRADED UNCL
ON: SEP -5 1997
BY OSR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DRSOPS USAINSCOM
1975

Page 1795 of 3957

[redacted]

7. (U) (C) CENTAUR RACE: (OACSI Approval - 30 Jul 73)

a. Location: Ninth Infantry Division and Fort Lewis, WA

b. Confidential Source Utilization: This operation currently has no Confidential Sources.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: Conventional Sources have reported damage to signal equipment and to a helicopter. Both incidents are still under investigation to determine whether the damage was intentional or accidental. Information was also obtained on the distribution of anti-military/dissident literature at Fort Lewis.

e. Operational Status: The impending courtmartial of SP4 b6 b6 for illegal distribution of literature on-post has increased the tempo of anti-military activity at Fort Lewis. Lead Development data on prospective Confidential Sources is expected by mid-January 1974. In the meantime, coverage is provided by 11 Conventional Sources, with another 12 under assessment.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC

1974

297

[redacted]

8. (U) (C) CENTAUR SALE: (OACSI Approval - 14 Dec 73)

a. Location: US Army Mobility Equipment Research and Development Center, Fort Belvoir, VA

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: Not applicable.

d. Useful Information Obtained: During this period three Agent Reports were produced. These reports are as follows: b6 b6, DPOB: b6 SSG b6, report submitted 26 October 1973, concerned suitability due to indebtedness; b6, DPOB: b6, CIV b6, report submitted 5 November 1973, concerned suitability due to alcohol drinking problems; b6 DPOB: b6 b6 SSAN b6, report submitted 21 November 1973, concerned a threatening telephone call. The information reported was developed by the Project Liaison Officer pending formal approval of the Operations Plan.

e. Operational Status: Formal implementation by the field element directed on 21 December 1973 is expected to be accomplished in January 1974.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
1999

Incl 8

9. (U) CENTAVO KID: (OACSI Approval - 18 Oct 73)

a. Location: Harry Diamond Laboratories, Washington, DC

b. Confidential Source Utilization: None utilized during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: One Agent Report was produced on suitability information developed on b6 DPOB: b6 b6 CIV b6

e. Operational Status: The Commander was advised on 12 November 1973 that the operation was being implemented. However, source recruitment is not expected until the next reporting period.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
1979

299

Ind 9

~~CONFIDENTIAL~~

10. (U) CENTRAL TAXI: (OACSI Approval - 16 Feb 72)

a. Location: Headquarters, US Army Electronics Command, Fort Monmouth, NJ

b. Confidential Source Utilization: Three such sources were used during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: A US Army truck has been observed delivering unidentified articles each week to a civilian residence in a nearby town; a civilian employee has a drinking problem to the extent that he has come to work inebriated. A civilian employee is allegedly involved in narcotics traffic.

e. Operational Status: Above items of information were passed to the appropriate officials at Fort Monmouth. The operation has been revitalized. The confidential sources have been reactivated by the newly assigned Project Control Officer, and the Project Liaison Officer has recruited three conventional sources; two in the Electronics Warfare Laboratory, ECOM's most sensitive activity and one in the Maintenance Directorate where the majority of the ECOM security violations originate.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM I-81/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINSCOM
[illegible]
[illegible] 1974

300

~~CONFIDENTIAL~~

Incl 10

11. (U) CENTURY SQUAD: (OACSI Approval - 3 Oct 73)

a. Location: US Army Management Systems Support Agency, The Pentagon

b. Confidential Source Utilization: Not applicable.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: Not applicable.

e. Operational Status: The Security Officer and his assistant were advised on 5 November 1973 that the operation had been approved for implementation. Ten individuals have been identified as potential Confidential Sources, and requests for Local and National Agency Checks have been initiated. Recruitment of these individuals will depend on the investigative results. The files of 17 civilian employees have also been reviewed and records checks have been requested.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

DCSOPS USAINTC

Page 1800 of 3957

~~CONFIDENTIAL~~

12. (U) GONDOLA STAR: (OACSI Approval - 17 Feb 72)

a. Location: Aberdeen Proving Ground, MD

b. Confidential Source Utilization: Two sources were used during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: The recently assigned Project Liaison Officer, who also handles the operation at Edgewood Arsenal, has served two previous tours at Aberdeen, and his contacts needed to spot and assess the additional Confidential Sources required for this operation have been re-established. Edgewood is a sub-post of Aberdeen, and it appears advisable to revise the GONDOLA STAR OPLAN to include CANAL LOOP. A single Project Control Officer handles the sources at both posts, and the Aberdeen Installation Intelligence Officer, who is the ICIP Coordinator, functions also for Edgewood.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM 1/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ...DCSOPS USAINSCOM...
...1979

~~CONFIDENTIAL~~

14. (U) (C) LANDLESS TIME: (OACSI Approval - 19 Jan 72)

a. Location: Philadelphia Facility, US Army Electronics Command

b. Confidential Source Utilization: One source was contacted during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: The single source available in this operation moved to a newly-purchased house near Fort Monmouth shortly before Christmas and he is commuting to Philadelphia. At the present time, source is employed in the Management Information Services Directorate, which is not included in the designated target areas of the Fort Monmouth operation. Retention of source depends upon his projected transfer in March 1974 to duties at Fort Monmouth.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DAMO-ODS USAINTC
SUBJECT TO GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS

~~CONFIDENTIAL~~

Item 14

Page 1802 of 3957

(U)

15. (C) LANYARD MOOD: (OACSI Approval - 22 Dec 71)

a. Location: Defense Language Institute East Coast Branch
Anacostia Naval Annex, Washington, DC

b. Confidential Source Utilization: None; coverage is provided by conventional sources.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: This facility has changed from the previous utilization of contract schools scattered throughout the Washington area to a more traditional self-contained facility with seven language departments and its own instructors. A revised operation plan reflecting this structure and placing emphasis on the utilization of confidential as well as conventional sources has been prepared and will be forwarded under separate cover.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM 701/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
ON
1979

16. (U) LENIENT CLOUD: (OACSI Approval - 16 Feb 72)

a. Location: US Army War College, Carlisle Barracks, PA

b. Confidential Source Utilization: Four such sources were used during the reporting period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: Information was developed indicating a captain has exhibited unexplained affluence, which served as basis for initiating an investigation.

e. Operational Status: The Project Liaison Officer has developed 31 conventional sources, whose information has identified a number of security weaknesses. The Commandant has been made aware of this situation and has established additional security safeguards. The Military History Research Collection, a tenant agency, has been added to the list of target activities.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM 701/PO
AUTH Para 1-603 DOD 5200.1R

Classified by DCSOPS USAINTC
1979

305

Incl 16

~~CONFIDENTIAL~~

(U)

17. (~~C~~) LENTIL MONKEY: (OACSI Approval - 26 Oct 71)

a. Location: Defense Language Institute West Coast Branch
Presidio of Monterey, CA

b. Confidential Source Utilization: One source was used as of the beginning of the reporting period. Three additional sources were added during the period.

c. Information Obtained Off-post and/or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained: A Czech class made a field trip to the same San Francisco restaurant mentioned in status report for the second quarter of CY 73. There was no repetition of the May 73 incident. Communist literature was found in the post gymnasium. Improper procedures were used in a briefing with a SECRET classification. This information was passed to appropriate staff personnel.

e. Operational Status: The lead Bank of prospective sources stands at 68 MI students. Twelve have been selected as prospective conventional sources and eight for confidential sources. The continued SAEDA briefings of class monitors has increased the security awareness of the students, and incidents which went unreported in the past are now being brought to the attention of the proper authorities.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FO1/PO
AUTH Para 1-603 DOD 5200.1R

Classified by ..... DCSOPS USAINSCOM .....
SUBJECT TO GENERAL DECLASSIFICATION
[illegible]
[illegible] 1979

306

~~CONFIDENTIAL~~

Incl 17

DEPARTMENT OF THE ARMY
HEADQUARTERS, 109TH MILITARY INTELLIGENCE GROUP
FORT MEADE, MARYLAND 20755

ICGP-B-SP

SUBJECT: Quarterly Progress Reports (QPR) and Quarterly Status Reports (QSR) (U)

Commander
United States Army Intelligence Command
ATTN: ICDC-OP
Fort Meade, Maryland 20755

1. (U) Forwarded herewith are ten Quarterly Progress Reports (QPR) and ten Quarterly Status Reports (QSR) for the period 15 September 1973 to 15 December 1973 for the following Internal Counterintelligence Program (ICIP) Projects:

a. CANAL LOOP (U)

b. GONDOLA STAR (U)

c. CANINE PLATE (U)

d. CENTAVO KID (U)

e. CENTRAL TAXI (U)

f. GONG SILK (U)

g. LANYARD MOOD (U)

h. CENTAUR SALE (U)

i. CANARY EFFORT (U)

j. LENIENT CLOUD (U)

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

2. (U) Project accomplishments are contained in individual QPRs; however, specific attention is invited to the following projects:

a. CANAL LOOP (U) and GONDOLA STAR (U): The new Project Liaison

307

Incl 18

[redacted]

ICGP-B-SP
SUBJECT: Quarterly Progress Reports (QPR) and Quarterly Status Reports (QSR)

Officer (PLO) is on station and the new Project Control Officer (PCO) has reactivated seven dormant sources. This Group will recommend combining these two operations in view of organizational changes in the mission and functions of Edgewood Arsenal and Aberdeen Proving Ground.

b. CANINE PLATE (U): During the reporting period, formal approval of the Operation Plan (OPlan) was received from the Office of the Assistant Chief of Staff, Intelligence (OACSI), Department of the Army, and the Commander, Seneca Army Depot was briefed. A PLO is assigned and the program is being implemented based on ground work previously initiated.

c. CENTAVO KID (U): During the reporting period OACSI approval of the OPlan was received and the Commander, Harry Diamond Laboratory was briefed regarding the project. A PLO has been assigned and the program has been implemented. Sources are under consideration.

d. CENTRAL TAXI (U) and LANDLESS TIME (U): The CENTRAL TAXI (U) OPlan is under revision and should be combined with LANDLESS TIME (U). This action is recommended in view of the deactivation next year of the Electronics Command, Philadelphia (ECOM/P) and transfer of its functions to Fort Monmouth (ECOM/M). As a result of the on-going drawdown, transfer of functions and necessary termination of all but the one Confidential Source who is moving to Fort Monmouth, no QPR or QSR will be submitted for Operation LANDLESS TIME (U).

e. GONG SILK (U): The newly assigned GREAT SKILL (U) PCO has reactivated the three dormant Confidential Sources and broadened his base.

f. LANYARD MOOD (U): ICIP Support to the Defense Language Institute, East Coast (DLIEC) has a new PLO designated, and the revised OPlan submitted to your headquarters for approval.

g. CENTAUR SALE (U): OACSI approval of the OPlan was received on 14 December 1973. The Commander, Mobility Equipment Research and Development Center (MERDC) elected to be briefed in January 1974. A PLO has been designated and is presently active in the overt aspects of the program.

h. CANARY EFFORT (U): The project in support of USACOM-CONUS and Fort Ritchie is the best example of what the ICIP can accomplish when aggressively pursued by all personnel involved. Specific attention is invited to the CANARY EFFORT (U) QPR and QSR. I have directed that CANARY EFFORT (U) serve as the pilot operation for all ICIP operations conducted by the 109th MI Group. A new PLO has been recently assigned.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

[redacted]

Page 1807 of 3957

ICGP-B-SP
SUBJECT: Quarterly Progress Reports (QPR) and Quarterly Status Reports (QSR)

i. LENIENT CLOUD (U): The Military History Research Collection (MHRC), at the request of the Commandant, US Army War College (USAWC) has been added to the LENIENT CLOUD (U) Target List. Information developed by the PLO has led to the initiation of background investigations concerning two individuals assigned to USAWC. Two Conventional Sources have been coded during the reporting period.

3. (U) The following items constitute group-wide accomplishments which have significantly improved all aspects of the ICIP:

a. Operational control of the ICIP has been returned to Field Office control and energized there. A Special Operations Letter of Instruction (LOI) has been published which will constitute 109th MI Group policy and procedures regarding the ICIP. I have placed great Command Interest throughout the quarter on the program and stressed the importance of the ICIP during the recent 109th MI Group Commanders' Conference. I will continue to emphasize this program during my periodic visits to all subordinate elements. Additionally, I have personally briefed a number of commanders of supported activities and their security managers concerning ICIP. This quarter we have placed first priority on the ICIP program and results have been satisfactory. More will be accomplished.

b. Action has been taken to fully coordinate the provisions of existing ICIP OPlans with the provisions of USAINTC and 109th MI Group OPlans 109-73, 110-73, and 111-73. Simultaneously, all ICIP OPlans will be revised and updated on a programmed basis. The object is to better our product and expand our base.

c. My staff has worked closely with your Special Operations personnel in the formulation of an ICIP Monthly Operational Status Report which is designed to update and replace the QSR and QPR.

d. GREAT SKILL (U) Personnel have been assigned and are operationally active as PCOs. All dormant Confidential Sources have been reactivated and are being retrained and redirected in line with increased standards of professionalism. More sources are being considered.

e. A Conventional Source Program is being developed to augment and support existing Confidential Sources.

f. Guidance has been formulated and disseminated directing subordinate commanders to evaluate supported installations and activities for potential ICIP implementation.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R,

309

Page 1808 of 3957

~~CONFIDENTIAL~~

ICGP-B-SP
SUBJECT: Quarterly Progress Reports (QPR) and Quarterly Status Reports (QSR)

4. (U) The preceding actions have resulted in the highest level of productivity since the ICIP was reactivated in late 1971. I am confident that continued emphasis upon ICIP by all personnel will result in significant, demonstrable enhancement of the security posture of supported activities and installations.

20 Incls
as (1 cy ea)

CHARLES E. THOMANN
Colonel, MI
Commanding

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

310

~~CONFIDENTIAL~~

Page 1809 of 3957

~~CONFIDENTIAL~~

CARLISLE BARRACKS LIAISON OFFICE
109th MILITARY INTELLIGENCE GROUP
CARLISLE BARRACKS, PA 17013

QUARTERLY PROGRESS REPORT NUMBER ____

Period 12 October 1973 to 18 December 1973

~~WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED~~

SUBJECT: OPERATION LENIENT CLOUD (U)

1. (U) CIRCUMSTANCES: At 0900, 18 December 1973, Major Franklin M. Davis, Jr., Commandant, US Army War College, (USAWC), Carlisle Barracks, PA, 17013, received the quarterly briefing concerning significant items of interest within the target areas defined by Installation Counterintelligence Program (ICIP), LENIENT CLOUD, from Special Agent John A. Nolan III, Project Liaison Officer, (PLO). No other persons were present during the briefing.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. Operational and administrative control of ICIP LENIENT CLOUD was placed in Field Office Commander, (FOC), Fort Ritchie Field Office (FRFO), 109th MI Group.

(1) Such operational control caused PLO to be responsible for the conduct of SAEDA Briefings. Two SAEDA briefings were presented to a total of 560 military and civilian personnel on the installation on 1 November 1973. Presentation of such briefings allowed greater exposure of PLO to military and civilian personnel as a representative of USAINTC; allowed PLO to include himself among those persons continuously present on the installation capable of resolution of security related problems; and greatly enhanced PLO's accessibility to records and personnel on the installation and vise versa.

(2) On 24 October 1973, MAJ Robert L. Brooks, FOC, FRFO, visited Carlisle Barracks for an orientation, which included meetings with the Directors, and tours, of Strategic Studies Institute, Operations Group, Military History Research Collection (MHRC), USAWC Library, USAWC itself and USACC-C facility, Carlisle Barracks.

(3) On 11 December 1973, COL Charles E. Thomann, Commanding Officer, 109th MI Group, accompanied by MAJ Brooks, visited Carlisle Barracks for an orientation and in addition to an office call on General Davis, received a tour through those facilities in paragraph 2a(2) above, with the exception of MHRC.

(4) As a result of the visit by COL Thomann and MAJ Brooks, a comprehensive paper is presently being prepared with a view toward reducing the administrative

CLASSIFIED BY CDR, 109TH MI GROUP
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652.
EXEMPTION CATEGORY ____
DECLASSIFY ON ____

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

311

~~CONFIDENTIAL~~

CONFIDENTIAL

time, especially in regard to security clearance procedures, involved in hiring of civilian professors and consultants at Strategic Studies Institute, possibly through USAINTC assets.

(5) An additional result of the visits by COL Thomann and MAJ Brooks was an appreciation of the physical plant, the functions and the key personnel of target areas defined within ICIP LENIENT CLOUD.

b. In response to General Davis' request of 23 October 1973, approval was sought for the addition of MHRC to the target list of those organizations and facilities covered by Project LENIENT CLOUD.

(1) On 14 November 1973, approval was granted by letter from Commanding Officer, USAINTC, to add MHRC to the target list.

(2) Since 1 April 1973, target operational research for operational data relative to MHRC has been conducted and has thus far resulted in the submission of two Agent Reports detailing security procedures in effect at MHRC and two Agent Reports concerning persons assigned to MHRC.

(3) Spotting and assessment of potential assets has not thus far resulted in the submission of any formal, comprehensive Lead and Development Reports; however, daily to weekly contact has been established with three individuals presently identified as casual sources, within MHRC.

(4) As a result of contact with casual sources within MHRC, a formal written request for counterintelligence technical services was submitted to HQ, 902nd MI Group and subsequently completed by elements of the AJCC Field Office, 902nd MI Group, Fort Ritchie, MD. The services resulted in an appreciation on the part of MHRC administrative personnel of the benefits which accrue to the facility by such technical services. By virtue of the established reluctance on the part of COL George S. Pappas as regards the need for counterintelligence services, the basis for request of the services primarily concerned the safeguarding of valuable manuscripts, weapons, uniforms and other exhibits maintained in MHRC. At this point in time, such emphasis establishes, in the mind of the Director, a compatability between academic and historical prespectives and counterintelligence services.

c. During the reporting period, in-depth spotting and assessment potential assets for utilization, has resulted in submission of seven Lead and Development Reports.

d. To date, a total of twenty-nine casual sources, with whom daily to weekly contact had been maintained, have been utilized. As a result of utilization, two casual sources have been coded as Source 9002 and Source 9003.

e. Establishment of the PLO as a quasi-officially assigned assistant to the USAWC Security Manager, and who has a capability of providing a liaison conduit to USAINTC as an adjunct to such duties, has resulted in:

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

312

CONFIDENTIAL

~~CONFIDENTIAL~~

(1) Casual and conventional sources providing information which they would normally not have occasion to report officially due to periodically vagarious requirements of military administrative procedures.

(2) Causing the PLO to be queried relative to organizations with which members of the USAWC Staff and Faculty deal. Such queries have resulted in very rapid resolution of requests for characterization, in two cases, through CPT B. A. Oullette, Special Investigations Branch, 109th MI Group, and establishment of the PLO, in the view of the Staff and Faculty members, as a viable contact for intelligence related matters.

(3) Causing requests for all classified and unclassified military information to be routinely channelled through the USAWC Security Office, as opposed to the previous "hit or miss" manner in which each department of USAWC validated the requestor's authenticity. Further results include an established procedure whereby the List of Collectors of Unclassified Military Information (LHCUMI) is reviewed and has caused the submission of three letters to the appropriate agency at ACSI, when organizations/individuals have appeared in the LHCUMI document.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

a. As a result of contact with a casual source in the administrative section of MHRC, a request for a background investigation of SGT b6 b6 MHRC has been submitted, through USAINTC channels, and is being conducted by PLO. Estimated date of completion of the initial portion of the investigation is 5 January 1974, dependent upon availability of sources who may be able to resolve derogatory information which has arisen.

b. As a result of inquiries by PLO, contact with conventional and casual sources on the installation, and in concert with information developed through confidential sources, a request for another investigation into the financial and moral background of CPT b6, assigned to Department of Command and Management, USAWC, has been initiated to be resolved by USAINTC elements. To date one Agent Report has been submitted to SIB, 109th MI Group, for forwarding to USAINTC, as background, prior to the submission of the request for investigation through the Deputy for Plans, Training and Security, Carlisle Barracks.

c. As a result of information supplied by casual sources, PLO is currently attempting to ascertain the true identity and purpose of a Mr. fnu b6, who has been "gate-crashing" parties and other social affairs at Carlisle Barracks, at which times he wears either a social or military name-tag. Local agency checks on Carlisle Barracks reveal that no individual by the name of b6 is assigned or employed at the installation.

d. An individual, subsequently coded, volunteered information in interview and sworn statement, relative to narcotics availability and use on Carlisle Barracks, as background information relative to the operation of

UNCLASSIFIED
SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

the installation, and which contained allegations relative to an individual assigned to Carlisle Barracks in possession of a TOP SECRET security clearance. To date, nine Agent Reports, Subject: Availability and use of Narcotics on Carlisle Barracks, PA 1973 and a Memorandum for the Record, Subject: Information and Circumstances Relative to Drugs on Carlisle Barracks, have been submitted.

4. (U) COMMENTS, REMARKS AND RECOMMENDATIONS:

a. General Davis commented that he appreciated the presence of a full time PLO, whose integration into both the official and social functioning of the installation has been such as to provide much more effective coverage than had previously been experienced. General Davis queried PLO relative to the PLO serving as the Security Manager, USAWC during the impending leave of the Security Manager during the latter two weeks in January 1974, and was assured that the PLO would so serve, without any substantial reduction in coverage. Further, the assumption of the Security Manager's duties for two weeks could only serve to cement the acceptability of the PLO as the assistant to the Security Manager.

b. General Davis was receptive to the PLO's suggestion that a consideration be given for a formal request for a penetration test of the USAWC, subsequent to the full implementation of additional security safeguards presently being substituted for systems previously determined to be inadequate. Formal request will probably be forthcoming in late January, 1974, when construction is completed.

c. General Davis was also receptive to a recommendation that consideration be given for up-grading the security posture of Root Hall, which houses USAWC, in respect to limiting access to the building and effectively reducing the threat posed by a stay-behind.

JOHN A. NOLAN III
PLO, LENIENT CLOUD

REGRADED UNCLASSIFIED
ON 7661
BY CDR USAINSCOM/J3S01/PO
AUTH Para 1-603 DOD 5200.1R

CONFIDENTIAL

DEPARTMENT OF THE ARMY
FORT ORD FIELD OFFICE
115TH MILITARY INTELLIGENCE GROUP
FORT ORD, CALIFORNIA 93941

ICGP-F-OR

11 December 1973

QUARTERLY PROGRESS REPORT NUMBER 4

For the Period 1 October to 31 December 1973

WARNING NOTICE - SENSITIVE SOURCES AND METHODS INVOLVED

SUBJECT: Operation LENTIL MONKEY (U)

1. (U) CIRCUMSTANCES:

a. At 1030 hours on 4 December 1973, a briefing on the progress of LENTIL MONKEY was conducted at the Fort Ord Field Office, 115th Military Intelligence Group, Fort Ord, California. Attending were:

Colonel Eric H. Vieler, Commander, 115th Military Intelligence Group
Major James H. Donnelly, Commander, Fort Ord Field Office
CW2 James E. McKinley, Project Liaison Officer, LENTIL MONKEY

b. Between 1430 and 1500 hours, 4 December, a similar briefing was held in the office of the Commandant, Defense Language Institute, West Coast (DLIWC), Presidio of Monterey, California. Persons present were:

Colonel John F. Hook, Commandant, DLIWC
Colonel Eric H. Vieler
Major Richard Erickson, Security Officer, DLIWC
Major James H. Donnelly
CW2 James E. McKinley

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. The On-Post Liaison Operation: A total of 80 students, who were Class and Section Monitors, received individual SAEDA briefings in this operation. Included in this total were four monitors who received second briefings, and five who received third briefings. Intelligence-trained students were also contacted and reminded of their professional responsibility to report anything of intelligence interest.

b. The Conventional Source Operation:

(1) At the start of the quarter this operation had 20 prospective sources. Eight more were selected during this period, giving the operation

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

315

CONFIDENTIAL

~~CONFIDENTIAL~~

ICGF-F-OR 11 December 1973
SUBJECT: Operation LENTIL MONKEY (U)

a total of 28 prospective sources. Information produced by this operation exceeded that of any previous quarter since the project was reactivated in November 1971.

(2) Colonel Hook and Major Erickson were not briefed on the following:

(a) During the reporting period the Lead Bank was expanded from 42 to 68 MI students. Twelve new Leads were selected as prospective Conventional Sources; however, four were later dropped because of academic difficulties with the language being studied.

(b) On 24 October 1973, this operation acquired a prospective source who is a DA civilian employee of the Systems Development Agency, Defense Language Institute, Presidio of Monterey. This individual was formerly Confidential Source IC-D-310 of the 112th Military Intelligence Group.

c. The Confidential Source Operation: When the quarter began, this operation had eight prospective sources. One was recruited on 11 October 1973, four are still under assessment, and three have been dropped as unsuitable. Seven additional leads are presently being screened for possible development as sources. Colonel Hook and Major Erickson were not briefed on the following:

(1) Lead and Development Reports have been forwarded for four prospective sources. Recruitment of one of these sources is awaiting Headquarters, USAINTC approval of the approach plan.

(2) The seven new Leads were selected to cover the Chinese (1), Czech (1), Hungarian (1), Polish (1), Russian (2), and Japanese (1). languages.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

a. Information was developed concerning the visit of a DLIWC Czech class to the Europa Restaurant, 2769 Lombard Street, San Francisco, CA, on 2 and 9 November 1973. A Confidential Source reported in May 1973 that the owner of this restaurant had encouraged Czech language students to establish "pen-pal" correspondence with three young females in Czechoslovakia. The class visited the restaurant as scheduled, but no further attempts to recruit "pen-pals" were noted.

b. A student reported that members of his Russian language class proposed a class visit of the Russian Consulate in San Francisco. Since the trip was not being planned for the immediate future, nothing further developed concerning this proposal.

316

REGRADED UNCLASSIFIED SEP 1997
ON
BY CDR USAINSCOM FOI/PO
AR 380-5 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1815 of 3957

~~CONFIDENTIAL~~

ICGP-F-OR
SUBJECT: Operation LENTIL MONKEY (U)

11 December 1973

c. Confidential Source IC-F-081 reported on Czechoslovakian publications available to his class which contained Communist propaganda.

d. A student provided a copy of a booklet published by the Central Committee for Conscientious Objectors, which he had received in the mail. Numerous copies of this same booklet have been received by military personnel at Fort Ord.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS: The briefing ended with no questions by the attending parties. Colonel Hook expressed his appreciation for the effort expended in the conduct of the Internal Counterintelligence Program, and was very pleased with the progress that had been made.

James H. Donnelly
JAMES H. DONNELLY
Major, MI
Commanding

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1816 of 3957

REGRADED UNCLASSIFIED
ON SEP -5 ...
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD ...

DEPARTMENT OF THE ARMY
Fort Ritchie Field Office
109th Military Intelligence Group
Fort Ritchie, Maryland 21719

ICGP-B-FR

15 December 1973

QUARTERLY PROGRESS REPORT NUMBER ____

Period 15 October 1973 to 15 December 1973

~~WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED~~

SUBJECT: Operation CANARY EFFORT (U)

1. (U) CIRCUMSTANCES:

a. Although a formal briefing per se has not been presented during reporting period, continual liaison has been effected and maintained with individuals briefed on the Counterintelligence Screening Program (CISP), Operation CANARY EFFORT, at Fort Ritchie. Continual/constant liaison has been effected and maintained with the following briefed individuals:

COL James A. Manning, b6 Armor, Commander, Fort Ritchie.

COL Daniel T. Larkin, b6 MPC, Deputy Commander, Fort Ritchie and Deputy Chief of Staff, Intelligence and Security, US Army Communications Command - CONUS and Fort Ritchie.

LTC Arlyn R. Madsen, b6 SC, Director, Telecommunications, Fort Ritchie.

CW4 Earl K. Osborne, b6 USA, COMSEC Officer, US Army Communications Command - CONUS and Fort Ritchie.

Mr. Joseph J. Carroll, DAC, GS-13, b6 Deputy Assistant Chief of Staff, Intelligence and Security, US Army Communications Command - CONUS and Fort Ritchie. Carroll is presently the CANARY EFFORT CISP Coordinator, Fort Ritchie.

Mr. Charles H. Koontz, DAC, GS-12, b6 Chief, Security Division, Deputy Chief of Staff, Intelligence and Security, US Army Communications Command - CONUS and Fort Ritchie.

Mr. William A. Kent, DAC, GS-11, b6 Chief, Intelligence Division, Deputy Chief of Staff, Intelligence and Security, US Army Communications Command - CONUS and Fort Ritchie.

b. On 19 November 1973, COL Charles E. Thomann, Commander, 109th Military Intelligence Group and LTC Leland J. Holland, Deputy Commander, 109th Military Intelligence Group, visited Fort Ritchie and effected personal contact with BG Albert Redman, Jr., b6 Commander, US Army Communications Command - CONUS, Fort Ritchie. BG Redman acknowledged that he was aware of the existence of a CISP at Fort Ritchie. BG Redman

... Cdr, 109th MI Group

318

cannot be determined

Page 1817 of 3957

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

ICGP-B-FR
SUBJECT: Operation CANARY EFFORT (U) 15 December 1973

further indicated a general knowledge of the aforementioned program as sponsored/directed by the US Army Intelligence Command (USAINTC). Undersigned Project Liaison Officer (PLO) was tasked with presenting an approximate ten minute informal briefing of the CISP in general.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. CW4 Gary L. Peisen was assigned as the PLO for Fort Ritchie on 10 October 1973 and became operational on 15 October 1973. Introduction to essential personnel was effected without difficulty and no apparant operational difficulties are foreseen. Four key personnel at Fort Ritchie were briefed on the CISP and executed required Security Oaths. Formerly briefed individuals with no placement and access due to assignment changes were debriefed and executed required Debriefing Statements. Overt liaison contacts were initiated and maintained with both military and appropriate civilian agencies and individuals during the reporting period. COL Manning, Commander, Fort Ritchie, expressed a keen interest in the CISP at Fort Ritchie and projected a sense of gratitude for accomplishments rendered during the reporting period. COL Manning further stated that he had every intention of continuing the CISP at Fort Ritchie as he believed it's contribution to enhancing the security posture of Fort Ritchie and the Alternate Joint Communications Center (AJCC), Site "R", was invaluable.

b. During reporting period a total of 22 Agent Reports (DA Form 341) were submitted by PLO pertaining to incidents and adverse suitability information concerning US Army personnel assigned to the US Army Communications Command - CONUS and Fort Ritchie. The majority of the aforementioned Agent Reports cited US Army personnel having access to the AJCC, Site "R", Fort Ritchie.

c. During reporting period Conventional Sources were vetted and provided reportable information concerning adverse suitability information regarding US Army personnel assigned to sensitive duties at Fort Ritchie. One Conventional Source was assigned a Key Sheet Identification Code and provided reportable information.

d. Spotting and Assessment for Confidential Sources with placement and access continues.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

a. As previously stated, a total of 22 Agent Reports (DA Form 341) were submitted by PLO pertaining to incidents and adverse suitability information concerning US Army personnel assigned to the US Army Communications Command - CONUS and Fort Ritchie. The majority of the aforementioned reports concerned US Army personnel, assigned to sensitive positions at Fort Ritchie, allegedly involved in drug abuse or drug abuse incidents. While drug abuse per se is not within the investigative purview of USAINTC

Page 1818 of 3957

ICGP-B-FR
SUBJECT: Operation CANARY EFFORT (U) 15 December 1973

the issue does involve suitabliity of the individuals concerned to hold security clearances and occupy sensitive positions. Upon receipt of the aforementioned adverse information, immediate action was taken to notify the CANARY EFFORT CISP Coordinator, the Commander, Fort Ritchie, and the Director, Telecommunications, if applicable. In addition to the aforementioned, action was initiated to disseminate information criminal in nature to the appropriate military and civilian authorities. In one case, liaison with a Conventional Source, disclosed that a member of the US Army assigned to Fort Ritchie, was experiencing adverse financial difficulties. Aforementioned information was brought to the attention of the CANARY EFFORT CISP Coordinator and resulted in serviced command having requested a Suitability Investigation from USAINTC concerning the individual involved.

b. SSG [b6] Operations Company, US Army Communications Command - CONUS and Fort Ritchie, with duty as a Teletype Repairman, Telecommunications Directorate, was reported as having questionable financial habits, i. e., indebtedness. Information contained in submitted Agent Report was reported to CANARY EFFORT CISP Coordinator, the Commander, Fort Ritchie, and the Director, Telecommunications. The Project Control Officer (PCO) and PLO will continue to monitor the aforementioned situation closely and report significant findings via appropriate Agent Report and to CANARY EFFORT CISP Coordinator.

c. Covert Sources within CANARY EFFORT target area continue to report information concerning drug and alcohol abuse by members of the US Army at Fort Ritchie and the AJCC. Covert Sources have also reported adverse suitability information, i. e., financial and moral indiscretion, involving both US Army and Department of the Army personnel at Fort Ritchie and the AJCC. Monitoring will continue.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS:

a. It is envisioned that a formal Quarterly Briefing will be presented to BG Redman, COL Manning, LTC Madsen, Mr. Carroll, and Mr. Kent in early January 1974. The aforementioned is deemed appropriate as this PLO did not become operational until 15 October 1973 and there is no record of a formal Quarterly Briefing having been presented concerning Operation CANARY EFFORT since 8 January 1973. The aforementioned proposed briefing will be held in abeyance until such time it is deemed appropriate, with USAINTC approval, to present BG Redman with the approved USAINTC CISP briefing, if applicable. The reader should also consider current instructions issued by Headquarters, 109th Military Intelligence Group, to the effect that ACIP coverage be expanded to include US Army Communications Command - CONUS elements not thus far included in the current operations plan governing CANARY EFFORT.

320

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

ICGP-B-FR
SUBJECT: Operation CANARY EFFORT (U) 15 December 1973

b. PLO and PCO enjoy an excellent working relationship as does PLO with his counterparts, liaison contacts, and Conventional Sources. It is invisioned that the CISP, Operation CANARY EFFORT, at Fort Ritchie will become increasingly productive and will ultimately afford the Commander, Fort Ritchie, with coverage desired, i. e., enhancement of the security posture of Fort Ritchie and the AJCC by means not locally available the Commander.

GARY L. PEISEN
CW4, USA
Project Liaison Officer

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

321

DEPARTMENT OF THE ARMY
FORT MONMOUTH FIELD OFFICE
109TH MILITARY INTELLIGENCE GROUP
P. O. BOX 176, EATONTOWN, NEW JERSEY 07724

QUARTERLY PROGRESS REPORT NUMBER 15

Period: 1 September 1973 to 10 December 1973

WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM I-S1/PO
AUTH Para 1-603 DOD 5200.1R

SUBJECT: CENTRAL TAXI (U)

1.(U) CIRCUMSTANCES:

On 10 December 1973, Quarterly Progress Report Number 15 was presented orally to LTC Richard O. Aamot, Chief, Security Office, US Army Electronics Command (ECOM), Fort Monmouth, New Jersey, in LTC Aamot's office; no others were present.

2.(U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. The Lead and Development Report mentioned in Quarterly Progress Report Numbers 13 and 14 (IC-B-075 (T)) was approved by the US Army Intelligence Command. Recruitment of this prospective confidential source has been delayed, however, due to his heavy travel schedule. The Project Liaison Officer recently arranged a meeting between the PLO, the Project Control Officer and this prospective source, which will take place on 12 December 1973. His recruitment will be effected at this time.

b. The new PCO is now on station and has re-contacted all CENTRAL TAXI confidential sources at least two times. The sources promised their continued cooperation with the new PCO.

c. The name of the program has been changed from Aggressive Counterintelligence Program (ACIP) to Counterintelligence Screening Program (CISP).

d. Emphasis continues on spotting, assessing and recruiting conventional sources. A vigorous spotting and assessing effort was implemented by the PLO during the reporting period. The names of nine prospective conventional sources were forwarded by the Fort Monmouth Field Office on 23 October 1973 to the 109th MI Group Headquarters requesting contact approval. Approval was granted, and to date, the PLO has contacted and recruited three of these sources.

e. Due to the move of ECOM/Philadelphia to Fort Monmouth, the mission of the ECOM/Philadelphia CISP will be incorporated into CENTRAL TAXI.

3.(U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

a. On 2 November 1973, information was received that GS-4 FILE CLERK [b6] (see Quarterly Progress Report Numbers 11, 12 and 13) was separated from Government

DEALS IN GUNS — TO BLACKS FROM WASH (40) CONFISCATED BY LOCAL POLICE

cc: [illegible]

322

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

Service and is no longer an employee at ECOM, Fort Monmouth. (CR-09-109-MON, re IC-B-072, dated 6 November 1973).

b. On 2 November 1973, information was received that ELECT TECH GS 11 b6 (see Quarterly Progress Report Numbers 11 and 12) allegedly continues to be involved in narcotics traffic. (CR-09-109-MON, re IC-B-072, dated 6 November 1973).

SUBJECT

c. On 2 November 1973, information was received that a US Army truck had been seen delivering unidentified articles on a weekly basis to a residence on Victor Avenue, West Long Branch, NJ, for approximately five months. This information was passed to CID, Fort Monmouth, for possible exploitation. (CR-09-109-MON, re IC-B-072, dated 6 November 1973).

d. On 5 December 1973, information was received that Ray Shields, later determined to be Sherman Ray Shields, DAC, b6 GS-11, Electronics Technician, Electronics Devices Branch, Production Engineering Division, Directorate of Research, Development and Engineering, ECOM, Fort Monmouth, was a heavy drinker of alcoholic beverages. An example of Shields' drinking problem was cited. On one occasion Shields came to work inebriated, and after being confronted by his supervisor, proceeded to urinate all over himself. (CR-10-109-MON, re IC-B-072, dated 7 December 1973; and Agent Reports by Special Agents Jerome A. Britton and Charles Grantham re Sherman Ray SHIELDS).

4. COMMENTS, REMARKS AND RECOMMENDATIONS:

a. Reference paragraphs 2a, 2b and 2d above: LTC Aamot expressed deep satisfaction with the progress of CENTRAL TAXI. He also stated that he intended on officially commending everyone connected with the CENTRAL TAXI CISP prior to his retirement in mid-1974.

b. Reference paragraph 2d above: Of the three conventional sources recruited, two are employees of the Electronic Warfare Laboratory, ECOM's most sensitive activity and previously void of source coverage; the third conventional source is employed with the Maintenance Directorate, originator of the majority of ECOM's security violations, also previously without source coverage.

c. Reference paragraph 3b above: LTC Aamot was advised that MAJ Quintarelli, Fort Monmouth Field Office Commander, and the PLO will pass the information concerning b6 alleged continued connection with narcotics to an appropriate agency.

d. Reference paragraph 3d above: LTC Aamot stated that he would handle the matter with utmost discretion.

Jerome A Britton

JEROME A. BRITTON
CW3, USA
323 PLO, CENTRAL TAXI

Page 1822 of 3957

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR SEA INSCOM-F01/PO
AUTH Para 1-603 DOD 5200.1R

DEPARTMENT OF THE ARMY
FORT MEADE FIELD OFFICE, 109TH MILITARY INTELLIGENCE GROUP
FORT MEADE, MARYLAND 20755

ICGP-B-FM

19 December 1973

SUBJECT: Operation GONDOLA STAR (U)

WARNING NOTICE: SENSITIVE SOURCE AND METHODS INVOLVED

QUARTERLY PROGRESS REPORT NUMBER
Period 15 September 1973 to 15 December 1973

1. (U) CIRCUMSTANCES: On 29 November 1973, LTC Leroy Walton, Chief of Security, Aberdeen Proving Ground, (APG), MD was given the initial ICIP briefing and a progress report by the undersigned. Mr. Harry A. Mencke, Installation Intelligence Officer, APG and CPT Charles H. Lightner, Deputy Commander, Fort Meade Field Office, 109th MI Group, Fort Meade, MD were present. On 5 December 1973, COL Walter R. Harris, Commanding Officer, APG was given a progress report; Mr. Mencke was also present at this meeting.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. This operation was inactive from the early spring of 1973 to October 1973. The Project Control Officer was reassigned during the spring of 1973 and the position was vacant until October 1973. The Project Liaison Officer retired in July 1973 and this position was vacant until November 1973. Both the new PCO and PLO are now in place and actively pursuing this operation.

b. Operation GONDOLA STAR (U) has two active covert Sources. The PCO has recontacted each Source and started a period of building rapport between the Source, PCO and Military Intelligence. During this period, the PCO is also concentrating on verifying placement and access, operational training and assigning current EEI. Initially, both Sources appear to be responding well to the PCO.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED: No significant counterintelligence information was developed during the reported period.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS:

a. Subject OPLAN is currently under revision. Strong consideration is currently being given to the consolidation of operations GONDOLA STAR (U) and CANAL LOOP (U) since Aberdeen Proving Ground and Edgewood Arsenal consolidated into one installation on 1 July 1971. A status report will be

324

~~CONFIDENTIAL~~

CLASSIFIED BY: CDR USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY: X
DECLASSIFY ON: Cannot be determined

~~CONFIDENTIAL~~

submitted to Headquarters, 109th MI Group by 6 January 1974.

b. This PLO has initially placed emphasis on re-establishing liaison and acquiring updated information in support of this operation. Liaison has been established with both the headquarters and security offices of Aberdeen Proving Ground and Edgewood area, Aberdeen Proving Ground. Liaison is also in effect with both Military Police offices, the local FBI office, state police and the Harford County Sheriff's Office. Effort will be given to the development of additional Confidential and Conventional Sources during the next quarters. This PLO has served two pervious tours of duty at Aberdeen Proving Ground and is a native of Harford County; consequently, much personal liaison was already established when this PLO was assigned.

c. COL Harris, LTC Walton and Mr. Mencke have expressed strong interest in the support available through ICIP and have offered their full cooperation.

RICHARD L. GREIDER
Project Liaison Officer
Briefer

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

[redacted]

DEPARTMENT OF THE ARMY
FORT MONMOUTH FIELD OFFICE
109TH MILITARY INTELLIGENCE GROUP
P. O. BOX 176, EATONTOWN, NEW JERSEY 07724

REGRADED UNCLASSIFIED
ON SEP - 8 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

QUARTERLY PROGRESS REPORT NUMBER 14

Period: 1 September 1973 to 30 November 1973

SUBJECT: Operation GONG SILK (U)

~~WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED~~

1. (U) CIRCUMSTANCES:

On 6 December 1973, Quarterly Progress Report Number 14 was presented orally to COL Jonathan L. Holman, Commander, Picatinny Arsenal (PA), Dover, New Jersey, and to Mr. John R. Greffe, DAC, Chief, Security Office, PA. Greffe is the CISP Coordinator for PA. The briefing was included in a liaison visit made by COL Charles E. Thomann, Commander, 109th Military Intelligence Group, Fort George G. Meade, Maryland. The primary purpose of this liaison visit was for COL Thomann to explain to COL Holman the methodology and purpose of the CISP, and to discuss conventional source limitations imposed by COL Holman during Quarterly Progress Report Briefing #3 on 6 September 1973. Other 109th MI Group representatives in attendance were LTC Glenn E. Vornsand, Commander, Northern Area Control Office; MAJ Nicholas F. Quintarelli, Commander, Fort Monmouth Field Office; MAJ Hugh Fitzpatrick, Assistant Group Operations Officer; and WO1 Eugene H. McNally, Project Liaison Officer, PA.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. When briefed on the CISP on 6 September 1973 (reference Quarterly Progress Report #13), COL Holman expressed apprehension over the establishment of a conventional source program on his installation. As a result, he imposed the requirement that the names of all potential sources be coordinated in advance with his Security Officer, Mr. Greffe. Greffe had later stated that initially he would want to coordinate the selection of all conventional sources directly with COL Holman. Because there was a question as to the advisability of taking such action, PLO was instructed to begin spotting and assessing potential conventional sources; to complete the necessary investigative checks on those individuals selected; but to hold contact in abeyance until the limitations imposed by COL Holman could be resolved. During the reporting period, PLO selected and completed the investigative checks on 12 civilian employees within the target area at PA. Since initiation of the checks, one of the individuals has retired from government employment, and his file has been eliminated. PLO has formulated a conventional source contact approach plan, and has coordinated it with the Commander, Fort Monmouth Field Office.

b. The new Project Control Officer is now on station and has recontacted all GONG SILK confidential sources. The sources pledged their continued support to the new PCO.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

326

[redacted]

Classified by [redacted]
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY [redacted]
DECLASSIFY ON [redacted]

Incl 29

~~CONFIDENTIAL~~

a. On 4 September 1973, an employee of the Aeroballistics Branch, Engineering Science Division, Feltman Research Laboratory, PA, visited the Security Office and stated that he believed that another employee possibly was tampering with equipment in the wind tunnel. PLO interviewed this unsolicited source on 5 September 1973 and on 20 September 1973 when he returned to relate further information. Additionally, a co-worker visited PLO on 21 September 1973, at the apparent encouragement of the individual who made the initial visit. These visits were recorded in Agent Reports, Subject: Possible Tampering of Equipment in Wind Tunnel, Engineering Science Division, Aeroballistics Branch, Experiment Evaluation Section, Feltman Research Laboratory, Picatinny Arsenal, Dover, New Jersey 07801, signed by PLO and dated: 4 September 1973, phase designation (OFFICIAL SOURCE); 6 September 1973, phase designation (MISCELLANEOUS); 20 September 1973, phase designation (MISCELLANEOUS); and 24 September 1973, phase designation (MISCELLANEOUS). Related reports were Agent Report, Subject: b6, CIV, b6 DPOB: b6 dated 4 September 1973, phase designation (201 FILE CHECK), signed by Thomas P. Ciccarelli, 109th MI Group; and Agent Report, Subject: SWETZ, Andrew J., CIV, b6 DPOB: 2 July 1920, Franklin, New Jersey, dated 10 September 1973, phase designation (201 FILE CHECK), signed by PLO. Information contained in all reports was provided to the Security Office, PA.

b. On 5 November 1973, a telephone call was received by the Office of the Army Materiel Command, Project Manager for Selected Ammunition, PA, from an individual who desired information regarding names and addresses of US Ammunition contractors. After telling the caller that he would check into the request and return the call, the employee receiving the call obtained the name and address of the caller and reported the matter to the Security Office, PA. Initial inquiries were made by the PLO and the 109th MI Group SECAP representative and the results of the inquiry were relayed to the Security Office, PA. The inquiry is reported in Agent Report, Subject: Request for List of Munitions Contractors in the United States, dated 6 November 1973, phase designation (MISCELLANEOUS), signed by PLO.

4. (U) (C) COMMENTS, REMARKS, AND RECOMMENDATIONS:

a. COL Holman obviously recalled the details of the last briefing, and indicated that he had given thought to a conventional source program at PA. His attitude was that although he was unaware of any threat, and did not feel that there was a threat, it would do no harm to have this preventive detection program implemented; therefore, he readily recommended that the conventional source program begin. COL Thomann gave an in-depth explanation of how the 109th Military Intelligence Group could be of assistance in the CISP and other fields, and COL Holman was impressed with the discussion and felt certain that those in Military Intelligence were the experts in the field. COL Holman was assured that before an individual would be selected as a potential conventional source, an extensive background check would be completed and that mature judgment would be employed throughout the operation. It was mutually agreed that the names of prospective conventional sources would be verbally cleared through Mr. Greffe, but that no list would be provided or maintained by the Security Office. COL Holman requested that if a "flap" appeared imminent during a contact, that he be immediately notified by PLO so that he could contact the individual and placate him. COL Holman was assured that this would be the procedure.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

[redacted]

b. Both COL Holman and Mr. Greffe appeared highly pleased with the command visit, and to have a proper awareness of the CISP. PLO has been given permission to initiate contact with the prospective conventional sources by HQ, 109th MI Group. Contacts will be effected on a deliberate "one-by-one" basis commencing mid December 1973. Because of this command visit, PLO feels that the obstacles have been removed and the operation can progress smoothly.

for Nicholas F. Quintarelli, Mgr
EUGENE H. McNALLY
WO1, USA
Project Liaison Officer

Cys Furn:
NACO
PCO
PLO, PA
FMFO

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

[redacted]

Page 1827 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
FORT MEADE FIELD OFFICE, 109TH MILITARY INTELLIGENCE GROUP
FORT MEADE, MARYLAND 20755

ICGP-B-FM

REGRADED UNCLASSIFIED ON SEP - 5 1997 BY CDR USAINSCOM FOI/PO AUTH Para 1-603 DOD 5200.1R

19 December 1973

SUBJECT: Operation CANAL LOOP (U)

~~WARNING NOTICE - SENSITIVE SOURCES AND METHODS INVOLVED~~

QUARTERLY PROGRESS REPORT NUMBER
Period 15 September 1973 to 15 December 1973

1. (U) CIRCUMSTANCES: On 29 November 1973 LTC Leroy Walton, Chief of Security, Aberdeen Proving Ground, (APG), MD was given the initial ICIP briefing and a progress report by the undersigned. Mr. Harry A. Mencke, Installation Intelligence Officer, APG and CPT Charles Lightner, Deputy Commander, Fort Meade Field Office, 109th MI Group, Fort Meade, MD were present at the briefing. On 5 December 1973 COL Walter R. Harris, Commanding Officer, APG was given a progress report; Mr. Mencke was also present at this meeting.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. This operation was inactive from the early spring of 1973 to October 1973. The Project Control Officer was reassigned during the spring of 1973 and the position was vacant until October 1973. The Project Liaison Officer retired in July 1973 and this position was vacant until November 1973. Both the new PCO and PLO are now in place and actively pursuing this operation.

b. Operation CANAL LOOP (U) has five active covert Sources. The PCO has recontacted each source and started a period of building rapport between Source, PCO, and Military Intelligence. During this period, the PCO is concentrating on verifying placement and access, operational training, and assigning current EEI. All Sources initially appear to be responding well to the PCO.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED: No significant counterintelligence information was developed during the reported period.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATION:

a. Subject OPLAN is currently under revision. Strong consideration is currently being given to the consolidation of Operations GONDOLA STAR(U) and CANAL LOOP (U) since Aberdeen Proving Ground and Edgewood Arsenal consolidated into one installation on 1 July 1971. A status report will

329

~~CONFIDENTIAL~~

CLASSIFIED BY: COMBINED
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY: 5
DECLASSIFY ON: Group 4 Restricted

~~CONFIDENTIAL~~

be submitted to Headquarters, 109th MI Group by 6 January 1974.

b. This PLO has initially placed emphasis on re-establishing liaison and acquiring updated information in support of this operation. Liaison has been established with both the headquarters and security offices of Aberdeen Proving Ground and Edgewood area, Aberdeen Proving Ground. Liaison is also in effect with both Military Police offices, local FBI office, state police and the Harford County Sheriff's Office. Effort will be given to the development of additional Confidential and Conventional Source during the next quarters. This PLO has served two previous tours of duty at Aberdeen Proving Ground and is a native of Harford County; consequently, much personal liasion was already established when this PLO was assigned.

c. COL Harris, LTC Walton and Mr. Mencke have expressed strong interest in the support available through ICIP and have offered their full cooperation.

d. COL Kenneth L. Stahl was assigned as the Commanding Officer, Edgewood Area, APG in September 1973. Since he had not been given the initial ICIP briefing, he was not given a progress report on 21 December 1973.

for Richard L. Greider

RICHARD L. GREIDER
Project Liaison Officer
Briefer

REGRADED UNCLASSIFIED
ON SEP 16 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

330

~~CONFIDENTIAL~~

Page 1829 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
902D MILITARY INTELLIGENCE GROUP
P. O. BOX 113
FALLS CHURCH, VA. 22046

ICGP-H/PCF-SOS

13 December 1973

SUBJECT: CENTURY SQUAD (U)

Commander
United States Army Intelligence Command
ATTN: ICDO-OP
Fort Meade, Maryland 20755

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

1. (U) Reference letter, USAINTC, ICDO-OP, 15 October 1973, subject: Aggressive Counterintelligence Program (C).

2. (U) Recapitulation of Operational Progress:

a. Official Military Personnel Files (OMPF) for ten (10) individuals appearing to meet the criteria for recruitment as a confidential source have been received from The Adjutant General's Office (TAGO). Meticulous review of these files is currently in progress.

b. Local and National Agency Checks concerning these individuals have been requested through channels established by the Liaison Branch, 902d MI Group. It is anticipated that the results of these checks will be forthcoming during the next reporting period.

c. Files maintained by the Civilian Personnel Office, The Pentagon, were examined concerning 17 individuals assigned to the target agency. Evaluation of the data contained in these files continues. Concurrently with this vetting process, Local and National Agency Checks were requested. It is anticipated that the results of the checks will be received during the next reporting period.

d. Additional identifying data on selected individuals assigned to the target agency has been submitted to the Investigative Records Repository. This information should resolve the problems encountered in dossier retrieval.

e. Attached as an inclosure is a report of counterintelligence inspection conducted at the target agency from 29 October to 5 November 1973.

RICHARD F. JUDGE
LTC, MI
Deputy Commander

1 Incl

CLASSIFIED BY as DR USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

~~CONFIDENTIAL~~ 331

Incl 27

[redacted]

REPORT OF COUNTERINTELLIGENCE INSPECTION
OF
United States Army Management Systems Support Agency
Room BD 1028, The Pentagon

SECTION I. INTRODUCTION

1. An announced counterintelligence inspection of the United States Army Management Systems Support Agency (USAMSSA), Room BD 1028, The Pentagon was conducted during the period 29 October through 5 November 1973, by the following Special Agents of the Pentagon Counterintelligence Force, 902d Military Intelligence Group:

William H. J. Count

George M. Vaughn.

2. Captain James K. Clements, Security Manager, acted as contact for and assisted in coordinating the activities of the inspection.

3. The last counterintelligence service was conducted during the period 21 to 25 August 1972.

SECTION II. SCOPE

4. This inspection included an examination of the degree of compliance with DOD Information Security Program Regulation 5220.1R and AR 380-5 of the following offices of USAMSSA:

Headquarters, Management and Administrative Support Group
Scientific Systems Division
Systems Development Division
Operations Division

5. USAMSSA has on hand approximately 850 SECRET documents and approximately 20 linear feet of CONFIDENTIAL material. No TOP SECRET documents are maintained within the USAMSSA.

SECTION III. FINDINGS AND RECOMMENDATIONS

6. There are no uncorrected or repeated findings.

7. Current Findings: No major deficiencies or shortcomings were noted during the inspection. Minor administrative deficiencies were corrected on the spot.

8. Physical Security: Only those aspects of physical security relating to classified storage were inspected in conjunction with this service. Four of the containers utilized for the storage of classified material do not meet the minimum requirements set forth in paragraphs 5-101 and 5-102, DOD Information Security Program Regulation 5200.1R. USAMSSA has requisitioned approved security containers to replace the unapproved containers. The unapproved containers are under 24-hour observation by USAMSSA personnel.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

[redacted]

332

SECTION IV. COMMENTS

9. The overall security posture of the serviced area is excellent. The USAMSSA Security Education Program is considered adequate. Incoming personnel are briefed concerning the handling, storage, and transmission of classified information. In addition, all personnel are given a periodic review to determine their compliance with existing security regulations. USAMSSA is currently revising its existing SOP to enhance the overall security posture. Reproduction of classified material is held to a minimum consistent with operational necessity. A copy of the restrictions imposed on reproduction of classified material is posted near the reproduction machine. The USAMSSA requires a 100% monthly inventory of all SECRET documents recorded on the Division Log. Additionally, the USAMSSA requires a doublecheck of each item of equipment within the individual offices and that DAS Form 11 (doublecheck List) be signed and maintained on a daily working basis. The duty officer is required to carry numerous keys during his after duty checks. Master keys would better serve this purpose. The Pentagon Custodial Engineers have such master keys and arrangements could be made with them to obtain master keys for the offices within the unit. The USAMSSA needs to implement a preventive-maintenance program on its security containers, as handles on several security containers are loose.

SECTION V. EXIT BRIEFING

10. All aspects of this service were discussed during an exit briefing on 5 November 1973 with Captain James K. Clements, Security Manager.

/BYRON W. HUNT
LTC, MI
Commanding

FOR OFFICIAL USE ONLY

CONFIDENTIAL

DEPARTMENT OF THE ARMY

WASHINGTON FIELD OFFICE
109th MILITARY INTELLIGENCE GROUP
WASHINGTON, D.C. 20319

IN REPLY REFER TO
ICGP-B-WA

13 December 1973

QUARTERLY PROGRESS REPORT NUMBER 1

Period: 25 October 1973 to 13 December 1973

WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED

SUBJECT: Operation Lanyard Mood

1. (U) CIRCUMSTANCES:

On 25 October 1973, OPLAN Lanyard Mood was formally re-activated in a visit to MAJ Clyde Bryant, Security Officer, Defense Language Institute East Coast (DLIEC), by MAJ D.N. Kappel, Commander WFO; CW3 Clarence E. Barker, Liaison Officer, WFO; and CW2 Guy J. Battiste II, Project Liaison Officer (PLO), DLIEC. On 30 October 1973, PLO briefed MAJ Bryant on the CISP. It was agreed that the briefing of the Commander, DLIEC, should be delayed until the Oplan was rewritten and a positive approach to the program was developed. To date, all meetings with MAJ Bryant have been to further that purpose.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

Screening of personnel at DLIEC has begun for the purpose of identifying those individuals whose backgrounds and/or activities might fall within the scope of the EEI in the Oplan, as well as those individuals who may be considered prospective sources in the future.

3. (C) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

Referred

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS:

The revised Oplan for Lanyard Mood was submitted to Headquarters, 109th MI Group on 5 December 1973. Pending approval of the Oplan, the PLO will continue laying the groundwork for the operation at DLIEC, and screening personnel files to determine those personnel who might be of operational interest. The formal briefing of the Commander, DLIEC, has not been scheduled, but a target date for the briefing is within the first two weeks of January 1974. DLIEC has proven in the past to be a successful CISP target,

334

Classified by: CSA, ...
Exempt from ..., Para ..., ... 11652
Declassify on: ...
Declassify only ...

CONFIDENTIAL

Ind 3)

~~CONFIDENTIAL~~

and can be as productive in the future if approached properly. The structure of DLIEC, being divided into separate departments for each language, results in the departments becoming cliques of persons from similar backgrounds or countries, and therefore the instructors have little contact with persons outside their own department. This creates a more delicate situation than normal,and means that the operation must be approached slowly and positively, as rushing into something might result in a case of bad judgement and turn the situation from delicate to explosive.

GUY J. BATTISTE II
CW2, MI
Project Liaison Officer

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

~~CONFIDENTIAL~~

Page 1834 of 3957

CONFIDENTIAL

DEPARTMENT OF THE ARMY
SYRACUSE-SENECA FIELD OFFICE
109TH MILITARY INTELLIGENCE GROUP
PO BOX 73 SYRACUSE NEW YORK 13201

ICGP-B-SY

11 December 1973

QUARTERLY PROGRESS REPORT NUMBER 1
Period 1 October 1973 to 31 December 1973

SUBJECT: Operation CANINE PLATE (U)

~~WARNING NOTICE SENSITIVE SOURCES AND METHODS INVOLVED~~

1. (U) CIRCUMSTANCES: On 16 November 1973, an initial briefing was given concerning the CISP at Seneca Army Depot, Romulus, New York, 14541, code named CANINE PLATE. Present for the briefing were COL Allen H. Light, Jr., Depot Commander; MAJ Noel L. Weaver, former Syracuse-Seneca Field Office Commander; CPT Denis F. Ausflug, present FO Commander; and CW2 Francis L. McGinn, Jr., CANINE PLATE Project Liaison Officer.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD: In the briefing of 16 November, COL Light was informed of the intent and aims of CANINE PLATE, reference MFR, 6 December 1973, re: CANINE PLATE. No other overt activity has taken place. See paragraph 4 below for additional remarks.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED: None.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS: The project liaison officer has been on station since December 1972. In the past year, through associations formed at social activities at the Seneca Army Depot Officers Club, the only area in which the PLO has sufficient reason for contact with depot personnel, three or four likely prospects for conventional sources have been spotted. An approach will be made as soon as one very significant problem has been resolved. It is almost certain, because of the very high degree of security consciousness of depot personnel, that any approach by the PLO will be treated with suspicion and reported to the depot security officials as a possible penetration attempt, or as a test of their SAEDA reporting system. This is directly against the wishes of COL Light, who wants knowledge of CANINE PLATE to be confined to himself. This leads to the conclusion that all prospective sources, at the time of recruitment, must be directed to ask COL Light any questions they may have concerning the PLO's veracity. This would reveal the identity of the sources

Classified by CDR USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON [illegible]

REGRADED UNCLASSIFIED
SEP 5 1997
ON
BY CDR USAINSCOM FOI/PO
AUTH Para 1-603 DOD 5200.1R

336

CONFIDENTIAL

CONFIDENTIAL
USAINTC

to the Depot Commander. The chances of having the project revealed with subsequent embarrassment to the Depot Commander and to the 109th MI Group are too likely to be ignored. Disclosure of the identity of conventional sources, when necessary, does not appear to contravene existing regulations; the same situation would apply to confidential sources although disclosure of their identity can only be done with the permission of the Commander, USAINTC. Fuller discussions of this matter will be held on 14 December 1973 with the Commander, Northern Area Control Office, at which time opinions and advice will be solicited.

DENIS F. AUZFLUG
CPT, MI
FIELD OFFICE COMMANDER

REGRADED UNCLASSIFIED
ON 5 SEP 1991/PO
BY CDR USAINSCOM
AUTH Para 1-603 DOD 5200.1R

CONFIDENTIAL
USAINTC

DEPARTMENT OF THE ARMY
HEADQUARTERS 115TH MILITARY INTELLIGENCE GROUP
PRESIDIO OF SAN FRANCISCO, CALIFORNIA 94129

REPLY TO ATTENTION OF:

ICGP-F-SO

14 December 1973

QUARTERLY PROGRESS REPORT NUMBER 1

For the Period 10 September 73 to 10 December 73

SUBJECT: ICIP CENTAUR RACE (U) SENSITIVE SOURCES AND METHODS INVOLVED

1. (U) CIRCUMSTANCES: On 5 December 1973, MAJ Glen E. Robinson, Fort Lewis Field Office Commander, briefed LTC Homer Pickens, ACofS, 9th Infantry Division and Fort Lewis, representative of the Commanding General, 9th Infantry Division and Fort Lewis, on the progress of Internal Counterintelligence Program (ICIP) CENTAUR RACE.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

a. A study concerning insertion of sources into the Fort Lewis military community has been completed and results will be forwarded by separate correspondence.

b. Aggressive screening, spotting, and assessment of Installation conventional sources and potential Confidential Sources is continuing and has been expanded to include all targets on Fort Lewis.

c. The first Source Lead and Development Report (SLDR) for ICIP CENTAUR RACE will be prepared and submitted within 30 days.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED: There has been no significant counterintelligence information developed through the ICIP to date due to the lack of formally recruited sources.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS: LTC Pickens, ACofS, 9th Infantry Division and Fort Lewis, continues to have an interest in ICIP CENTAUR RACE, and has cooperated with Fort Lewis Field Office to the fullest extent. It is the desire of the Commanding General, 9th Infantry Division and Fort Lewis, not to be present for briefings unless significant counterintelligence information is to be discussed.

REGRADED UNCLASSIFIED
SEP -5 1997
ON
BY CDR USAINSCOM FOI/PO
IAW EP 380-380 CCD 5200.1R

EUGENE F. OVERHOLT
MAJ, MI
Acting Operations Officer

338

Incl 23

[redacted]

3 December 1973

QUARTERLY PROGRESS REPORT NUMBER 2

CENTAUR SALE

Period 13 October 1973 to 28 November 1973

1. (U) CIRCUMSTANCES:

On 28 November 1973, CW3 James E. Harnish, Project Liaison Officer (PLO), MERDC, provided Colonel Tehno R. Hukkala, Commander, MERDC, Leslie L. Askew, Security Officer, MERDC, and Edna T. Payne, Assistant Security Officer, MERDC, with the 2nd Quarterly CISP Briefing. The briefing was presented one week earlier than projected due to the uncertainty of the Commander's pre-holiday December schedule. The briefing was well received with no problems encountered.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

Six prospective Sources were spotted during this period.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

During this period three Agent Reports were produced. These reports were as follows: b6, DPOB: b6 SSG b6, report submitted 26 October 1973, concerned suitability due to indebtedness; b6, PDOB: b6 b6 CIV b6 report submitted 5 November 1973, concerned suitability due to alcohol drinking problem; b6 DPOB: b6 b6 SSN b6 report submitted 21 November 1973, concerned a threatening telephone call.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS:

At the present time there is no approved CPLAN available for this project at the Washington Field Office. The next Quarterly Briefing of the Commander, MERDC, will be within the first two weeks of March 1974, and will realign the briefing schedule. MERDC is a good CISP target, and has the potential for a successful project, however the PLO's time on site is limited due to being PLO at another installation also. To be more effective MERDC must be a full time project.

James E Harnish

JAMES E. HARNISH
CW3
Project Liaison Officer

Classified by: CO USAINTC
Exempt from [illegible] Executive Order 11652
Exemption category: 2
Declassify on: [illegible]

339

Incl 24

[redacted]

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY USAINSCOM FOIPA
Auth Para 4-102 DOD 5200.1R

3 December 1973

QUARTERLY PROGRESS REPORT NUMBER 2

SUBJECT: CENTAVO KID

Period 12 October 1973 to 12 November 1973

WARNING NOTICE-SENSITIVE SOURCES AND METHODS INVOLVED

1. (U) CIRCUMSTANCES:

On 12 November 1973, the Commander, Harry Diamond Laboratories(HDL), was briefed on the revised CENTAVO KID OPLAN. Present at the briefing were, Colonel David W. Einsel, Commander, HDL, Major D.N. Kappel, Commander, WFO, 109th MI Group, Major Thomas R. Mooney, Executive Officer, HDL, CW3 James E. Harnish, PLO, Alfred F. Schneider, Security Officer, HDL, and James H. Yeick, Assistant Security Officer, HDL. Due to the close proximity between this briefing and the December Quarterly Briefing, both were combined. The briefing was well received and no problems were encountered. The next Quarterly Briefing will be delivered within the first two weeks of March 1974, and will realign the briefing schedule.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING THE PERIOD:

Since the approved and revised OPLAN has been available, six potential Sources are undergoing Local Agency Checks. A problem in cooperation as indicated in Quarterly Progress Report Number 1 within the HDL Security Office has been resolved and cooperation from the Security Office has improved.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED:

One Agent Report was produced during this periodas follows: LAMERS, Guillermo B., DPOB: 29 January 1935, Buenos Aires, Argentina, CIV b6 , b6 report submitted 19 October 1973, concerned suitability information.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS:

None.

James E Harnish

JAMES E. HARNISH
CW3
Project Liaison Officer

Classified by: CO USAINTC
Exempt from General Declassification Schedule of Executive Order 11652.
Exemption category: 2
Declassify on: UNDETERMINED

340

REGRADED UNCLASSIFIED
ON SEP 5, 1997
BY USAINSCOM FOIPA
Auth Para 4-102 DOD 5200.1R

Incl 25

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
FORT CARSON FIELD OFFICE
115TH MILITARY INTELLIGENCE GROUP
COLORADO SPRINGS, COLORADO 80901

ICGP-F-CA

10 December 1973

QUARTERLY PROGRESS REPORT NUMBER 1.

PERIOD: 11 September 1973 to 10 December 1973

~~WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED.~~

SUBJECT: Operation Canary Stone (U)

1. (U) CIRCUMSTANCES.

Effective 1 December 1973, the Dugway Proving Ground Resident Office was established and became operational. SFC Pete A. Gonzales (PLO) has been assigned to the Dugway Resident Office. ~~and will documented as a Resident Office for operational purposes.~~ To date, the PCO has not been assigned to Operation Canary Stone, therefore, no progress briefing was presented to the Commander, Dugway Proving Ground, pertaining to the past quarter's activities.

2. (U) RECAPITULATION OF OPERATIONAL PROGRESS DURING PERIOD.

No operational assets were utilized during the reporting period.

3. (U) SIGNIFICANT COUNTERINTELLIGENCE INFORMATION DEVELOPED.

None has been developed during the reporting period.

4. (U) COMMENTS, REMARKS, AND RECOMMENDATIONS.

The Dugway Resident Office is located in Room 2204, Building 5234, Dugway Proving Ground, Dugway, Utah. The Intraservice Support Agreement between the 115th MI Group and Dugway Proving Ground has been finalized and is in the process of being signed by appropriate unit representatives.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM F01/PO
AUTH Para 1-603 DOD 5200.1R

Timothy E. Dowling, CPT
FOR: JOHN C. SIMS, JR
LTC, MI
Commanding

~~CONFIDENTIAL~~

CLASSIFIED BY CDR USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY
DECLASSIFY ON

341

Inc 1 21

THIS MUST REMAIN T O P D O C U M E N T

DOSSIER NO. ZF011946W
Vol 4 of 7 Vols

As of 18 Sep 85 (Date) all material included in this file conforms with DA policies currently in effect.

Delmar Smith (Signature) 18 Sep 85 (Date Signed)

Delmar Smith (Printed Name) GS5 (Grade)

Reviewed for Retention
Criteria UP AR 381-10
Reviewer [illegible] Date 4 Jan 93

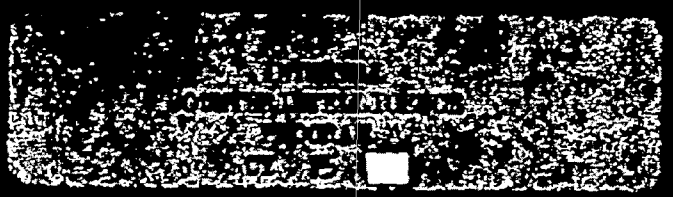
THIS MUST REMAIN T O P D O C U M E N T

IA (HQ) Form 2214
(1 Sep 78)

Replaces MIIA Fm 315, 1 Jun 75, which may be used until supplies are exhausted.

342

Best Copy Available



Page 1842 of 3957

CONTENTS

TAB	TITLE	DATE
A	Memo for VCSA from USofA, SUBJ: ICIP	21 Jan 75
B	Memo thru VCSA for USofA, SUBJ: ICIP	4 Feb 75
C	1st Ind to USAINTA, Approval of CANTER RIDE	7 Mar 75
D	Ltr from USAINTA, Evaluation of Selected Installations in Panama Canal Zone	28 Apr 75
E	Quarterly Report, 1st Qtr, CY 75	27 May 75
F	Ltr to Cdr, APGapproving continuation of GONDOLA STAR	11 Jul 75
G	Ltr to Cdr, PCF, disapproving OPlan	1 Aug 75
H	Quarterly Rpt, 2nd Qtr, CY 75	16 Sep 75
I	1st Ind to USAINTA, Approval of revised OPLAN CANARY EFFORT	15 Sep 75
J	Quarterly Rpt, 3d Qtr, CY 75	20 Nov 75
K	Memo for Record, SUBJ: ICIP CANARY EFFORT	21 Nov 75
L	Msg to USARSO on proposed ICIP	19 Nov 75
M	DF to USAINTA, Quarterly ICIP Reports	17 Dec 75

Page 1843 of 3957

~~CONFIDENTIAL~~

ICIP'S TERMINATED, AS OF FEB 75

1. CANAL ROPE - US Army Communications Command, Ft Huachuca, AZ
2. CANARY STONE - Dugway Proving Ground, UT
3. CANTINA ARCH - US Army Air Defense Center, Ft Bliss, TX
4. CANYON ROSTER - UMatilla Army Depot Activity, Hermiston, Oregon
5. CENTAUR SALE - US Army Mobility Equipment Research and Development Center, Ft Belvoir, VA
6. CENTRAL TAXI - USArmy Electronics Command, Ft Monmouth, NJ
7. CENTURY SQUAD - US Army Management Systems Support Activity, The Pentagon, Washington, DC
8. GONDOLA FLAG - US Army Electronics Proving Ground, Ft Huachuca, AZ
9. LANYARD MOOD - Defense Language Institute East Coast, Wash. Navy Yard
10. LEND TONE - Picatinny Arsenal Armaments Command, Dover, NJ
11. LENIENT CLOUD - US Army War College, Carlisle Barracks, PA
12. GONDOLA STAR - Reinstated for 6 Months.

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

DAMI-DOH

Quarterly ICIP Reports (U)

CDR, USAINTA
ATTN: MIIA-SO
FT MEADE MD 20755

DAMI-DOH

LTC Haendle/mjb/56159

1. (U) Reference, message, DAMI-DOH, 032115Z Dec 75.

2. (U) Attached for your files is a copy of the INFORMATION MEMORANDUM to the Under Secretary of the Army (less inclosures) which forwarded summaries of the nine on-going CONUS ICIP operations as submitted by your headquarters. The summary pertaining to a proposed ICIP by the 66th MI Group in support of USASA was not included in this submission. Upon receipt of a response to the above referenced message, a decision will be made whether to include that operation in the next quarterly report.

3. In staffing the Quarterly ICIP Report within OACSI, the Acting Director of Intelligence Operations noted that many of the summaries of on-going actions contained too many details of individual character/behavior issues. In future quarterly reports, suitability-type information pertaining to individuals covered by the ICIP project should be either eliminated or summarized in general comments.

4. On a seperate matter, when the ACSI reinstated the ICIP CONDOLA STAR in July 1975, he indicated he would review the ICIP in six months to determine if significant information had been developed to warrant continuation of the project. It is requested that your headquarters conduct a review of this ICIP and furnish your comments and recommendations to this office by 9 January 1975.

FOR THE DIRECTOR OF INTELLIGENCE OPERATIONS:

(sgd) L. A. S[illegible]

1 Incl
as

L. A. SPIRITO
Colonel, GS
Chief, HUMINT Division

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

346

Classified by ACSI DA
EXEMPT [illegible]
SUBJECT [illegible]
EXEMPT [illegible]
DECLASSIFY [illegible]

ROUTING AND TRANSMITTAL SLIP		ACTION
TO: Col. Spratto DOA.	INITIALS	CIRCULATE
	DATE	COORDINATION
AGENDA	INITIALS	FILE
	DATE	INFORMATION
	INITIALS	NOTE AND RETURN
	DATE	PER CONVERSATION
	INITIALS	SEE ME
	DATE	SIGNATURE

REMARKS

Lee: Quarterly ICIP Report Summaries sent on to ACSI for signature, both they (some of them) contain too many details on character/behavior issues. Ask USAINTA to refine. P.F.O.

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM: MERRILL L. KELLY
Acting Director
of Intelligence Operations

DATE: 2 Dec

PHONE:

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41CFR) 100-11.206

347

GPO: 1973 OF—525-336 5041-101

[redacted]

future submissions,
and summarize kinds
of info desired, but
avoid loading with
the social/marital
misconduct for the
USec A.

MFR: [redacted]

Contacted Mr Tom Hughes, CI Division, USAREUR re: response to attached msg this date.

He indicated a response on status of I CIP msg would be sent out next week. USAREUR saw no urgency in that operation has not been finalized as they view it but will forward a proposal ~~to~~ the HQ SI when it is. I mentioned desire to include the project in ~~the~~ quarterly report if possible.

349

KVH

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

HANDLE

~~WARNING NOTICE SENSITIVE SOURCES AND METHODS INVOLVED~~

~~[illegible] ACSI DA WASH [illegible] INTEL ACCT~~

~~[illegible] WOFORN LIMDIS WARNING NOTICE SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED~~ HBG 0072 TOPIC

FROM COL IADEROSA, CHIEF, CI DIV, ODCSI, USAREUR FOR COL SPIRITO, CHIEF, CI DIV, OACSI, DA; INFO LTC GRIMES, CDR, SO DET, USAINTA.

SUBJECT: INTERNAL COUNTERINTELLIGENCE PROGRAM (ICIP) (U)

A. DA DAMI-DOH 032152Z DEC 75 (S).

B. HBG 4200 TOPIC 1714312 SEP 74 (U).

C. INT 1146-74 TOPIC 1841362 SEP 74 (U).

D. HBG 2882 TOPIC 1917552 JUN 73 (S).

E. INT 1892 TOPIC 0113402 JUL 73 (U).

F. LTR, AEAGB-CI (380), USAREUR, 14 MAY 73, SUBJECT: REQUEST FOR SPECIAL COUNTERINTELLIGENCE SUPPORT WITH ATT ENCL. DAMI-DOI-E, 29 MAY 73 (S).

G. USAINTC ICDO-OP 051703Z JUN 73 (C).

(4) -> BASED ON THE NEW POLICY CONTAINED IN REF A, THIS OFFICE WILL FORWARD OPLAN'S FOR ALL USAREUR ICIP'S, ONGOING AND PLANNED,

350

FOR ACSI APPROVAL. HOWEVER, IN THE ABSENCE OF DETAILED ARMY-WIDE GUIDANCE ON ICIP, IT IS DIFFICULT TO DETERMINE WHICH USAREUR CI PROGRAMS AND PROJECTS MEET THE CRITERIA AND DEFINITION OF ICIP AS PERCEIVED BY OACSI. IN THIS REGARD, THE FOLLOWING [illegible] CI OPERATIONS ARE DESCRIBED:

A. CARELESS TOKEN: ICIP DEVELOPED, AND IMPLEMENTED BASED UPON REF B THRU E IN SUPPORT OF DET N, USASA FIELD STA AUGSBURG, LOCATED AT RIMBACH , FRG. THE OPLAN WAS APPROVED BY CDR, USASA ON 30 JUN 75 AND BY ODCSI, USAREUR ON 15 JUL 75. THE ICIP IS IN ITS EARLY STAGES OF IMPLEMENTATION AND WHILE A NUMBER OF COUNTER-INTELLIGENCE RECRUITMENT LEADS HAVE BEEN DEVELOPED, NO FORMAL RECRUITMENT OF CONFIDENTIAL SOURCES HAS YET BEEN ACCOMPLISHED.

B. GROUP BAND: CI PROJECT BASED UPON REF F AND G INVOLVING USAINTA RECRUITMENT OF 10 STERILE SOURCES IN CONUS FOR INSERTION INTO 56TH ARTY BDE, USAREUR FOR COLLECTION OF COUNTER-SUBVERSION AND COUNTERSABOTAGE INFO. THE END OF US INVOLVEMENT IN VIETNAM AND THE CONCOMITANT SHARP DECREASE IN SUBVERSION/SABOTAGE INCIDENTS VIRTUALLY ELIMINATED THE NEED FOR THESE SOURCES. NORMAL ATTRITION HAS RESULTED IN ONE REMAINING GROUP BAND SOURCE IN USAREUR WHO IS CURRENTLY HANDLED AS A CASUAL DEFENSIVE COUNTERESPIONAGE SOURCE.

C. CERTAIN SMILE: AN ICIP IMPLEMENTED IN 1973 WITHIN CERTAIN KEY STAFF OFFICES AT HQ USAREUR IN AN EFFORT TO IDENTIFY

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[illegible] ILLEGAL CONDITIONS CONDUCIVE TO HOIS EXPLOITATION. THE [illegible] DEVELOPED CONSIDERABLE INFORMATION REGARDING GENERAL [illegible] SECURITY VIOLATIONS [illegible] AND PERSONNEL SUBJECTIVE INFORMATION; HOWEVER, THE PROJECT WAS EVENTUALLY DEEMED [illegible] AND SUPERFICIAL TO BE OF VALUE IN IDENTIFYING ACTUAL [illegible] OPERATIVES OR ACTIVITIES. CERTAIN SMILE WAS [illegible] AS AN SCIP IN 1975 AND IT'S ASSETS REDIRECTED TO- [illegible] A SCI CASUAL SOURCE PROGRAM. THIS OFFICE IS CURRENTLY PREPARING AN OPLAN FOR CINCUSAREUR APPROVAL WHICH WILL IN- VESTIGATIVELY ADDRESS THE SUSPECTED HOIS THREAT AGAINST HQ USAREUR.

D. CAREFREE TALENT: RECENT DEVELOPMENTS IN BERLIN BASED OFCO'S HAVE REVEALED INTENSE INTEREST BY SIS IN DET A, A SPECIAL FORCES UNIT STATIONED IN WEST BERLIN. MOREOVER, SIS CASE OFFICERS HAVE DISCLOSED SUFFICIENT KNOWLEDGE OF DET A TO RAISE THE POSSIBILITY OF A SUCCESSFUL SIS PENTETRATION OF DET A. BASED ON A REQUEST BY CDR, BERLIN BDE, A CONCEPT OF OPERA- TIONS (COPO) WAS FORMULATED, DESIGNED TO FULLY IDENTIFY, NEUTRALIZE OR EXPLOIT THIS APPARENT SIS THREAT THROUGH DEFENSIVE AND OFFENSIVE COUNTERESPIONAGE ASSETS, INCLUDING JUDICIOUS RECRUITMENT OF SOURCES WITHIN SPECIAL FORCES RANKS. THE COPO [illegible] APPROVED BY ODCSI, USAREUR FOR IMPLEMENTATION ON 18 SEP 78.

E. CARDINAL FLIGHT: BERLIN OFCO'S HAVE ALSO REVEALED KEEN

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1851 of 3957

INTEREST BY SIS IN USMLM ACTIVITIES/PERSONNEL AND OBVIOUS EFFORTS BY SIS TO EFFECT PENETRATION. 66TH MI GP HAS BEEN TASKED TO PREPARE A COPD DESIGNED TO NEUTRALIZED OR EXPLOIT THIS SIS ACTIVITY.

3. (U) ALTHOUGH ICIP IN CONUS IS TREATED AS A CI SERVICE, THOSE FOREIGN PROGRAMS/PROJECTS DESCRIBED IN PARA 1, SUPRA, WITH THE EXCEPTION OF GROUP BAND, ARE CONSIDRED DEFENSIVE COUNTERESPIONAGE OPERATIONS INITIATED AS THE RESULT OF DEMONSTRATED OR SUSPECTED HOIS THREATS. IN ALL CASES, APPROPRIATE COMMANDERS HAVE BEEN BRIEFED ON THE PERCEIVED HOIS THREAT AND HAVE EITHER REQUESTED OR CONCURRED WITH THE CI NEUTRALIZATION PLAN.

4. (U) THE OPLAN PERTAINING TO CARELESS TOKEN IS BEING FORWARDED TO YOUR OFFICE FOR APPROVAL; QUARTERLY STATUS REPORTS ALSO WILL BE FURNISHED

5. (U) REQUEST YOUR COMMENTS AS WHETHER EITHER OF THOSE PROJECTS DESCRIBED IN PARA 1D AND 1E, SUPRA MEET THE CRITERIA FOR ICIP AND THUS REQUIRE ACSI APPROVAL.

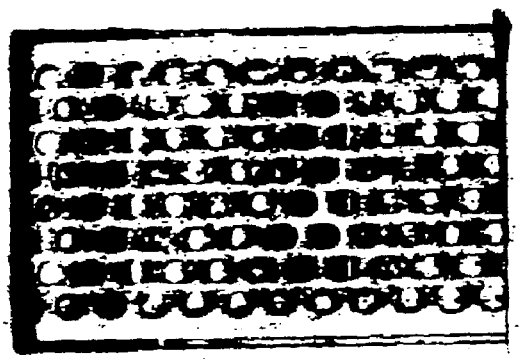
6. (U) FURTHER REQUEST DETAILED GUIDANCE REGARDING OACSI ICIP POLICY AND PROCEDURES BE FURNISHED AT AN EARLY DATE.

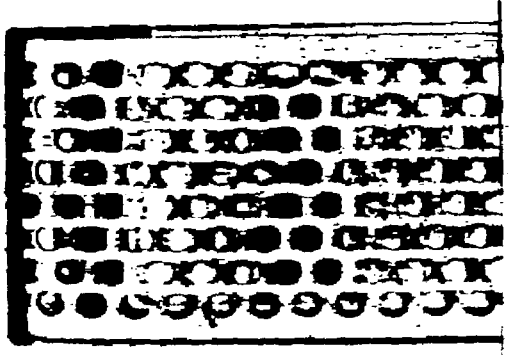
7. (U) ODCSI, USAREUR, ACTION OFFICER IS MR DAVID R. SMITH, AEAGB-CI(SO), MM 7354 (AUTOSEVOCOM 6742).

XGDS-2

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1852 of 3957





ROUTING AND TRANSMITTAL SLIP

TO		INITIALS	ACTION
1	LTC HAENDLE DAMI-DOH		CIRCULATE
		DATE	COORDINATION
2		INITIALS	FILE
		DATE	INFORMATION
3		INITIALS	NOTE AND RETURN
		DATE	PER CONVERSATION
4		INITIALS	SEE ME
		DATE	SIGNATURE

REMARKS

Per our fonecon 29 Dec 75, attached is the [illegible] of ICIP Status report from USAREUR. One of our people was given the copy during a visit to Arlington Hall Station.

Happy New Year!

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions.

FROM		DATE
JA Pennett Spec Act Sect, SOD 354		29 Dec 75

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41CFR) 101-11.206

DEPARTMENT OF THE ARMY
UNITED STATES ARMY SECURITY AGENCY FIELD STATION, AUGSBURG
APO NEW YORK 09458

IAEASC

15 December 1975

SUBJECT: Internal Counterintelligence Program Quarterly Status Report (U)

EXCLUSIVE FOR Colonel William B. Holden
Deputy Chief of Staff Security
Headquarters
U.S. Army Security Agency
Arlington Hall Station
Arlington, Virginia 22212

1. (U) Attached at inclosure 1 is the first Quarterly Status Report, for the period ending 15 October 1975.

2. (U) Your attention is invited to potential source B58,786 referred to in paragraph 5. Appropriate coordination will be effected by the 66th Military Intelligence Group, this Command and your Headquarters before utilization is effected.

FOR THE COMMANDER:

ANTHONY C. DURSO
Captain, MI
Assistant Adjutant

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by: Para 4b, AR381-12, 18Oct74
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Notification of ACSI, DA

355

CONFIDENTIAL

AEUHI-N-CE
D03130-518-75

24 October 1975

SUBJECT: Internal Counterintelligence Program (ICIP)
(QUARTERLY STATUS REPORT) (QSR)

Commander
66th Military Intelligence Group
ATTN: AEUHI-I-CI (EXCLUSIVE FOR ICIP CONTROL OFFICER)
APO 09108

1. (U) References:

a. OPLAN, 511th MI Battalion, AEUHI-N-CE, 1-75, 1 May 1975

b. AEAGB-CI(SO), DTG 151640Z July 1975, ICIP

2. (U) This is the first ICIP Quarterly Status Report, in accordance with references, covering the period ending 15 October 1975.

3. (U) General:

a. Activity at the target is in the drawdown stage, pending automation in early 1976 under the LA FAIRE VITE Program. Since 1 July 1975, personnel manning has been reduced to about 50 percent of previous target strength; most personnel have been reassigned to USASAFS Augsburg. In June 1975, an official release was made by letter to the Buergermeister (mayor) of Rimbach, which provided details of the withdrawal. Portions of the letter were reportedly published in area newspapers. A copy of the English translation of the letter to the mayor's office is attached as Inclosure 1.

b. Contrary to the letter inclosure, it appears that some target personnel in excess of the programmed approximately seven (7) individuals who will maintain and guard the automated site, may remain in the area for varying periods up to 1 July 1976. These include all personnel who

2

[illegible] OF ACSI, DA

356 REGRADED UNCLASSIFIED ON SEP 5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

AEUSI-N-CE 24 October 1975
SUBJECT: Internal Counterintelligence Program (ICIP)

are scheduled for DEROS or ETS in FY76 as funding is not available for two PCS moves in a single fiscal year. No figures were available at the time of the QSR preparation as to how many personnel would be affected, nor had it been determined what would be their duties during the approximate period 1 March-30 June 1976.

c. The USAF communications site (6913th USAF Security Squadron) located in the same area is scheduled to close at about the same time the target is automated; no USAF personnel will remain in the area. As far as can be determined, the French and Bundeswehr sites will continue to operate.

d. The seven or eight personnel scheduled to remain at the target permanently will be billeted at the top of Mount Hoherbogen, in a newly constructed building, adjacent to the present operational area. The senior individual will be an NCO, grade E6 or E7, who will probably have one of the supervisory communications equipment maintenance MOS's. Other personnel stationed there will be equipment and antenna array repair and maintenance specialists and guards. All personnel will be single or unaccompanied. At the writing of this report, none of the permanent party had been selected.

4 (U) (C) Operational Matters:

a. SMLM-F makes a reconnaissance of the Rimbach area approximately once a month. The sightings usually involve travel along the PRA perimeter roading leading north and south out of Rimbach. Perimeter roads of PRAs, excluding Autobahnen, are off limits to SMLM-F vehicles. On 3 June 1974, a SMLM-F vehicle was disabled on the access road leading to the target operational site, well within a PRA, and was assisted by a Chief Warrant Officer assigned to the target, who was not aware of the correct PRA boundary. There have been no SMLM-F detentions in the area, and none are likely, since the closest Military Police are located at Hohenfels Training Area (HTA), 80 kilometers away.

b. In March1975, during a liaison visit with MAJ Richard Douma, the target commander, the PLO was advised that MAJ b6 b6 had been transferred to Ramstein, FRG after appearing before a board to face charges of homosexuality.

c. In April 1975, SP4 b6 reported a possible SAEDA incident (Group Case 75-061P); during the subsequent investigation it was determined she had reported to Field Office Augsburg a similar approach by the same individual a year earlier. Target personnel were dubious as to the veracity of statements made by b6 who was transferred to USASAFS, Augsburg on 1 August 1975.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

AEUTI-H-CE 24 October 1975
SUBJECT: Internal Counterintelligence Program (ICIP)

d. In May 1975, MAJ Douma advised the PLO that some of the target personnel had a tendency to talk too openly about their jobs in public, and that his solution had been constant reiteration to unit personnel on the dangers of loose talk. No specifics were provided on individuals concerned. The PLO did not press for details as he considered it a command matter. MAJ Douma believed the security posture of the target was steadily improving.

e. The preliminary investigation of b6 continued, however, in low key due to the lack of credible specific allegations. b6 operates the Hoherbogen Restaurant, situated near the target administrative area. He allegedly travels regularly to CSSR to visit relatives and to attend dog shows. Target personnel patronize the restaurant regularly, primarily because of its convenient location. b6 was never reliably reported to have shown undue curiosity about target operations and personalities, but remains, nevertheless, well-informed because of overheard conversations of target personnel-customers. In June1975, b6 told the PLO he was not looking forward to the departure of the Americans because he would have to "put up" with local German customers, who were much more troublesome than target personnel. In October 1975, b6 remarked to MAJ Douma that he had made several trips to Augsburg to negotiate the purchase of a tavern there. b6 said he intended to sell the Hoherbogen Restaurant and move to Augsburg, where he will open a tavern/restaurant two kilometers from the "ASA kaserne." Activity of b6 will continue to be monitored in the Rimbach area, and if he moves to Augsburg, he should be made a target of continuing interest by Field Office Augsburg.

f. In July 1975, CPT (Chap) b6 Protestant Chaplain at HTA, advised that an individual assigned to the target had sought his spiritual guidance as a result of extreme emotional anxiety, due to his/her involvement with a group of USASA personnel who were engaged in satanic religious practices at the target. b6 revealed no details nor identities, due to the sensitivity of communications to a chaplain, however, the identity of the individual involved is believed to have been established (see para 4j, below).

g. In July 1975, two target personnel applied for Military Intelligence duties in ACGP-97. One (SP5 b6 was assisted in completion of required forms and processing/interview is in progress. The other individual (SP4 b6 will not be able to apply until December 1975, when he has 12 months remaining to DEROS. He expects to be transferred to USASAFS, Augsburg prior to that time and has been advised to initiate his processing at Field Office Augsburg.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

358

~~CONFIDENTIAL~~

Page 1857 of 3957

AEUMI-R-CE 24 October 1975
SUBJECT: Internal Counterintelligence Program (ICIP)

h. In July 1975, USASAFS, Augsburg requested agency checks on the German national intended spouse and relatives of SP4 b6 Subsequently, during a subject interview, b6 stated that his fiancee had contact, through an acquaintance, with b6, a photographer/reporter for a Furth-im-Wald newspaper and that he suspected b6 was receiving money from the CSSR for photographs of facilities in the Rimbach area. b6 had no specific reason to back up his suspicion and said it was common knowledge among target personnel. (b6 was the subject of a bilateral MI/MAD investigation in 1973 and 1974, during which none of the allegations of possible intelligence activity were substantiated.) b6 also said he personally was suspicious of fnu b6, a former member of the target unit, who operates "b6's Club" in Koetzting. b6 is curious as to the status of US installations at Rimbach and uses his US citizenship and former Army service as a method of gaining access to information from US Forces members who patronize his establishment. b6 and his activity was previously known to MI/MAD during the b6 investigation and not determined to warrant further investigation. b6 is a non-DoD affiliated US citizen.)

i. In July 1975, USASAE, Augsburg requested agency checks in Koetzting on b6 and Dr. b6, who were friendly with target personnel and who had become knowledgeable of classified defense information as a result of this relationship. There was no indication any of the b6's had attempted to elicit defense information. Agency checks failed to reveal any derogatory information concerning the b6 family; Dr. b6 was a practicing dentist in Koetzting. In early August 1975, MAJ Douma advised the PLO that in early 1975, SP4 b6 and her dependent husband, b6, a US citizen, had attempted to establish a German-American Club between target personnel and the local communities. In this connection, the b6's mentioned being acquainted with a dentist in Koetzting, nfi. Nothing of consequence ever came of the attempt to form an organization. Later, date unknown, Douma was advised by Commander, Forward Operations Battalion, Augsburg (his supervisor) of a report that b6 had discussed classified information with German acquaintances. In an interview of b6 by Douma, she admitted having discussed details of LA FAIRE VITE with her husband in early 1975, and to have mentioned the project in the presence of one b6, a German national acquaintance residing in Munich. b6 was subsequently given a written reprimand in connection with the compromise. b6 mentioned nothing about any other German acquaintances, and denied compromising any classified information to any other foreign nationals. No information was made available to Douma when he was tasked by his higher headquarters to investigate the incident, as to the identity of the German acquaintances who were supposed to have received the classified defense information. b6 departed the target on 19 July 1975 for CONUS and separation from active duty.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOIPO
AUTH PARA 1-603 DoD 5200.1-R

359

Page 1858 of 3957

~~CONFIDENTIAL~~

AEUAI-N-CE 24 October 1975
SUBJECT: Internal Counterintelligence Program (ICIP)

j. In August 1975, MAJ Douma advised the PLO that SP4 [b6] attached to the target from the 502d ASA Group as a Czech linguist Voice Intercept Specialist (98G2LCX), had exhibited severe mental trauma immediately following the departure of a close female acquaintance from the target on 30 June 1975, and had been placed on extended leave status. [b6] consulted CPT (Chap) [b6] at HTA and the USASAFS Augsburg staff chaplain, but had allegedly declined psychiatric counselling. On her return from leave, her access to classified material was to be suspended and Douma could direct [b6] to receive counselling, as he was very concerned about her emotional stability. [b6] had a DEROS of September 1975.

k. In August 1975, the PLO advised MAJ Douma that a German agency had reported a US soldier named [b6] was trafficking in drugs in Goetzting. After the PLO provided descriptive data obtained from a FRG agency, Douma identified [b6] as SP4 [b6] a Russian-linguist Voice Intercept Specialist, attached from the 502d ASA Group. Douma was requested to watch [b6] activities closely and pass any information to CID at HTA. [b6] DEROS is June 1976, putting him in the category of those mentioned in paragraph 3b, above, who may remain at the target without any specific duties.

l. In September 1975, B58,786 (who is undergoing preliminary source assessment) advised that in approximately April 1975, a female soldier traffic analyst assigned to the target, whose name he could not recall, had compromised a TOP SECRET/CRITIC/CODEWORD message to [b6] a dependent and GS-2 clerk typist in the unit administrative office. [b6] had only a Confidential clearance. The compromise although known by the target commander, was not reported to USASAFS, Augsburg.

m. No specific information has been reported to indicate that Hostile Intelligence agencies are in contact with any target personnel.

(U) Source Activity:

a. One potential source (B58,786), has been spotted at the target and is being assessed. Name traces are not yet complete. He is scheduled for reassignment to USASAFS, Augsburg on approximately 15 December 1975. In accordance with paragraph 3b of reference a, a Lead Development Report is being prepared and will be forwarded separately, recommending his possible utilization as a defensive installation source in Augsburg.

b. The lack of identification of any personnel who will make up the permanent party at the target has inhibited any meaningful spotting/assessing activity to date.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

5 360

~~CONFIDENTIAL~~

AEUMI-N-CE 24 October 1975
SUBJECT: Internal Counterintelligenee Program (ICIP)

6. (U) Comments:

a. The PLO was indoctrinated for SI on 9 October 1975. Request Special Operations Detachment determine if any more Quarterly Security Inspections are scheduled for target, and arrange for prior notification and coordination so that the PLO may accompany the inspecting team. Any insight gained into security problem areas not evident from routine liaison contacts would be of great value to the PLO in accomplishment of his mission.

b. The PLO has reported that he is unable to pursue a more aggressive approach with the target commander concerning identities of personnel who will remain at the target, without arousing suspicion as to his true motives. Request Special Operations Detachment attempt to identify those individuals as soon as the determination is made.

c. The short period remaining of continued operations at the target raises the question as to whether the project would be justified at that location in the long term. As presently visualized, according to available information, any source recruited at the target would be primarily reporting on six or seven other personnel, with whom he is living in a very close, restrictive environment. It can be expected the majority of the information reported will be of an adverse suitability nature. Further, it can be expected that with target automation, Hostile Intelligence efforts at the target will take a lower priority inasmuch as product expolitation through the human exploitable factor will no longer be present. The Commander, USASAFS, Augsburg raised some of these points when reference a was staffed through his office.

1 Incl
as

Tel: Nbg Mil (2621)-6446/Fost

FADLO M. HAGSABNI
LTC, MI
Commanding

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

6 361

~~CONFIDENTIAL~~

[illegible]

[illegible]

[illegible]

REGRADED UNCLASSIFIED
SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH: DoD 5200.1-R

ACTION SHEET [redacted] CONFIDENTIAL

SUBJECT	OFFICE SYMBOL	SUSPENSE
Internal Counterintelligence Program (ICIP) (U)	DAMI-DOH	
	DATE: 18 November 1975	

ACTION REQUIRED

To advise USAREUR of the Quarterly Report requirement for ICIP.

MEMORANDUM FOR RECORD. (Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without resource to other sources.)

1. (U) (C) BACKGROUND:

a. (U) (C) In an exchange of SSO messages between USAREUR and USAINTA, HBG 2802, 191755Z Jun 75 and DNT 1092, 0111540Z Jul 75 (TAB B), ODCSI, USAREUR requested assistance in coordinating with CDR, USASA a draft OPLAN of an ICIP in support of USASA Field Station, Augsburg, FRG. The CDR, USASA approved the proposed Operations Plan.

b. (U) (C) A Memorandum for Record prepared by former ICIP action officer, dated 27 Sep 75 (TAB C), outlines the ACSI's stated policy regarding his validation of all future operation plans for the ICIP.

c. (U) At TAB D is a Memorandum to the Vice Chief of Staff from the Under Secretary of the Army which outlines the requirement for quarterly reports on the ICIP.

2. (U) (C) DISCUSSION:

a. (U) (C) The USAREUR proposed ICIP in support of the USASA Field Station in Augsburg marks the first extension of the program overseas. There is no indication that the ACSI has validated the OPLAN for the project.

b. (U) This action advises USAREUR by message of the ACSI's policy on the ICIP and requests the OPLAN be forwarded for ACSI review. The message further advises of the quarterly report requirement to the Under Secretary.

3. (U) RECOMMENDATION: That the Acting Director of Operations sign the message to CINCUSAREUR at TAB A.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		
			DIR		
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER (Name, grade, phone and signature)
LTC Haendle/56159 H.V. Haendle

CONFIDENTIAL 363

ACSI FORM 28, 13 Sep 71

[redacted]

REGRADED CONFIDENTIAL WHEN SEPARATED FROM CLASSIFIED DOCUMENT

Page 1862 of 3957

01 03 RR RR ~~8333~~

NO

DA WASHDC//DAMI-DOH//

CINCUSAREUR HEIDELBERG GERMANY//AEAGB-CI//

INFO: CDR USAINTA FT MEADE MD//MIIA-SO//

~~SECRET NOFORN~~

SUBJ: INTERNAL COUNTERINTELLIGENCE PROGRAM (ICIP) (U)

A. USAREUR MSG 1917552 JUN 75 (SSO MESSAGE)

B. USAINTA MSG 011540Z JUL 75 (SSO MESSAGE)

C. DISCUSSION MG DILLARD/MR KELLY, 21 NOV 75

1. (U) ~~SEC~~ REFS A AND B PERTAIN TO AN ICIP FOR THE USASA FIELD STATION, AUGSBURG, FRG WHICH INDICATED CDR USASA HAD APPROVED AN OPLAN PREPARED BY 66 MI GP. DURING REF C MR KELLY BRIEFED MG DILLARD ON BACKGROUND AND SPECIAL CONTROLS PERTINENT TO ICIP.

2. (U) ~~SEC~~ IN LIGHT OF YOUR POSSIBLE ENTRY INTO THE ICIP FIELD, THE FOLLOWING INFORMATION IS FURNISHED AS BACKGROUND: (U)

A. (U) THE PRESENT ICIP (FORMERLY KNOWN AS ACIP) IS A CI SERVICE TO VARIOUS SENSITIVE INSTALLATIONS IN CONUS UNDER USAINTA'S MONITORSHIP AND CONDUCTED BY THE TWO CONUS MI GROUPS. SINCE THE PROGRAM HAS BEEN PRIMARILY A CI SERVICE CONDUCTED BY USAINTA, THERE IS NO DETAILED ARMY-WIDE GUIDANCE ON ICIP. THE NEWLY PUBLISHED

LTC HAENDLE/DAMI-DOH/56159/2 DEC 75

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

364

02 02 RR RR

NO

AR 381-20 MENTIONS ICIP AS A CI SERVICE BUT DOES NOT CONTAIN POLICY OR PROCEDURAL SPECIFICS.

(U) BY MEMORANDUM TO THE VICE CHIEF OF STAFF, ARMY, DATED 8 FEB 72, THE UNDER SECRETARY OF THE ARMY DIRECTED THAT QUARTERLY REPORTS ON THE ICIP BE FURNISHED HIS OFFICE BASED UPON HIS CONCERN AT THE TIME FOR COMPLIANCE WITH THE VARIOUS DOD AND DA DIRECTIVES PERTAINING TO THE PROTECTION OF NON-AFFILIATED US CITIZENS AND ORGANIZATIONS. THESE QUARTERLY REPORTS HAVE BEEN REGULARLY FURNISHED SINCE MARCH 1972.

(U) IN SEPTEMBER 1974, THE ACSI ESTABLISHED POLICY FOR USAINTA THAT ICIPS WOULD BE CONDUCTED ONLY AT THE MOST SENSITIVE INSTALLATIONS OR ACTIVITIES. HE PERSONALLY REVIEWED THE EXISTING PROJECTS AND DIRECTED THAT THEIR NUMBER BE REDUCED FROM 19 TO 8, LATER REINSTATING ONE ON AN INTERIM BASIS. HE ALSO ASSURED THE UNDER SECRETARY OF THE ARMY THAT HE WOULD PERSONALLY APPROVE ALL NEW USAINTA ICIP PROJECTS.

3. (U) THE PROPOSED ICIP IN SUPPORT OF THE USASA FIELD STATION IN FRG WOULD EXTEND THE PROGRAM OUTSIDE CONUS FOR THE FIRST TIME. IN VIEW OF THE ACSI'S COMMITMENT TO THE UNDER SECRETARY, ARMY-WIDE

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1864 of 3957

03 03 RR RR ~~SECRET~~

NO

PROCEDURES NEED BE ESTABLISHED WHEREBY PROPOSED ICIPS ARE REVIEWED AND APPROVED BY THE ACSI AND QUARTERLY REPORTS OF ON-GOING ICIPS ARE FURNISHED THE UNDER SECRETARY.

4. (U) IF YOU STILL WISH TO PROCEED WITH THE ICIP IN SUPPORT OF THE USASA FIELD STATION, IT IS REQUESTED THAT A COPY OF THE FINALIZED OPLAN BE FORWARDED FOR ACSI REVIEW, ATTN: DAMI-DOH. AFTER ACSI APPROVAL, INSTRUCTIONS AND FORMAT FOR THE QUARTERLY REPORT WILL BE FURNISHED ALONG WITH SAMPLES OF PREVIOUS REPORTING. XGDS-2005

XGDS-(02)(05)

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

11 June 75

DAMI-P
DAMI-DOI
DAMI-DOI-S
DAMI-DOI-P
DAMI-DOS
DAMI-DOS-F
DAMI-DOS-P
DAMI-DOA-Z
OTHERS
SANITIZED COPY FURNISHED TO:

/COPY FURNISHED: maj Eberle
DATE: 20 JUN 1975

F 191755Z JUN 75
FM SSO HEIDELBERG GERMANY
TO SSO INTEL AGENCY FT MEADE MD
INFO SSO ACSI LA WASH DC

~~CONFIDENTIAL LIMDIS~~ REG 280Z TOPIC

FROM COL IALEROSA, CHIEF, CI DIV, ODCSI, USAREUR FOR LTC GRIMES, CDR, SO DET, USAINTA; INFO MR KELLY, DEP DIR OPS, OACSI, LA.

SUBJECT: INTERNAL COUNTERINTELLIGENCE PROGRAM (ICIP) (U)

A. INT 1126-74 TOPIC, 182138Z SEP 74 (U).

1. (U) IN ACCORDANCE WITH GUIDANCE IN A, 66TH MI GP PREPARED ICIP OPERATIONS PLAN (OPLAN) TARGETTING AN ELEMENT OF THE USASA FIELD STATION, AUGSBURG, FRG (USASAFSA). ON 26 MAY 75, FINALIZED OPLAN WAS PROVIDED S-2, USASAFSA, FOR COORDINATION AND COMMENT THEN TO BE RETURNED TO 66TH MI GP FOR FORWARDING THRU ODCSI USAREUR TO USAINTA FOR FURTHER COORDINATION WITH USASA. CONTRARY TO SPECIFIC REQUEST BY 66TH MI GP, COMMANDER, USASAFSA, FORWARDED OPLAN DIRECT TO DEPUTY CHIEF OF STAFF SECURITY, HEADQUARTERS, USASA, ARLINGTON HALL STATION FOR COORDINATION AND GUIDANCE.

2. (C) IN VIEW OF FACT USAINTA INTENDED TO REVIEW AND EFFECT CO-ORDINATION OF OPLAN, RECOMMEND APPROPRIATE OFFICE AT USASA BE CONTACTED IN EFFORT TO OBTAIN COPY OF OPLAN AND EFFECT COORDINATION.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

367

619

3. (U) USAREUR ACTION OFFICER IS MR BENJAMIN J. ROSETO, (SECURE PHONE 6742) HEIDELBERG MILITARY 2121-7354.

XGDS-2

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1867 of 3957

COPY FURNISHED: Dist Eberole
DATE: 2 JUL 1975

DAMI-DOI
DAMI-DOI-S
DAMI-DOI
DAMI-DOS
DAMI-DOS-F
DAMI-DOS-P
DAMI-DOA-Z
OTHERS
SANITIZED COPY FURNISRED TO:

P [illegible] JUL 75
FM SSO INTEL AGY
TO SSO HEIDELBG GERMANY
INFO SSO ACSI DA

~~CONFIDENTIAL LIMDIS~~

~~C O N F I D E N T I A L LIMDIS INT ICS TOPIC~~

FM LTC GRIMES CDR SP OP DET USAINTA
FOR COL IALEROSA CH CI LIV OACSI USAREUR
INFO MR KELLY REP DIR OPS OACSI DA
SUBJECT: INTERNAL COUNTERINTELLIGENCE PROGRAM (ICIP) (U)
A. HSC [illegible] TOPIC 19-1952 JUN 75

(DOS) UPON RECEIPT OF REF MSG COPY OF ICIP OPLAN OBTAINED FROM HQ USASA AND ARRANGEMENTS MADE FOR ADDITIONAL COORD. 25 JUN 75 ASA WAS ADVISED THAT USAINTA HAD NO MAJOR OBJECTION TO OPLAN AND WAS PREPARED TO EFFECT COORDINATION AS REQUESTED BY OACSI USAREUR. 30 JUN 75 HQ ASA REP INFORMED USAINTA THAT GEN GOLDARE HAD APPROVED THE OPLAN AND CONCEPT AS OUTLINED AND HAD APPROVED CORRESPONDENCE WHICH NOTIFIES THE ASA FIELD ETA OF THIS ACTION. THE HQ ASA REP WAS INFORMED THAT OACSI USAREUR WOULD BE ADVISED IMMEDIATELY VIA MSG OF THE FAVORABLE COORD RECEIVED FROM HQ ASA.

(DOS) FOLLOWING OBSERVATIONS ARE BASED ON REVIEW OF OPLAN AND EXPERIENCE GAINED BY THIS HQ CONDUCTING ICIP:

A. (U) THE OPLAN IS THOROUGH AND WELL WRITTEN, AND IF DET

369

~~CONFIDENTIAL LIMDIS~~

REGRADED UNCLASSIFIED ON SEP 15 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~ ~~LIMDIS~~

CONTINUES AS AN ASA SUBORDINATE UNIT OF SUFFICIENT SIZE, IMPLEMENTATION OF OPLAN SHOULD BE PRODUCTIVE.

B. DUR AMC IG INSPECTION THIS HQ WAS QUERIED RE OVERALL AUTHORITY FOR CONDUCTING ICIP. USAINTA WAS INFORMED THAT AR 381-100, CI INVES, SUPERVISION AND CONTROL (CHAP III) IS AT OACSI FOR APPROVAL AND IMPLEMENTATION, AND THIS AR WILL PROVIDE NECESSARY AUTHORIZATION FOR ICIP.

C. INCLUDING AS REF, AR 380-13, ACQUISITION AND STORAGE OF INFO CONCERNING NON-AFFILIATED PERSONS AND ORGANIZATIONS SHOULD BE CONSIDERED.

D. ANY INFO DEVELOPED THAT BECOMES OFCO OR APPEARS TO HAVE OFCO EXPLOITABLE POTENTIAL SHOULD BE REPORTED THRU OFCO CHANNELS.

3. (U) THIS HQ IS PREPARED TO RENDER ADDITIONAL ASSISTANCE AS REQUIRED. REQUEST THIS HQ BE KEPT INFORMED RE DEVELOPMENTS THIS ICIP. XGDS-2(X5)

~~CONFIDENTIAL~~ ~~LIMDIS~~

REGRADED UNCLASSIFIED
ON SEP 26 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

370

~~SECRET~~

DAMI-DOI-C 27 September 1974

MEMORANDUM FOR THE RECORD

SUBJECT: ICIP Briefing for Under Secretary of the Army (U)

1. (U) On 25 September 1974 MG Aaron briefed Mr. Herman Staudt, on the ICIP. Mr. Staudt expressed reservations about operational control within the program and concern about the sudden rapid growth. He wanted assurances that the program was carefully monitored precluding the possibility for embarrassment.

2. (U) General Aaron assigned the following tasks to USAINTA through Mr. Leslie Hime, the USAINTA representative at the meeting.

a. Prepare all the operations plans for review; General Aaron will personally re-validate each plan.

b. Prepare source dossiers for review. General Aaron wants to be able to personally be assured that all sources are of such maturity and stability that they would not cause any embarrassment to the Army.

3. (U) General Aaron will personally validate and approve all future operations plans and will assume command and control of the program. Only essential plans will be approved and permitted to continue. General Aaron did not consider the operation at the War College to be essential.

4. (U) Operations plans and dossiers will be reviewed on 4 October 1974.

Richard Ebersole

RICHARD EBERSOLE
Major, GS

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Regraded SECRET When Separated From Classified Inclosures.

371

~~SECRET~~

TAB C

~~SECRET~~

OSA,OGC/RGreene/pf/13Jan72

8 FEB 1972

MEMORANDUM FOR THE VICE CHIEF OF STAFF
United States Army

SUBJECT: Aggressive Counterintelligence Program (ACIP) Operations

On 4 December 1971 you forwarded to me a memorandum from the Assistant Chief of Staff for Intelligence, SUBJECT: Counterintelligence Policy Guidance, which informed me of the ACSI's decision to reactivate certain Aggressive Counterintelligence Program (ACIP) Operations. Attached to the memorandum was the operation plan for one such operation. I have reviewed that memorandum and the attached plan, and although I appreciate the conscientious steps which have been taken to assure adherence to current policies in this area, I remain concerned that this program may be placing us in a highly vulnerable position.

DoD Directive 5200.27 and the implementing Army policy letter dated 1 June 1971 impose two restrictions which are particularly relevant to ACIP operations. First, they require that there be "no covert or otherwise deceptive surveillance or penetration of civilian organizations" without the prior approval of the Chairman, DIEC (now the Assistant Secretary of Defense (Comptroller)). Second, they prohibit assigning DoD personnel "to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information the collection of which is authorized" without my prior approval, except in emergency situations. These prohibitions apply whether or not the formal "target" of the operation is affiliated with the Department of Defense. Although the ACSI letter approving the first reactivated ACIP operation incorporates these restrictions by reference (paragraph 3a), the operation plan and related documents obviously assume that confidential sources working in the operation may obtain and report information which they receive in the course of activities off military installations. While the plan prohibits extending the collection effort "directly" to non-DoD personnel (paragraph 4a(a)), and while the ACSI approval letter prohibits making non-DoD personnel "targets" of off-post surveillance, I would assume that it is entirely possible that in the course of their off-post activities confidential sources might obtain and report information

OSA,OGC - ~~ort~~
OSA,ASG
USA - ~~ort~~
Mr. Greene

~~SECRET~~

372

2770B

OSA, ASS Control No. 2770F

TAB D

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH: ARA 1-603 DoD 5200.1-R

on non-affiliated civilians. Although such activity might not in all situations be forbidden by DoD Directive 5200.27, it is clearly on the borderline, and I therefore feel it is very important that these operations be closely supervised and tightly controlled.

In order to make an informed decision about whether further controls are necessary (including possible Under Secretary or DIRC review of each operation), I would appreciate your taking the following steps:

1. Beginning March 31, 1972, I would like to receive a quarterly report containing the following information on each ACIP operation in progress at any time during the reporting period. Date approved, code-name, location, number of confidential sources used during reporting period, number of instances in which information on non-affiliated civilians is obtained off-post and reported, and a brief narrative statement explaining whether useful information was obtained during the reporting period, whether the operation is to be continued, and if so, why. These reports may be submitted 30 days after the close of the calendar quarter which they cover.

2. With the second quarterly report, which will be due July 31, 1972, I would like to receive a full analysis of this program, including its value in terms of producing useful information and the adequacy of the controls which have been imposed. Recommendations for any further necessary controls should be included.

(sgd) Kenneth E. BeLieu

Kenneth E. BeLieu
Under Secretary of the Army

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

ATTACHED TO TRANSMITTAL
OFFICE
FEB 8 10 07 AM '72
ATTACHED
ADMINISTRATIVE
DISPATCHED

373

2

SECRET

~~CONFIDENTIAL~~
~~CONFIDENTIAL~~

THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20301

THE JOINT STAFF

DASM-666-75
2 December 1975

MEMORANDUM FOR THE COMMANDER, US ARMY INTELLIGENCE AGENCY,
FORT GEORGE G. MEADE, MARYLAND 20755

Subject: ICIP Coverage

1. Reference is made to J3M-1994-74, dated 26 November 1974, subject: Request for Internal Counterintelligence Program (ICIP) Coverage (C).

2. Subject program authorized by the reference is hereby rescinded.

PETER O'BRIEN
Colonel, USA
Director,
Administrative Services

REGRADED UNCLASSIFIED
ON SEP 5 1985
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by Chief, ANMCC
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY - Indefinite

374

~~CONFIDENTIAL~~
~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ROUTING AND TRANSMITTAL SLIP

TO	ACTION
Mr. Kelly Acting Director of Operations	CIRCULATE
	COORDINATION
	FILE
	INFORMATION
	NOTE AND RETURN
	PER CONVERSATION
Re: ICIP CANARY EFFORT (U)	SEE ME
	SIGNATURE

C/DOH

Tell USAINTA to include ... update ... for FY 1978 ... JCS

REMARKS

1. (U) The JCS support portion of the ICIP at Ft. Ritchie, MD has been cancelled in response to a letter from the Director, Admin Services Div, JCS, dated 2 Dec 75, which rescinded the earlier request for support. However, the ICIP continues to support Army elements at Ft. Ritchie.

2. (U) The current Commander, 902d MI Gp is reviewing all current ICIPs managed by his group and anticipates furnishing recommendations in March regarding continuation of each project. CANARY EFFORT (U) will be included in his review.

Classified by C/H HUMINT Div
SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS
NOT AUTOMATICALLY DECLASSIFIED

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM	DATE
375 L. A. SPIRITO COL, GS, Chief, HUMINT Division	2 Feb 76 PHONE 74087

OPTIONAL FORM 41 (Rev. 7-76) ... 5041-101
AUGUST 1967
GSA FPMR (41CFR) 100-11.206

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

ROUTING AND TRANSMITTAL SLIP

TO: Cal. Spirito DDE	INITIALS / DATE	ACTION: CIRCULATE / COORDINATION
Ch HAENDEL	INITIALS / DATE	FILE / INFORMATION
Pls follow up & provide info.	INITIALS / DATE	NOTE AND RETURN / PER CONVERSATION
	INITIALS / DATE	SEE ME / SIGNATURE

REMARKS

Lou: Please check up on this (Canary Expert) Any developements? Any action needed on our part? Phone call answer OK

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM: MERRILL T. KELLY, Acting Director of Intelligence Operations — 3716

DATE: 31 Jan

PHONE:

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41 CFR) 100-11.206

GPO: 1973 O-525-336 5041-101

ROUTING AND TRANSMITTAL SLIP		ACTION
TO Mr Kelly	INITIALS DATE 24 Nov	CIRCULATE COORDINATION
2 MG Aaron ACSI	INITIALS DATE	FILE INFORMATION
3 Mr Kelly DO	INITIALS DATE	NOTE AND RETURN PER CONVERSATION
4	INITIALS DATE	SEE ME SIGNATURE

REMARKS

1. Re: MG Aaron's question attached Ops 41, the individual who met with the JCS Security Officer was CWO Garry Peisen, FI. Ritchie RO, 902d MI Gp, and not a representative of PCF as previously reported. A PCF representative escorted Peisen to the JCS Security Office but did not participate in the discussions.

2. Mr. Guerrieri has still not determined if any sort of briefing will be required and will advise this office when a decision is reached.

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM	DATE
L. A. SPIRITO, COL, GS Chief HUMINT Division 377	25 Nov 75 PHONE 74087

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41CFR) 100-11.206

GPO: 1973 O-529-336 5041-101

[redacted]

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

DAMI-DOH

21 Nov 75

MEMORANDUM FOR: MR. KELLY, ACTING DIRECTOR OF INTELLIGENCE OPERATIONS

24 Nov

SUBJECT: Discussions with JCS Security Officer on ICIP CANARY EFFORT

1. (U) (C) At the request of LTG Grimes, Special Operations Detachment, USAINTA, LTC Haendle from this office visited Mr. Guerrieri, Chief, Security Office, JCS on 20 Nov 75 to determine if he had requested briefings for the Director of the Joint Staff and the J3, JCS. LTC Grimes had learned that the 902d MI Group was preparing to brief on the ICIP CANARY EFFORT at Fort Ritchie, MD and questioned the need for such briefings.

2. (U) (C) Mr. Guerrieri stated that he had learned in passing conversation with a member of the PCF that Army was providing ICIP support to Joint Activities at Fort Ritchie, MD. He was disturbed about the potential embarrassment of such activities and stated he had not previously been aware of this type of support. He had requested that various JCS offices be briefed. He read from a letter prepared by the Commander, Alternate National Military Command Center (ANMCC) to the Commander, USAINTA, dated November 1974 which had requested ICIP support and indicated this request had not been cleared with either his predecessor or the J3, JCS. (This request was never forwarded to OACSI so far as can be determined).

3. (U) (C) It was explained that an existing ICIP CANARY EFFORT in support of Army organizations at Fort Ritchie, MD had recently (Sep 75) been revalidated by the ACSI resulting from a reorganization of the supported command. Included in the revised OPLAN was overlapping support to the ANMCC and its Support Directorate. However, the ICIP, which has been in existence for several years, was primarily in support of Army activities.

4. (U) (C) Mr. Guerrieri indicated he would prefer that no such operation existed in support of JCS activities at Fort Ritchie and would so recommend this to his supervisor, COL O'Brien, Director of Admin Services, JCS. It

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

378

Classified by Dir et Int ltr dtd
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 21 Dec 85

DAMI-DOH
SUBJECT: Discussions with JCS Security Officer on ICIP CANARY EFFORT

was agreed that a USAINTA representative would brief Mr. Guerrieri and COL O'Brien at their convenience on ICIP CANARY EFFORT. Further that no higher representatives need be briefed unless it was determined to be necessary after the initial briefing. Mr. Guerrieri would inform DAMI-DOH when (or if) a briefing on the ICIP was required.

L. A. SPIRITO
Colonel, GS
Chief, HUMINT Division

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

379

[redacted] 1 NOV 75

DAMI-DOH

MEMORANDUM FOR: MR. KELLY, ACTING DIRECTOR OF INTELLIGENCE OPERATIONS

SUBJECT: Discussions with JCS Security Officer on ICIP CANARY EFFORT

1. (U) At the request of LTC Grimes, Special Operations Detachment, USAINTA, LTC Haendle from this office visited Mr. Guerrieri, Chief, Security Office, JCS on 20 Nov 75 to determine if he had requested briefings for the Director of the Joint Staff and the J3, JCS. LTC Grimes had learned that the 902d MI Group was preparing to brief on the ICIP CANARY EFFORT at Fort Ritchie, MD and questioned the need for such briefings.

2. (U) Mr. Guerrieri stated that he had learned in passing conversation with a member of the PCF that Army was providing ICIP support to Joint Activities at Fort Ritchie, MD. He was disturbed about the potential embarrassment of such activities and stated he had not previously been aware of this type of support. He had requested that various JCS offices be briefed. He read from a letter prepared by the Commander, Alternate National Military Command Center (ANMCC) to the Commander, USAINTA, dated November 1974 which had requested ICIP support and indicated this request had not been cleared with either his predecessor or the J3, JCS. (This request was never forwarded to OACSI so far as can be determined).

3. (U) It was explained that an existing ICIP CANARY EFFORT in support of Army organizations at Fort Ritchie, MD had recently (Sep 75) been revalidated by the ACSI resulting from a reorganization of the supported command. Included in the revised OPLAN was overlapping support to the ANMCC and its Support Directorate. However, the ICIP, which has been in existence for several years, was primarily in support of Army activities.

4. (U) Mr. Guerrieri indicated he would prefer that no such operation existed in support of JCS activities at Fort Ritchie and would so recommend this to his supervisor, COL O'Brien, Director of Admin Services, JCS. It

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Dir at Datel ops

380 31 Dec 75

[redacted]

DAMI-DOH
SUBJECT: Discussions with JCS Security Officer on ICIP CANARY EFFORT

was agreed that a USAINTA representative would brief Mr. Guerrieri and COL O'Brien at their convenience on ICIP CANARY EFFORT. Further that no higher representatives need be briefed unless it was determined to be necessary after the initial briefing. Mr. Guerrieri would inform DAMI-DOH when (or if) a briefing on the ICIP was required.

/Signed/ MVR
L. A. SPIRITO
Colonel, GS
Chief, HUMINT Division

NOTE:

AT 0845 HRS, 4 DEC 75, COL SPIRITO ADVISED COL STUBBLEBINE, CDR 902D MI GP, THAT HE SAW NO OBJECTION TO COL STUBBLEBINE DEALING DIRECT WITH THE SECURITY OFFICER, JCS TO DISCUSS ICIP SUPPORT

KFH

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

DAMI-DOH

21 Nov 1975

MEMORANDUM FOR RECORD

SUBJECT: ICIP CANARY EFFORT

1. (U) On 19 Nov 75, LTC Grimes USAINTA requested that I visit a Mr. Guerrieri, Chief, JCS Security Office, 1A688, The Pentagon to determine if Guerrieri had requested briefings on CANARY EFFORT for the Director of the JCS and J3. LTC Grimes indicated he had just learned the 902d MI Gp was ginning up for these briefings which he considered unnecessary. LTC Grimes advised the 902d MI Gp to hold up until informed otherwise.

2. (U) Mr. Guerrieri was not in his office on 19 Nov 75 and was not visited until 1430 hours, 20 Nov 75. In the meantime, the undersigned determined that a request for an ICIP had been initiated by the Commander, Alternate National Military Command Center (ANMCC) to the Commander, USAINTA in November 1974. Correspondence between USAINTA and the 902d MI Gp established that the existing ICIP CANARY EFFORT could be expanded to provide coverage to the ANMCC. (None of this correspondence was discussed at OACSI level so far as could be determined). In the meantime the 902d determined that the OPLAN for CANARY EFFORT required revision due to a reorganization of the Supported Army Command. It was decided to add target coverage to the ANMCC as well as the AJCC, ANMCCSD, and ECTC, all at either Ft Ritchie (Site R) or Ft Detrick. The revised OPLAN was approved by the ACSI on 15 Sep 75.

3. (U) In conversation with Mr. Guerrieri, it was determined that he learned of the ICIP in passing during a conversation with a representative of the PCF. He was more than a little disturbed that no one in JCS, particularly the Security Office, was aware of the project. He reiterated at great length that he recognized the Army was merely responding to a legitimate request, prepared on JCS stationary, but that the potential for embarrassment from such an operation clearly disturbed him. The undersigned discussed briefly the fact that the Army ICIP in support of Army activities at Ft Ritchie had existed for many years. Even though the ANMCC request for support occurred in 1974, the expansion of the Army Security service to include joint activities was not approved by the ACSI until Sep 75.

382

Classified by Dir of Intel Ops
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 05

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

DAMI-DOH
SUBJECT: ICIP CANARY EFFORT

Further, from correspondence received at OACSI, the indications were that the ICIP still supported Army commands in the main, but could be of assistance to the ANMCC if serious breeches of security were uncovered which affected joint activities in adjoining areas. Mr. Guerrieri reiterated his concern for the Privacy Act impact upon such security operations and generally gave the impression he was concerned that the ICIP would cause his office headaches in the future. He would prefer that no such operation supported JCS activities and would so recommend this to his boss, COL O'Brien, USA, Director of Admin Services, JCS.

4. (U) It was agreed that a USAINTA representative would brief Mr. Guerrieri and COL O'Brien at such time as he preferred. No higher or other JCS representatives would be briefed unless it was decided to be necessary after the initial briefing. Mr. Guerrieri will contact DAMI-DOH to arrange for a briefing.

K. V. Haendle
KARL V. HAENDLE
LTC, GS
DAMI-DOH

Cy furnished LTC Grimes, 7th Inf Div - Ft Ord

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

383

~~CONFIDENTIAL~~

Page 1882 of 3957

R TING AND TRANSMITTAL SLIP		ACTION
TO	INITIALS	CIRCULATE
MFR	DATE	COORDINATION
2	INITIALS	FILE
	DATE	INFORMATION
3	INITIALS	NOTE AND RETURN
	DATE	PER CONVERSATION
4	INITIALS	SEE ME
	DATE	SIGNATURE

REMARKS Telephone conversation w/ Mr Heiss, MIIA-50

HDC corporate HQs has moved from Connecticut Ave, Nash, DC to 2800 Powder Mill Rd, Adelphi, Md in the past 6 months but still retains an office in the former location. The Woodbridge Research Facility, HDC, is on Dawson Beach Rd, Woodbridge, Va. The ICIP CENTRIC RID covers all locations to some degree.

The Memo to the undersecretary should have identified the Woodbridge Research Facility and not just HDC in paragraph 1.

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM	DATE
Kit Hendle, ITC 384	18 Dec 75
	PHONE

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41 CFR) 100-11.206

GPO: 1973 O-526-336 5041-101

ROUTING AND TRANSMITTAL SLIP		ACTION
TO	INITIALS	CIRCULATE
Col Jones III	DATE	COORDINATION
MW K. Hyatt 17 Dec	INITIALS	FILE
LTC Harrell	DATE	INFORMATION
	INITIALS	NOTE AND RETURN
Col Spurgeon	DATE	PER CONVERSATION
	INITIALS	SEE ME
	DATE	SIGNATURE

REMARKS

Returned for USA & CSA

Henry Diamond Labs

at Adelphia, Md

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM		DATE
SFC Lucas	385	15 Dec 75
		PHONE

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41CFR) 100-11.206

GPO : 1973 OF - 525-336 5041-101

ROU JG AND TRANSMITTAL SLIP		ACTION
TO: Maj Gen Aaron, ACSI	INITIALS: HWM	CIRCULATE: —
	DATE	COORDINATION
Mr. Kelly, DO	INITIALS	FILE
	DATE	INFORMATION
	INITIALS	NOTE AND RETURN
	DATE	PER CONVERSATION
	INITIALS	SEE ME
	DATE	SIGNATURE: 7

REMARKS

Gen. Aaron: Regular quarterly ICIB report for Under Secretary. I note a tendency to include too much low level character deficiency info in these. Pls request USAINTA to refine them in future submissions.

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM: MERRILL KELLY, Acting Director of Intelligence Operations — Bruce Kelly 3866 — DATE: 20 Dec — PHONE:

OPTIONAL FORM 41 (AUGUST 1967) GSA FPMR (41CFR) 100-11.206 — GPO: 1973 O-525-336 — 5041-101

10104-75

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PA
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

AC... SHEET

CONTROL NUMBER

OFFICE SYMBOL: DAMI-DOH | SUSPENSE:

DATE: 17 Nov 75

Internal Counterintelligence Program (ICIP) (U)

ACTION REQUIRED

To obtain approval of the quarterly ICIP report

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) Background: By memorandum dated 8 February 1972 (TAB B), the Under Secretary of the Army requested that the VCSA provide a quarterly report on all ICIP operations.

2. (U) Discussion:

a. (U) During the past quarter, the ICIP OPLAN at Fort Ritchie, MD was revised to reflect target area realignment resulting from the reorganization of the US Army Communications Command. The ACSI approved the revised OPLAN on 15 Sep 75.

b. (U) The Commander, USASA approved an Operation Plan in July 1975 for an ICIP under the purview of DCSI, USAREUR and 66th MI Group at the Augsburg Field Station, USASA, FRG. A separate staff action directs a message from the Acting Director of Operations, OACSI to DCSI, USAREUR to furnish the Operations Plan for this ICIP for ACSI validation. Information regarding this new ICIP is not included in the attached quarterly report.

3. (U) Recommendation: That the memorandum at TAB A be approved and signed.

DOH
Not used - separate tab
because of revision
of communication to
USAREUR - Quarterly
report sent to ACSI
under

ACSI DA

CLASSIFY AS: 2

DECLASSIFY ON: 31 Dec 05

(continue on plain bond)

REPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		19 Nov 75
			DIR		
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

389

ACTION OFFICER *(Name, grade, phone and signature)*

LTC Haendle/56159 J. V. Haendle

CONFIDENTIAL

ACSI FORM 28, 13 Sep 71

[redacted]

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

0 4 DEC 1975

DAMI-DOH

MEMORANDUM THRU: ~~VICE CHIEF OF STAFF, UNITED STATES ARMY~~

FOR: ~~UNDER SECRETARY OF THE ARMY~~ Noted by USA 8 DEC 1975

SUBJECT: Internal Counterintelligence Program (ICIP) (U)
INFORMATION MEMORANDUM

1. (C) During the past quarter, five of the ongoing operations provided information which served to enhance the security at the facilities concerned. Personnel participating in ICIP operations at Harry Diamond Laboratories, Virginia, and Fort Ritchie, Maryland, identified security hazards which required follow-up investigative action.

2. (C) With the revalidation of the ICIP at Aberdeen Proving Ground, Maryland in July 1975 for a period of six months, the total number of active ICIPs in CONUS was raised to nine. The ICIP OPLAN at Fort Ritchie, Maryland was revised on 15 September 1975 to reflect target area realignment resulting from the reorganization of the US Army Communications Command.

3. (U) Summaries of the nine on-going CONUS ICIP operations are inclosed.

9 Incl
as

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

8 DEC 1975

NOTED - OCSA

WILLIAM G. HANDLE
Major, GS
Assistant to the Director
of the Army Staff

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOUPO
AUTH PARA 1-603 DoD 5200.1-R

ACSI DA
EXECUTIVE ORDER 11652
31 Dec 05

388

~~CONFIDENTIAL~~

LTC Haendle/56159
Typed by T. Shamblen

~~CONFIDENTIAL~~

1. (U) CANARY EFFORT: (OACSI Revalidation - 4 Feb 75)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three confidential sources

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) At an undetermined time within the past year, the Pentagon Telecommunications Center (PTC) requested that the Joint Chiefs of Staff (JCS) Communications Center provide the PTC with a magnetic tape containing test messages recorded by the Burroughs D825 Automated Message Processing System, a system used by the JCS, in order for the PTC to devise a coding system which would provide compatibility between the PTC's IBM 360/50 System and the Burroughs System used by the JCS. The JCS Communications Center could not provide the test message tape because of technical factors. This led to the Telecommunications Directorate, Site R, Ft Ritchie, receiving the tasking for the test tape preparation. A number of innocuous, unclassified messages were prepared by the communications personnel at Site R on a 2,500 foot reel of magnetic tape, which was sent to the PTC, where, because the messages were unclassified, it lay in open storage, unsecured, for about six weeks. During the processing which followed to make the two systems compatible, it was discovered that the tape also contained fragments of highly sensitive, classified messages which had been picked up from residual magnetism on the drums or reels of the Burroughs equipment when the test messages were recorded. A source of this ICIP reported this information believing that a compromise could have occurred when the test tape was not secured. The information was reported to the Commander, US Army Communications Center Operations Command, who initiated an investigation of the incident which resulted in a change of security procedures for the handling/storage of computer tapes, reels, and discs. Since the PTC is a secure area in itself, it is believed that the information in question had not been compromised.

(2) During the reporting period, sources surfaced adverse suitability information on 47 individuals assigned to Fort Ritchie and the Alternate Joint Communications Center (AJCC), Site R. In the majority of instances, the adverse suitability information dealt with drug abuse. Information was brought to the attention of the ICIP Coordinator of the supported command. Individuals concerned are being monitored, and an investigation was requested on one individual.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

CONFIDENTIAL

e. Operational Status:

(1) The revised CANARY EFFORT Operations Plan which reflected target realignment resulting from reorganization of the USACC into the 7th Signal Command was approved by the ACSI on 15 September 1975. A request has been submitted for assignment of an additional Great Skills PCO to provide more adequate coverage of the increased target areas which have resulted from this reorganization.

(2) On 1 July 1975, CPT Richard E. Graff, Project Liaison Officer (PLO), CENSUS TIME, was introduced to COL Donald E. Clark, Commander, USACC Operations Command, at the AJCC, Site R. COL Clark had been previously briefed on the ICIP on 18 March 1975, but the purpose of this meeting was to acquaint COL Clark with the ICIP CENSUS TIME which is conducted at the Pentagon Telecommunications Center (PTC), prior to his assumption of command at the PTC. On 1 August 1975, the CENSUS TIME and CANARY EFFORT Project Liaison Officers briefed COL Clark at the USACC PTC on both of these ICIPs since both of them involve USACC Operations Command and its subordinate elements.

(3) On 18 August 1975, the CANARY EFFORT PLO and COL Stubblebine, Commander, 902d MI Group, visited the USACC East Coast Telecommunications Center (ECTC), Ft Detrick, MD, for a facility briefing, since the facility is now being covered in the revised CANARY EFFORT OPLAN. The introductory briefing on the ICIP was presented to LTC Jackie L. Manbeck, Commander, USACC ECTC, and CW2 George S. Trivett, OIC, Security Division, USACC ECTC. The CDR, 902d MI Group, and the PLO also made a courtesy visit to COL J. A. Pastore, CDR, Fort Detrick.

(4) On 27 August 1975, COL John S. Eberle, CDR, USACC Site R Telecommunications Center, was provided an introductory briefing on the ICIP CANARY EFFORT.

(5) On 18 September 1975, the Quarterly Progress Briefing was presented to the CDR, USACC Operations Command, COL Clark, at the USACC Operations Command, USACC PTC, Wash, DC, in conjunction with the CENSUS TIME Quarterly Progress Briefing because of the inter-relationships of both ICIPs.

(6) On 25 September 1975, the PLO presented the Quarterly Progress Briefing to the supported command with the following in attendance: COL Harold G. deMoya, CDR, Ft Ritchie; COL John S. Eberle, CDR, USACC Site R Telecommunications Center; COL John J. Plosay, Jr., Deputy CDR, Fort Ritchie, and ACSI&S, 7th Signal Command. All of the above officials expressed their appreciation and continued enthusiasm for the ICIP and made laudatory comments concerning the counterintelligence support rendered during the reporting period.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 6200.1-R

390

CONFIDENTIAL

~~CONFIDENTIAL~~

2. CANINE PLATE: (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD) Romulus, NY

b. Confidential Source Utilization: None.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: On 23 September 1973, COL Alden L. Cox, Commander, Seneca Army Depot, was given the ICIP Quarterly Progress Report which included the history of CANINE PLATE from its inception. COL Cox assumed command of Seneca Army Depot on 4 Sep 75 from recently promoted BG Alan A. Nord. With the PLO now having full, unescorted access to Directorate for Special Weapons and the Special Weapons Storage Area, the prime target area, source recruitment has increased with six (6) conventional sources being used. Additionally, initial assessment was made of one potential source. With the favorable attitude toward ICIP operations evinced by COL Cox it is anticipated that development of the operation will continue. COL Cox stated that he was happy with present state of the operation; he did caution that under no circumstances did he want any "flap" over the program.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

391

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

3. (C) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal, AL

b. Confidential Source Utilization: One

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) Source continues to provide substantial information concerning eight of the persons who were subjects of the allegations which led to the request for the operation. Although Source has been unable to absolutely confirm or refute the allegations made, he has been able to develop associations with all of the individuals involved, to include being invited to social functions at which these persons were in attendance. Fragmentary information provided thus far has caused reason to doubt certain of the allegations, but investigation continues and further information will be reported as received.

(2) Source continues to monitor the security posture of the target area, reporting security infractions, hazards and weaknesses as they occur. Source has reported a renewed practice of poor housekeeping, and a continued lack of compartmentation, lack of control of production facilities, absence of control of hand baggage brought into and out of the target area, and possible compromise of the present badge system due to loss and improper exposure off-post. In an attempt to contribute to the security posture of the target area, Source, in his official capacity as the Administrative Technical Assistant to the Director, Advance Sensors Directorate (ASD), has created and published a complete guide to current security regulations and policies. Copies of the publication were distributed throughout ASD with specific distribution to those persons involved with the storage, creation, or control of classified defense information.

(3) Source is attempting to monitor the duty-hours activities of an individual of Jordanian birth presently employed in ASD as a DAC. This employee appears to be of possible CI interest because of his alleged enthusiastic involvement with other Arabic linguists and his reported recurring trips to New York City, ostensibly for the purpose of purchasing items for his off-duty business interests.

e. Operational Status:

(1) COL Arthur G. Lange, Jr., Chief of Staff, USAMICOM, was briefed on the information provided by Source during the 25-26 June meetings on

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

18 July 1975 by the PLO and on information provided during the 6-7 August meetings on 22 Aug 75 by the PLO. Information provided during the 17-18 September meetings will be provided to COL Lange during the next reporting period. COL Lange expressed his appreciation for the information provided, noted the security weaknesses developed, and indicated that he would examine ways to improve the security posture of USAMICOM. COL Lange was cautioned that corrective actions must be taken in such a manner as to protect the Source.

(2) COL Axelson, former Deputy Director, US Army Missile Research, Development and Experimental Laboratory (USAMRDEL), retired on 31 Jul 75 and was replaced by COL William P. Gojsza on 2 Sep 75. The PLO briefed COL Gojsza on the background of the operation and the individuals involved on 25 Sep 75. MG Vincent H. Ellis, USAMICOM Commander, was succeeded by MG George E. Turnmeyer on 1 Oct 75. The PLO will brief MG Turnmeyer on the ICIP during the next reporting period after coordination has been conducted with COL Lange, CofS, USAMICOM.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1892 of 3957

~~CONFIDENTIAL~~

4. (U) CANVAS TAX: (OACSI Revalidation - 4 Feb 75)

a. Location: Sierra Army Depot (SIAD), US Army Materiel Command, Herlong, CA

b. Confidential Source Utilization: One

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status: One confidential source was recruited during the reporting period. In addition, three conventional sources are currently being used to provide coverage in the target area. The quarterly progress report to SIAD officials has been delayed until 28 October by the direction of the Commander, 525th MI Group. The Commander, SIAD, continues to be interested in suitability information especially about the illegal use of drugs among SIAD personnel and has requested the Project Liaison Officer to continue to emphasize such requirements to Sources. In addition, the commander was provided support to augment depot security during exercise Golden Gloves which terminated 29 September 1975.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

5. (C) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC

b. Confidential Source Utilization: One

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: The Commander, PTC, has reassigned the civilian employee reported in the Fourth Quarter FY 1975 Quarterly Report as having questionable suitability characteristics and conduct to a new job within PTC requiring minimum contact with classified information. Supervisors will continue to monitor his conduct and activities. An Army NCO assigned to PTC attempted to commit suicide by slashing his wrists. The NCO reportedly did so in a moment of deep despair and depression over personal and financial problems. Local police officers, investigating the suicide attempt, reported that the NCO denied being in financial straits and produced his wallet for the officer showing him about $2,000.00 in $100 denominations. The investigating officer observed a screen in the NCO's apartment, of the type believed to be used by marijuana dealers. All information regarding the incident was provided PTC. The NCO's access has been suspended and the Security Officer of PTC has requested that a limited investigation be conducted.

e. Operational Status:

(1) On 18 July 1975, COL Donald E. Clark assumed command of PTC. COL Clark formerly had been at Site R, Ft Ritchie, one of the primary targets of the ICIP CANARY EFFORT. In his initial briefing on CENSUS TIME on 1 August 1975, COL Clark indicated to LTC Chad B. White, CDR, PCF/NCR Field Office, 902d MI Gp, that he desired to have an evaluation of the current security posture of PTC. During the period 8-12 August 1975, a courtesy Security Vulnerability Analysis (SVA) was conducted and provided the supported command.

(2) During the reporting period, PTC was directed by its higher headquarters to comply with Army Regulation 50-5, Human Reliability Program, in conjunction with their storing of two-man control items. The PTC Security Manager requested implementation assistance from the PLO. The PLO, by means of liaison with the US Army Nuclear and Chemical Surety Group, Fort Belvoir, VA, provided PTC with the requested direction and guidance.

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(3) On 18 September 1975, the PLO presented the Quarterly Briefing on the progres of the ICIP to COL Clark, CDR, PTC, and Mr. Daniel E. Thompson, Technical Director, PTC.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 1895 of 3957

~~CONFIDENTIAL~~

6. (U) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories (HDL), Washington, DC

b. Confidential Source Utilization: None

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) During the reporting period no additional information was developed since the previous quarter concerning the visits of the First Secretary, USSR Embassy, Washington, DC to meetings of the Institute of Electrical and Electronics Engineers, a professional society for engineers, which were held in the HDL auditorium. COL Einsel, Commander, HDL, made a determination that the society could no longer hold meetings at HDL in order to preclude any potential security threat and any potential for a repeat of the incident.

(2) The Security Officer, HDL, took several actions in response to recommendations contained in the Courtesy Security Inspection report submitted during the last quarter. These included a pilot 100% inventory of SECRET material to determine feasibility of a complete inventory at HDL, guard force personnel were shifted to new areas and security routines were considerably tightened because of laxness; a study was completed or possible new badges for HDL and security lectures were presented.

(3) On 5 and 17 September 1975, unidentified light aircraft flew over the test site, Woodbridge Research Facility (WRF), HDL, where a series of tests on foreign equipment under the ROUGE-EMORY program was in progress. In both instances the aircraft circled over the ROUGE-EMORY test site for about 5-7 minutes. During the years WRF has been at its present location no known overflights of this type have been reported. The overflights are being investigated in coordination with the FBI.

(4) On 8 Aug 75 a civilian employee, HDL, was referred to the PLO by the FBI. The employee claimed that she was being followed by members of the HDL Security Office, who were involved with a homosexual group at the Van Ness Avenues Facility, HDL. She named a number of persons at HDL as being involved in the group. After investigating her story the Commander, HDL, believed that she is suffering from psychiatric problems. The Commander plans to have employee visit a psychiatrist for a complete evaluation.

e. Operational Status:

(1) A final decision has not been reached by the Secretary of the Army on the creation of the Harry Diamond Developmental Center, a decision

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

had been expected by the middle of September 1975. Criticism by a state congressional delegation to the move, which would result in the loss of 1200 jobs in the state, has delayed a final decision.

(2) On 17 September 1975, COL Thomas McGregor, Commander, HDL, who replaced COL Einsel, MAJ Kenneth F. Keller, HDL, and Mr. James F. Yeick, Security Officer, HDL were briefed on the quarterly progress of the ICIP. COL McGregory, an MI Officer showed considerable interest in the ICIP. It is expected that the excellent attitude toward the program that was shown by COL Einsel will be continued by COL McGregor.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 1897 of 3957

~~CONFIDENTIAL~~

7. GONDOLA STAR: (OACSI Revalidation - 11 Jul 75)

a. Location: Aberdeen Proving Ground (APG), Aberdeen, MD

b. Confidential Source Utilization: Eight confidential sources

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Sources reported that on 13 August 1975, an unknown number of Swedish citizens visited the US Army Ballistic Research Laboratories (BRL) The PLO determined that the visit had been fully coordinated with the proper officials. A Source reported on 26 September 1975 that seven Swedish citizens visited the US Army Materiel Systems Analysis Activity (AMSAA), APG. The PLO determined that the visit had not been properly coordinated, but that AMSAA had taken steps to insure that the visitors would not be given access to classified information until guidance was provided by HQ, US Army Materiel Command (AMC).

(2) Sources reported three instances of foreign travel during the period. A civilian pharmacologist employed at the Biomedical Laboratory, Edgewood Arsenal, attended the Sixth Congress of the International Union of Pharmacologists (IUPHAR) in Helsinki, Finland, held from 20 to 25 July 1975 and attended a luncheon during the Congress hosted by a representative of the USSR. After the Congress, the employee took part in a five-day tour to Leningrad, USSR, sponsored by IUPHAR. This information is being exploited as a DOMEX lead. In another instance, a civilian employee of the Development and Engineering Directorate, Edgewood Arsenal, visited Poland and Czechoslovakia for about one month in June and July 1975. The employee and his spouse allegedly visited relatives in both countries. The employee will be debriefed by USAINTA. In the third instance, a civilian employee of the Human Engineering Laboratory (HEL), APG, planned to take part in a National Geographic Society tour of the USSR in October 1975. The employee will be debriefed by USAINTA after his return.

(3) A source reported three instances of alien enlistees who were assigned to the Human Engineering Laboratory (HEL), APG. Follow-up action by the PLO determined that the Installation Intelligence Officer was aware of the status of the three, that they did not have security clearances and had no access to classified information. In the case of one of the enlistees who allegedly suffers from periods of amnesia, action was taken to deny him a security clearance.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

(4) Source reported three instances of civilian employees of Edgewood Arsenal and one employee of AMSAA, APG, who allegedly engaged in extramarital affairs with other civilian employees. The situations are being discreetly monitored to determine if there is any substance to the allegations before investigations are conducted. An official source reported that an Army officer assigned to AMSAA was allegedly an alcoholic, was cohabitating with a female secretary of AMSAA and had engaged in sexual relations with an Israeli female captain assigned to act as the officer's interpreter during an Oct 74 TDY trip to Israel. Follow-up action disclosed that the officer had been transferred to the US Army Concepts Analysis Agency. A Summary of Information has been prepared and will be forwarded to that Agency. A source reported that a physical scientist employed in the Chemical Laboratory, Edgewood Arsenal, displayed indications of mental and emotional instability. Follow-up by the PLO revealed that the employee had been directed to undergo a "fitness for duty" physical examination which includes a psychiatric evaluation.

(5) An official source reported to the PLO rumors that a civilian employee of the BRL, APG, was involved in difficulties with the police. Follow-up revealed that the Havre de Grace Police Department, Havre de Grace, MD has seven charges on file against the employee ranging from possession of marijuana to grand larceny and assault and battery. The employee is absent without leave. An investigation for suitability of the employee is underway.

(6) A source reported that a high ranking civilian employee of the Human Engineering Laboratory (HEL), APG, brought his eight-year old son in a controlled access area where a classified test was being conducted and remained overnight. The incident was reported to the APG Security Officer and the employee was admonished and counselled by his supervisor. The same source reported that within the HEL classified reports were being typed on one-time typewriter ribbons and carbon that were not being handled as classified waste. The Security Officer, HEL, has stopped the practice and these items are now being disposed of with the classified waste. Another source reported ten separate situations at AMSAA which constituted security hazards or violations. Brought to the attention of the AMSAA Security Officer, all have been corrected.

e. Operational Status:

(1) Following revalidation of the ICIP on 11 July 1975, both the PLO and the PCO concentrated their efforts on reactivating and expanding the ICIP. During the latter half of July, the six confidential sources which had been used previously were recontacted and reactivated, one CIRL whose

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

400

~~CONFIDENTIAL~~

recruitment had been postponed when the project was suspended was recruited on 5 Aug 75; a Source Lead Development Report on another CIRL was approved and this source was recruited on 4 Sep 75. These two sources were the first ones recruited in the US Army Materiel Systems Analysis Activity (AMSAA), a critical sensitive activity at APG. The PLO reestablished liaison contacts with local, state, and federal agencies in addition to maintenance of contacts with ICIP coordinators and security officers of those activities receiving ICIP support at APG. The PLO also established new casual sources in critical areas of the ICIP-supported activities at APG and vetted two new CIRLS who are under initial assessment.

(2) On 22 Aug 75, COL Kenneth L. Stahl, CDR, Edgewood Arsenal, was provided an up-date briefing by the PLO on the status of the ICIP and informed that the ICIP would require revalidation in six months. COL Stahl named CPT Vincent J. Falconio, Security Officer, Edgewood Arsenal, as the new ICIP Coordinator and requested that he be given the initial ICIP briefing. CPT Falconio was given the initial ICIP briefing and a status report on GONDOLA STAR on 22 Aug 75. COL Stahl advised that COL Burt Dall had been assigned as Deputy Commander, Edgewood Arsenal, and requested that COL Dall be given a briefing.

(3) On 17 September 1975, presented the initial ICIP briefing to COL Dall. In the absence of COL Stahl, who was on leave, COL Dall and CPT Falconio, Edgewood Arsenal Security Officer, were also given the Quarterly Progress Briefing on 17 September 1975.

(4) The PLO presented the Quarterly Progress Briefing to COL Alvin D. Ungerleider, Commander, APG; and Mr. Harry A. Mencke, Installation Intelligence Officer, APG. Both COL Stahl and COL Ungerleider expressed their pleasure that the GONDOLA STAR ICIP had been reinstated by the ACSI for an additional six months.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

[redacted]

8. (U) LENS HOLDER: (OACSI Revalidated - 4 Feb 75)

a. Location: White Sands Missile Range (WSMR), NM

b. Confidential Source Utilization: Two confidential sources were utilized during the reporting period.

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status: One additional confidential source was recruited during the reporting period and one individual is presently under assessment as a potential confidential source. On 30 September 1975, the Project Liaison Officer presented the Quarterly Progress Report to MG O. L. Tobiason, Commanding General, WSMR. The following personnel were also present at the briefing: LTC Charles I. Davis, Chief, Security Office, WSMR; LTC Arthur D. McQueen, Operations Officer, 525th MI Gp, CPT Marcel Hull, SAIC, Ft Bliss Resident Office, 525th MI Gp and GS-13 William F. Arket, Chief Intelligence Division, WSMR. Since MG Tobiason was unfamiliar with the Internal Counterintelligence Program (ICIP), the ICIP was explained in detail from its initiation to the present at WSMR. MG Tobiason was pleased with the ICIP LENS HOLDER.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 6200.1-R

[redacted]

~~CONFIDENTIAL~~

9. (U) LENTIL MONKEY: (OACSI Revalidation - 4 Feb 75)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA

b. Confidential Source Utilization: Eight (8) confidential sources

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) The temporary instructor in the Chinese-Mandarin Department, previously reported in the 4th Quarter, FY 75 Quarterly Report, who questioned her students about their future duties and expressed her displeasure at teaching Chinese to students to enable them to spy on the People's Republic of China, submitted her resignation on 4 September 1975. Her last working day was 5 September and she departed the Presidio of Monterey area.

(2) The instructor in the German Language Department, previously reported in the 4th Quarter, FY 75 Quarterly Report, who travelled to East Germany without notifying the DLI Security Officer, has been officially admonished by the Chairman of the German Language Department. She was advised that any future disobedience of DLI Regulations will be punished with a 10 day suspension in accordance with Civil Service Regulations.

(3) An ICIP source developed information that an instructor in the Russian Language Department is a former member of the Soviet Army's equivalent to the US Army Security Agency and that he had received special training in the English language while in the Soviet Army. This individual left the Soviet Union in Apr 74 and was hired at DLI in Oct 74. This instructor was recently joined by a former coworker in the Soviet Union. The new instructor left the Soviet Union in Apr 75 and was hired at DLI in Jul 75. These two individuals taught together at the Leningrad Herzen Pedagogical Institute in Leningrad, USSR in the late 1960s and early 1970s. Messages of inquiry concerning these individuals were sent to USAREUR and a request was sent to the 525th MI Group to conduct discreet checks on the first individual and the Civilian Personnel Office, DLI, submitted a NAC request on the second individual.

e. Operational Status:

(1) During the reporting period three sources were terminated due to their graduation and five sources were recruited. Four students and a

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Technical Language Assistant are presently being assessed.

(2) On 5 Sep 75, COL Samuel L. Stapleton, who replaced COL Koenig as Commandant of DLI, received his first Quarterly Briefing on ICIP LENTIL MONKEY. As a result of the briefing, COL Stapleton directed his security officer to prepare a videotape security lecture to be given to all students on their arrival at DLI. COL Stapleton further directed his security officer to closely coordinate the videotape with the Project Liaison Officer in order to insure coverage of all aspects of the security situation at DLI and to determine the most expeditious was to obtain background investigation for all instructors who have not previously had such investigations. The Security Officer was instructed to investigate the possibilities of having bring-up investigations conducted on previously checked instructors; in addition, he is to coordinate with the Civilian Personnel Office to initiate procedures whereby the hiring of new instructors would be contingent on their receiving favorable security checks. In attendance with COL Stapleton at the Quarterly Briefing was MAJ Richard A. Erickson, Security Officer, DLI.

(3) On 5 Sep 75, subsequent to the Quarterly Briefing, a visit was made to DLI by USAINTA personnel concerning the ICIP. The purpose of the visit was to acquaint the incoming DLI Commandant with some of the potential security problems at DLI which have arisen in the past from the varied, foreign backgrounds of the instructors and the fact that the students are destined for intelligence assignments. The Commandant indicated that he believed the ICIP would prove to be a valuable adjunct to the DLI security program and that he would support the program wholeheartedly. Key personnel in attendance were COL Stapleton; COL William F. Strobridge, CDR, 525th MI Group; LTC Grimes, CDR, Special Operations Detachment, USAINTA; MAJ Richard A. Erickson, Security Officer, DLI; and Mr. Jeremy H. Hughes, PLO.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 1903 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U.S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

OCT 28 1975

MIIA-SO-SA

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOI-C/MAJ EBERSOLE)
WASH DC 20310

1. (U) During September 1975, at the Woodbridge Research Facility (WRF), Harry Diamond Laboratories, personnel conducted a series of classified tests on foreign equipment under the ROUGE-EMORY Program. Since HDL is supported by the ICIP CENTAVO KID, the Project Liaison Officer (PLO) provided assistance to WRF to determine times when the air space over WRF would be free of satellites. The storage area was checked for security and the PLO made several suggestions concerning the camouflaging of the test material while it was in the open. WRF adopted the suggestions. On 5 September, a light aircraft identified only as a Piper Cherokee 140, flew over the test site at which the ROUGE-EMORY material was located, circling and hovering over the site from 5-7 minutes. On 17 September, an unidentified light aircraft again flew over the WRF, particularly circling over the area where the ROUGE-EMORY test equipment had been set up previously. Light aircraft normally avoid the WRF because of the numerous antennas and towers at the Facility. During the time WRF has been at its present location, no known overflights of this type have been reported. The overflights are being investigated in coordination with the FBI.

2. (U) The ICIP providing support to activities located at Edgewood Arsenal and Aberdeen Proving Ground was reactivated during the reporting period as a result of revalidation action by the OACSI on 11 July 1975, raising the total number of active ICIPs in CONUS to nine. The ICIP OPLAN at Fort Ritchie was revised on 15 September to reflect target area realignment resulting from reorganization of the US Army Communications Command (USACC).

3. (U) USAINTA is monitoring an ICIP started on about 1 July 1975 at the Army Security Agency (ASA) Augsberg Field Station, Federal Republic of Germany. USAINTA reviewed the operations plan for the ICIP, coordinated

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

405

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

MIIA-SO-SA
SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

the plan with ASA, and notified ODCSI, USAREUR that the ICIP was approved by the CG, ASA. During the reporting period, no information was received concerning the ICIP.

4. (U) Brief status reports for each ICIP operation reported upon are attached as inclosures.

WILLIAM I. JENNINGS
Special Assistant (OPS)

10 Incl
as

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 6200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

OCT 28 1975

MEIA-SO-SA

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-ZXI-C/MAJ [redacted])
WASH DC 20310

1. (U) During September 1975, at the Woodbridge Research Facility (WRF), Harry Diamond Laboratories, personnel conducted a series of classified tests on foreign equipment under the ROUGE-EMORY Program. Since HDL is supported by the ICIP CHESTAVO KID, the Project Liaison Officer (PLO) provided assistance to WRF to determine times when the air space over WRF would be free of satellites. The storage area was checked for security and the PLO made several suggestions concerning the camouflaging of the test material while it was in the open. WRF adopted the suggestions. On 5 September, a light aircraft identified only as a Piper Cherokee 140, flew over the test site at which the ROUGE-EMORY material was located, circling and hovering over the site from 5-7 minutes. On 17 September, an unidentified light aircraft again flew over the WRF, particularly circling over the area where the ROUGE-EMORY test equipment had been set up previously. Light aircraft normally avoid the WRF because of the numerous antennas and towers at the Facility. During the time WRF has been at its present location, no known overflights of this type have been reported. The overflights are being investigated in coordination with the FBI.

2. (U) The ICIP providing support to activities located at Edgewood Arsenal and Aberdeen Proving Ground was reactivated during the reporting period as a result of revalidation action by the OACSI on 11 July 1975, raising the total number of active ICIPs in CONUS to nine. The ICIP OPLAN at Fort Mitchie was revised on 15 September to reflect target area realignment resulting from reorganization of the US Army Communications Command (USACC).

3. (U) USAINTA is monitoring an ICIP started on about 1 July 1975 at the Army Security Agency (ASA) Augsberg Field Station, Federal Republic of Germany. USAINTA reviewed the operations plan for the ICIP, coordinated

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOIPO
AUTH PARA 1-603 DoD 5200.1-R

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Indefinite

407

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

MIIA-SO-SA
SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

the plan with ASA, and notified CDCSI, USAREUR that the ICIP was approved by the CG, ASA. During the reporting period, no information was received concerning the ICIP.

4. (U) Brief status reports for each ICIP operation reported upon are attached as inclosures.

10 Incl
as

WILLIAM I. JENKINS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

408

~~CONFIDENTIAL~~

D-5

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) Operation

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 11 September 1975

ACTION REQUIRED: CANARY EFFORT (U)
To furnish ACSI, DA approval of subject OPLAN to CDR, USAINTA.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) BACKGROUND: By letter dated 9 September 1975, subject as above (TAB B), the Director of Operations, USAINTA (MIIA-GPC-SO) forwarded to OACSI (DAMI-DOH) for review and approval, a revised operations plan for CANARY EFFORT (U) which provides for continuation of the existing ICIP at Fort Ritchie, Maryland. Revision of the existing OPLAN was necessitated by the reorganization and redesignation of the US Army Communications Command (USACC) - CONUS as the 7th Signal Command effective 1 July 1975.

2. (U) DISCUSSION:

a. Major changes in the revised OPLAN are as follows:

(1) Realignment of target areas and increased coverage to the Telecommunications Directorate, the Alternate Joint Command Center (AJCC), the Alternate National Military Command Center (ANMCC), the Alternate National Command Center Support Directorate (ANMCCSD), and the East Coast Telecommunications Center (ECTC). All are considered priority I for the purposes of counterintelligence support. The ECTC is located at Fort Detrick and the other activities are all at Fort Ritchie.

(2) The Execution Phase of the revised OPLAN remains essentially unchanged except for the addition of a Project Case Officer (PCO) at Fort Detrick to assist in providing coverage for the ECTC.

(3) The OPLAN provides that each source and individual involved in the conduct and control of the operation will sign a certificate stating that he has been briefed and understands the provisions and constraints imposed by AR 380-13.

b. There is no significant change in the objectives of the OPLAN.

3. (U) RECOMMENDATION: That the ACSI approve the revised OPLAN and sign the 1st Indorsement to the USAINTA letter at TAB A.

(Continue on plain bond)

IMPLICATIONS: CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		11 Sep 75
			DIR		11 Sep 75
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*
K. V. Haendle, LTC, GS/56159

409

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED ON 5 SEP BY USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

ACSI FORM 28, 13 Sep 71

CONFIDENTIAL

DAMI-POM (9 Sep 75) 1st Ind
SUBJECT: Internal Counterintelligence Program (ICIP) Operation CHAOS
Report (U)

HQDA, Office of the Assistant Chief of Staff for Intelligence, ATTN: DAMI-POM, Washington, DC 20310 15 SEP 1975

TO: Commander, US Army Intelligence Agency, ATTN: MIIA-GPC-SO(M), Fort Meade, Maryland 20755

The attached SMLR, subject as above, is approved.

(sgd) Harold R. Aaron

2 Incl
nc

HAROLD R. AARON
Maj Gen, GS
ACofS for Intelligence

470

CONFIDENTIAL

Regraded Unclassified when
Separated From Classified
Inclosure

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

09 SEP 1975

MI1A-GPC-SO(SA)

SUBJECT: Internal Counterintelligence Program (ICIP) Operation CANARY EFFORT (U)

HQDA (DAMI-DOI-C/LTC HAENDLE)
WASH DC 20310

1. (U) The 1 July 1975 reorganization and redesignation of the US Army Communications Command (USACC) - CONUS as the 7th Signal Command resulted in a realignment of target areas of the ICIP CANARY EFFORT (U) at Fort Ritchie, Maryland. Attached as inclosure 1 is a revised operations plan for CANARY EFFORT (U) which provides for continuation of the existing ICIP and reflects the changes brought about by this reorganization.

2. (U) The new 7th Signal Command reorganization has necessitated a change in the mission of the ICIP to provide increased coverage for the Alternate Joint Command Center (AJCC) and those activities designated by the Commander, 7th Signal Command, as listed in paragraph 4, below, and Annex A. There is no significant change in the objectives. The activities listed in Annex A will be considered Priority I for purposes of counterintelligence support. The Execution Phase of the revised OPLAN remains essentially unchanged except that an additional PCO will have a base of operations at Fort Detrick, MD, to assist in providing coverage for the East Coast Telecommunications Center (ECTC), which is located at Fort Detrick. The revised OPLAN provides that each source and individual involved in the conduct or control of the operation will be thoroughly briefed on the provisions and constraints of AR 380-13 and additionally will be required to sign a certificate stating that they have been briefed and understand the limits imposed by AR 380-13.

3. (U) Four organizational charts which show the former and present command and staff organization by line charts of the 7th Signal Command are attached as inclosure 2. These charts illustrate the principal internal changes occurring as a result of the 1 July 1975 reorganization.

411

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 2005

~~CONFIDENTIAL~~

U 0 SEP 1975

MIIA-GPC-SO(SA)
SUBJECT: Internal Counterintelligence Program (ICIP) Operation CANARY EFFORT (U)

4. (C) The Telecommunications Directorate, primary target for the present ICIP, was formerly under the operational control of the Commander, Fort Ritchie. With the reorganization, the Telecommunications Directorate, as well as USACC Site R Telecommunications Center and all other USACC Telecommunications Centers in CONUS, are under the operational control of the newly established USACC Operations Command. In addition to the USACC Operations Command elements indicated, the following additional activities will be supported by the revised operations plan:

a. Alternate National Military Command Center (ANMCC).

b. Alternate National Military Command Center Support Directorate (ANMCCSD).

c. East Coast Telecommunications Center (ECTC).

5. (U) Recommend approval of revised plan at inclosure 1.

FOR THE COMMANDER:

2 Incl
as

for ARION N. PATTAKOS
LTC, MI
Director of Operations

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

412

~~CONFIDENTIAL~~

Page 1911 of 3957

[redacted] CONFIDENTIAL

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 3 Sep 75

ACTION REQUIRED: To obtain approval of the quarterly ICIP Report

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) Background: By memorandum dated 8 February 1972 (TAB B) the Under Secretary of the Army requested that the VCSA provide a quarterly report on all ICIP operations.

2. (U) Discussion:

a. During the past quarter, in response to a request from the Commander Aberdeen Proving Ground, the ICIP which had been terminated at that installation was revalidated for six months. This operation will be reexamined during the first calendar quarter 1976.

b. Memorandum at TAB A provides the information required by the Under Secretary of the Army for the remaining eight ICIP operations.

3. (U) Recommendation: That memorandum at TAB A be approved and signed.

MFR - Cy of VCSA/USofA appr fwd to USAINTA 29 Sep 75

RAE

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

(Continue on plain bond)

IMPLICATIONS: CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		
			DIR		7-24-75
			EX		
			ACSI		
			DISPATCHED (DTG)		
SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET					

ACTION OFFICER *(Name, grade, phone and signature)*

MAJ Ebersole/56159 L. Ebersole 413 9467-75

ACSI FORM 28, 13 Sep 71

[redacted] CONFIDENTIAL

REGRADED CONFIDENTIAL
WHEN SEPARATED FROM CLASSIFIED
ENCLOSURE

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U.S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

JUL 17 1975

MIIA-GPC-SO

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOI-C)
WASH DC 20310

1. (U) ~~(C)~~ Three incidents of counterintelligence interest involving Soviets or persons tentatively identified as Soviets were reported upon during the fourth quarter of FY 1975. One such report was that a First Secretary of the USSR Embassy visited an auditorium in the Harry Diamond Laboratories (HDL), on two occasions to attend evening meetings of the Institute of Electrical and Electronics Engineers, Inc., (IEEE), a professional society for engineers. The Soviet official attended one IEEE meeting, but was refused entrance to a second meeting. Although only unclassified matter is presented at these meetings, the potential security dangers are self evident. Details of the incident were reported to the FBI.

2. (U) ~~(C)~~ Two other incidents involving persons tentatively identified as Soviets occurred in the Fort Ritchie area. The first report, which was in April 1975, concerned an individual bearing a strong resemblance to a KGB member who paid an unusual amount of attention to a shipment of sensitive equipment destined for Fort Ritchie. The second incident concerned an individual assigned to Fort Ritchie who reported that a man representing himself as a contract employee attending a DOD-sponsored conference in Pennsylvania claimed extensive contact with Soviets in Hagerstown, MD. Although the latter incident occurred in 1974, because of the sensitivity of Ft Ritchie, both incidents have been reported to the FBI with a request for an investigation to include a determination if there is any relationship between the two incidents.

3. (U) ~~(C)~~ Correspondence was submitted on the ICIP GONDOLA STAR at Aberdeen Proving Ground which was reported in the 3d Qtr, FY 75, as scheduled for termination, requesting that the Operation be reconsidered for continuation. Excluding this ICIP, there were eight active ICIPS at the close of the reporting period.

Classified by CDR, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
AUTOMATICALLY ON 31 DEC 2005

414

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

MIIA-GPC-SO
SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

4. (U) Brief status reports for each ICIP operation reported upon are attached as inclosures.

FOR THE COMMANDER:

Albert N Weidhas

8 Incl
as

ALBERT N. WEIDHAS
Colonel, MI
Director of Operations

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 1914 of 3957

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

DAMI-DOH

18 SEP 1975

MEMORANDUM THRU: VICE CHIEF OF STAFF, UNITED STATES ARMY

FOR: ~~UNDER SECRETARY OF THE ARMY~~ NOTED BY 24 SEP 1975 THE UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) (U) -- INFORMATION MEMORANDUM

1. (U) During the past quarter, three incidents surfaced as a result of ICIP operations which involved known or suspected Soviets. One report concerned a USSR Embassy official who visited an auditorium at the Harry Diamond Laboratories on two occasions, to attend evening meetings of the Institute of Electrical and Electronics Engineers. The official attended one meeting, but was denied entrance on a second occasion. The other two incidents occurred in the Fort Ritchie, MD area. One concerned a report of an individual bearing a strong resemblance to a KGB member who was particularly concerned about a shipment of sensitive equipment destined for Fort Ritchie, while the other involved a man representing himself as a contract employee attending a DOD-sponsored conference in Pennsylvania, who claimed extensive contact with Soviets in Hagerstown, MD. All three incidents were reported to the FBI.

2. (U) In response to a request from the Commander, Aberdeen Proving Ground, MD, I have revalidated GONDOLA STAR for a six-month period. I plan to closely monitor the results of this operation, and will make a final determination in January 1976 as to whether or not it should continue.

3. (U) Summaries of the eight on-going ICIP operations are inclosed.

18 SEP 1975

RECOMMEND APPROVAL - VCSA

HAROLD R. AARON
Major General, GS
ACofs for Intelligence

8 Incl
as

WILLIAM G. HANNE
Major, GS
Assistant to the Director
of the Army Staff

Classified by: ACSI, DA
Declassify on: 31 Dec 2005

~~CONFIDENTIAL~~

MAJ Ebersole/56159
Typed by G. Rivera

REGRADED UNCLASSIFIED ON SEP 5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

[redacted]

1. (C) CANARY EFFORT: (OACSI Revalidation - 4 Feb 75)

a. Location: Fort Ritchie, MD.

b. Confidential Source Utilization: Three confidential sources.

c. Information obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Information was surfaced pertaining to the alleged abuse of drugs on the part of seven (7) individuals assigned sensitive/critical duties. Additionally, adverse suitability information concerning nine (9) individuals was reported. This information involved indebtedness, alcohol abuse, moral improprieties and mental instability. As a result of the information furnished, four individuals had their access to classified information suspended; investigations were requested on three individuals; and the activities of the other individuals are being monitored.

(2) Information was reported concerning an individual who resembled a suspected KGB member. The individual has paid an inordinate degree of attention to the activities of a US civilian firm and a sensitive shipment destined for Fort Ritchie. Another individual reported conversations that occurred in August 1974 in a bar in Waynesboro, PA where he learned that an individual believed to be a contract employee claimed to have had contacts with Soviets who worked in Hagerstown, MD. Both incidents were reported to the FBI with a request for investigation.

e. Operational Status:

(1) On 25 June 1975, the PLO briefed COL Harold G. deMoya, Cdr, Fort Ritchie, and COL John J. Plosay, Jr., Deputy Cdr, Fort Ritchie.

(2) COL Donald E. Clark assumed command of the 7th Signal Command (which includes the Pentagon Telecommunications Center) on 18 July 1975 and was briefed on CANARY EFFORT. The 902d MI Group which is conducting the ICIP at Fort Ritchie prepared a revised operations plan reflecting changes in mission and target areas which resulted from the reorganization of the US Army Communications Command (USACC) into the 7th Signal Command. Prior to the reorganization the Telecommunications Directorate, located at Site "R" and the primary target for the ICIP, was under the operational control of the Cdr, Fort Ritchie. Under the new organization, the Telecommunications Directorate, as well as the telecommunications centers throughout CONUS, are under the operational control of a new established activity, the USACC Operations Command.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 6200.1-R

417

[redacted]

~~CONFIDENTIAL~~

2. ~~(S)~~ CANINE PLATE: (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD), Romulus, NY

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: On 6 May 1975, COL Alan A. Nord, recently assigned as Commander, Seneca Army Depot, was provided an initial briefing on the ICIP Operation CANINE PLATE (U). COL Nord stated that he favored the expansion of the Operation and the PLO should be allowed full, unescorted access to the Directorate for Special Weapons and the Special Weapons Storage Area. The last change would permit spotting and assessing potential sources in areas not open previously to the PLO except by peripheral contact. During the reporting period, contact was made with four conventional sources. Additionally, initial assessments were made of two potential sources, one in the Transportation Division and one in the Directorate for Quality Assurance. The PLO has been involved with providing informal counterintelligence assistance to the Military Police Company responsible for the physical security of SAD. Since the initial briefing on the ICIP was presented to the Commander on 6 May 75, a subsequent Quarterly Progress Report was not given. With the expanded latitude and favorable attitude toward ICIP operations evinced by COL Nord it is anticipated that development of the operation will be accelerated.

RELEASED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

418

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

3. (C) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal, AL

b. Confidential Source Utilization: One.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: The ICIP confidential source provided substantial information on security weaknesses within the supported command to include poor housekeeping practice, lack of control of reproduction facilities, lack of proper control of area access, lax security attitudes and possible compromise of security badges through continued loss. As a result of the information provided by the source, the Director, US Army Missile RD&E Lab, directed that poor housekeeping practices be corrected prior to 1 July 1975 subject to his personal inspection. Source will continue to monitor the security posture of the target area. Additional information has been obtained on the personalities involved in the previous investigation under provisions of AR 15-6 which led to the initiation of the operation for the insertion of a Confidential Source into the target area. Information provided has resulted in the initiation of credit checks and local agency checks to confirm or refute allegations.

e. Operational Status: On 16 April 1975, confidential source, a Military Intelligence warrant officer was inserted into the target area as an administrative officer. This source appears to be very well received within the target area and has provided substantial information to include information noted in paragraph 1d above. His outgoing, friendly manner coupled with his professional intelligence background will increase the potential of the ICIP operation. COL Arthur G. Lange, Jr., Chief of Staff, USAMICOM, was briefed on the implementation of the operation on 7 April 1975. He was subsequently briefed on 9 June and will be briefed subsequent to each meeting with the confidential source. The briefing given COL Lange after each meeting with the confidential source will be given in lieu of the Quarterly Progress Briefing since this will keep USAMICOM informed of the progress of the operation on a more current basis than would be the case if briefing were confined to Quarterly Progress Reports. The PLO's briefing was well received by COL Lange, who indicated that he would inform MG Ellis.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1918 of 3957

~~CONFIDENTIAL~~

4. (24) (C) CANVAS TAX: (OACSI Revalidation - 4 Feb 75)

a. Location: Sierra Army Depot (SIAD), US Army Materiel Command, Herlong, CA

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: Four conventional sources are currently being used to provide coverage in the Priority I Targets which are Exclusion Area I, Storage Area for Special Weapons; and Exclusion Area II, Maintenance and Calibration Facilities for Special Weapons. Recruitment of one confidential source is pending and a second potential source in Exclusion Area II is undergoing initial assessment. The Quarterly Progress Report was presented by the PIO on 3 July 1975 to the following SIAD officials: COL Robert Hawlk, Commander, SIAD; LTC Bernard Render, Dep CDR, SIAD; MAJ John Jolley, Provost Marshal/ Security Officer, SIAD; CPT Wayne Herringer, Intelligence Officer, SIAD; and Mr. Anthony Tornabene, Asst Intelligence Officer, SIAD. The Commander, SIAD, requested that the PIO brief him on the nature of the EEI levied on sources in the ICIP. The Commander indicated that he is interested in determining if the remoteness of the area and the type of duty has any bearing or influence on the number of suitability cases among SIAD personnel. The Commander feels that there may be a number of suitability cases among his present personnel involving such factors as sexual promiscuity, alcohol or drug abuse, or excessive indebtedness. By identifying these individuals, the Commander will strive to reduce personnel problems at SIAD. COL Hawlk indicated that he was satisfied with the progress being made in efforts to develop the ICIP and make it a more viable operation.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

420

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

5. (C) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC

b. Confidential Source Utilization: One.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: An ICIP source reported that a PTC civilian employee's effeminate gestures and high pitched voice were responsible for office gossip that the employee was a homosexual. The employee, who is currently employed as a relay operator, was transferred from the coding and decoding section because he allegedly coded an obscene message that was to be sent to an overseas user. The ICIP source provided other information concerning possible security violations involving the employee. The employee's dossier was examined and it was noted that during a background investigation conducted approximately ten months ago, there were recommendations that the employee not be considered for positions of trust and responsibility. Investigative efforts are continuing to verify or refute allegations concerning the employee.

e. Operational Status: The reorganization of the US Army Communications Command at Ft Ritchie into the 7th Signal Command has had an effect on the operational status at the PTC. COL Clark, who has a positive attitude toward the ICIP assumed command of PTC in July, and was given a full progress report of this operation. All personalities in the operation have changed. In addition to the new commander who is amiable to the program, there is a new security manager, CPT Richard Pederson, who gave the program support previously when he was assigned to the Defense Language Institute, East Coast, Washington, DC. A new PLO has also been assigned to the operation. With the above personnel changes and COL Clark's encouraging attitude, this ICIP is now afforded an excellent opportunity to expand and be more productive.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 1920 of 3957

6. (U) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories (HDL), Washington, DC.

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians - None.

d. Useful Information Obtained:

(1) It was reported that a First Secretary at the USSR Embassy in Washington, DC had attended a meeting of the Institute of Electrical and Electronics Engineers, a professional society for engineers, which was held in the HDL auditorium. The subject matter presented during the evening was unclassified. When the Soviet official attempted to attend a second meeting of the society, he was denied entry. Both incidents were reported to the FBI. The Commander, HDL was advised that the use of the auditorium by outside groups would render it insecure until appropriate security checks were conducted.

(2) The PLO noted and called to the attention of the HDL Security Officer several minor security problems during the period. These were either corrected on the spot, or recommendations for correction were made.

e. Operational Status: The final report for the reorganization of HDL into the Harry Diamond Developmental Center (HDDC) was submitted to Congress and the Secretary of the Army. It was expected that the Secretary of the Army would make a final decision by September 1975. The consolidation of various electronics facilities under the control of HDDC will make HDDC the prime center for electronics research and development in Department of the Army. If approved, the consolidation at HDL would begin in October 1976. COL Einsel, Cdr, is scheduled to depart HDL about September 1975. His replacement will be COL Richard H. Sawyer, who is now serving as the Commander of the Watervliet Arsenal, Watervliet, New York. On 11 June 1975, COL Einsel, Cdr, HDL, and Mr. James F. Yeick, Security Officer, HDL, were briefed on the quarterly progress of the ICIP.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

422

[redacted]

7. (U) LENS HOLDER: (OACSI Revalidation - 4 Feb 75)

a. Location: White Sands Missile Range (WSMR), NM.

b. Confidential Source Utilization: One confidential source was utilized during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: The following information on WSMR personnel reported by the confidential source in this ICIP was reported to the Chief, Intelligence Division, WSMR, who took action as indicated:

(1) A report to the Security Officer, Army Missile Test and Evaluation (ARMTE) Directorate that an ARMTE employee frequently left his security container open and unattended resulted in a special briefing on WSMR Regulation 380-5 (Security Regulation) for all ARMTE employees who also were required to sign certificates that they understood the requirements of the security regulation.

(2) The civilian firm which contracts for security guards at WSMR permitted an enlisted man to work part-time as a guard in the Exclusion Area of TRASANA without having the proper security clearance for that area. The Security Office, WSMR, has now insured that the enlisted man has been processed for the proper clearance by the contractor.

(3) Reports of several instances of laxity on the part of TRASANA security guards at night and instances of classified material left in in/out boxes after duty hours. The Security Officer took immediate action upon receiving this information to re-orient guards and personnel on their security obligations. Source has reported a noticeable improvement in security since the earlier reports.

(4) Reports of an Army Officer assigned to the Office of Missile Electronics Warfare (OMEW) who allegedly was misappropriating computer and electronics equipment to build his own computer at home were passed in a Summary of Information to the Sixth Region US Army Criminal Investigation Division Command for action by that agency.

e. Operational Status: One confidential source was recruited early in the reporting period. A second confidential source is in the final stages of assessment in the Office of Missile Electronics Warfare. On 17 June 1975, the PLO presented the Quarterly Progress Report to MG R. J. Proudfoot, Commanding General, WSMR. The following personnel were also present at the briefing: COL William F. Strobridge, Cdr, 525th MI Group, LTC Charles I. Davis,

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

Chief, Security Office, WSMR, and Mr. William F. Arket, Chief, Intelligence Division, WSMR. MG Proudfoot indicated that he was pleased with the progress of LENS HOLDER and stated that WSMR needed this type of program.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1923 of 3957

~~CONFIDENTIAL~~

8. (U) LENTIL MONKEY: (OACSI Revalidation - 4 Feb 75)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Six (6) confidential sources.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) A Source in the Chinese-Mandarin Language Department furnished information concerning a temporary instructor of that department who closely questioned her students about their knowledge of their future duties and expressed her displeasure at teaching Chinese to students to enable them to "spy" on the People's Republic of China. A DCII check, made to review the instructor's USAIRR Dossier, revealed no dossier in the files. The instructor who was born in Canton China and is a British citizen, will not have her employment contract with DLI renewed when it expires in September 1975.

(2) Information was reported concerning the travel of an instructor of the German Language Department to East Germany without the required notification to the DLI Security Officer. The DLI Security Officer plans to permit the instructor to perform the travel and upon return to DLI will question her concerning non-compliance with DLI regulations.

(3) A Technical Language Assistant in the Russian Language Department reported a visitor to that Department in late May. The visitor requested copies of training material used in the Russian Dept, claiming he wanted it for training purposes in his reserve unit. The visitor was given two training exercises which were unclassified and taken largely from Russian language periodicals. The visitor, who was told to return later because additional material was not readily available did not return. Sufficient identifying data was not obtained on the visitor but an attempt is being made to obtain fuller identification. As a result of the incident the Director DLI, at a staff meeting placed special emphasis on the responsibilities of all staff members to be alert for unauthorized visitors. In addition, visitor requirements and restrictions were published and distributed throughout DLI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 30 July 1975

ACTION REQUIRED: To provide approval/disapproval to an operation plan.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) ~~(C)~~ BACKGROUND: Inclosure to TAB A is an operations plan for an ICIP submitted informally by the Pentagon Counterintelligence Force. The plan calls for an ICIP in the OACSI Communications Center.

2. (U) ~~(C)~~ DISCUSSION: While the OACSI Communications Section is a sensitive element of OACSI, it is extremely small and confined. Security would be difficult to maintain as evidenced by the fact that several individuals in the OACSI administrative office were aware of the proposed ICIP.

3. (U) RECOMMENDATION: That the proposed ICIP be disapproved and the memorandum at TAB A be signed and forwarded to the Commander, Pentagon Counterintelligence Force.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

(Continue on plain bond)

IMPLICATIONS — CMPO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		31 JULY 75
			DIR		31 JUL
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*: R. A. Ebersole, MAJ/56074 426 R Ebersole

Classified by ACSI DA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2a
DECLASSIFY ON 31 Dec 2005

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

DOWNGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

1 AUG 1975

DAMI-DOH

MEMORANDUM FOR: COMMANDER, PENTAGON COUNTERINTELLIGENCE FORCE

SUBJECT: Internal Counterintelligence Program (ICIP)(U)

1. (U) Subsequent to the submission of the inclosed operations plan, the entire ICIP was critically reviewed. The result of this review was the termination of operations at installations and facilities where degree of sensitivity of the facility, or the type information developed did not justify the expenditure of resources.

2. (U) (C) The OACSI Communications Section, while an extremely sensitive element of OACSI, is staffed primarily with senior NCO's and a number of civilians who have been employed in the same area for considerable periods of time. The number of personnel employed in the Communications Section is approximately 30, and these individuals man the area on a 24 hour basis. They process large volumes of mail and messages each month and there is considerable pressure exerted continually to insure correspondence handling is correct. Considering the size of this element, and the working conditions under which they operate, the security of an ICIP is doubtful. Further, the pressures and frustrations could be expected to increase if there were any indications of the existence of an ICIP.

3. (U) (C) The activities of this element have been examined, and other than the sensitivity of the facility, there is no indication as to why this element would be a more lucrative target for an ICIP than any other element in OACSI.

4. (U) The attached operations plan is not favorably considered because the target is not considered sufficiently appropriate for an ICIP.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Signed
E. R. THOMPSON
Brigadier General, GS
Director of Intelligence
Operations

1 Incl
as (CONFIDENTIAL)

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 2005

HUMINT DIVISION
RECORD COPY

427

~~CONFIDENTIAL~~

[redacted]

OPERATIONAL PLAN

SUBJECT: Operations Plan, Internal Counterintelligence Security Program, Office Chief of Staff for Intelligence, The Pentagon, Washington, DC

DATE: 5 November 1974

REPORT NO:

PROJECT NO:

REFERENCES: (U)

a. Chapter 5, Section III, USAINTC Regulation 381-100, 1 March 1974 (C)

b. Chapter 2, USAINTC Regulation 381-100-1, 8 February 1974 (S)

c. DOD Directive 5100.49, dated 3 December 1965, Subject: Pentagon Counterintelligence Program.

d. AR 381-115, dated 2 July 1969, Subject: Counterintelligence Investigative Agencies.

e. AR 381-130, with changes 2-4, Subject: Counterintelligence Investigations, Supervision and Control.

f. FM 30-17, dated January 1972, Subject: Counterintelligence Special Operations.

g. FM 30-17A, dated February 1973, Subject: Counterintelligence Special Operations (C).

h. AR 380-13, dated 30 September 1974, Subject: Acquisition and Storage of information Concerning Non-Affiliated Persons and Organizations.

[redacted]

---

1. (U) MISSION:

a. Requirement: The mission of the OACSI, Administrative Office, Communications Section is to process incoming and outgoing mail; provide mail pick-up and delivery; world wide attache pouch support via coordination with the State Department. The Communications Section also maintains a registered mail record; a TOP SECRET Control Office; and operates a NATO, SEATO and CENTO sub-registry. There are approximately twenty thousand messages per month up to and including collateral TOP SECRET handled by this section.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

428

[redacted]

Classified by [redacted] USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY [redacted]
DECLASSIFY ON: Dec 31, 2004

CONFIDENTIAL

b. Objective: This operation will provide the ACSI with a concentrated, aggressive security service within the confines of the Pentagon Reservation, and will provide a fast factual reporting system of any imminence of activities which would necessitate immediate command action and possibly pose a direct threat to the security of OACSI Communications Section. In order to accomplish the objective of this operation, an effective and coordinated use of overt and covert counterintelligence sources and techniques will be implemented which are designed to detect, neutralize, and eliminate the following elements and factors which pose a direct threat to the security of the Communications Sections.

(1) Acts of espionage, sabotage, or subversion.

(2) Hostile foreign intelligence activities.

(3) Disloyalty, disaffection, and other threats to the security of OACSI.

(4) Character weakness, habits, or improper conduct which makes personnel assigned to the Communications Section vulnerable to coercion or blackmail.

(5) Acts of the Communications Section personnel affiliated with anti-Army dissident organizations which seek to disrupt the maintenance of good order, discipline, and morale within the Pentagon.

c. Base of Operations: Special Operations Section, Pentagon Counterintelligence Force/National Capital Region Field Office, 902d MI Group, Room BE 800, The Pentagon, Washington, DC 20310.

2 (U) ~~(C)~~ PERSONNEL:

a. Confidential Source Personnel: To be selected from personnel assigned to the Communications Section, OACSI.

b. US ARMY Intelligence Personnel: The following personnel of PCF/NCR FO will function in the capacities indicated:

(1) Project Officer: CPT Kenneth R. Schlag

(2) Project Control Officer (PCO): CW2 Shawn M. Sandlin

(3) Alternate PCO: CW2 Leonard NMN Gross

(4) Project Liaison Officer (PLO): CPT Kenneth R. Schlag

(5) Alternate PLO: SFC George E. Perry

3. (C) COVER AND DOCUMENTATION: (SEE ANNEX A)

REGRADED UNCLASSIFIED ON SEP - 5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

429

CONFIDENTIAL

Page 1928 of 3957

a. The ICIP Project Officer and PLO will function in a completely overt manner. No attempt will be made to conceal their affiliation with military intelligence.

b. The PCO will employ shallow cover in his contacts with confidential sources. He will not disclaim affiliation with US Army Intelligence, since to do otherwise would alarm prospective sources.

4 (U) ~~(C)~~ EXECUTION:

a. Concept of Operations:

(1) The ICIP will be implemented by using the coordinated employment of overt liaison contacts and confidential source(s). Only confidential sources will be used in this operation due to the small size of the target area.

(2) A concerted effort will be exerted towards the collection of information concerning military personnel assigned to the Communications Section. Collection will not extend to non-DoD personnel. In the event any individual not affiliated with DoD is identified as posing a threat against the Cables Section, the provisions of reference h will apply and prompt coordination will be effected with the appropriate authority. Each individual and source involved in the conduct or control of the operation will be briefed on current policies and constraints pertaining to counterintelligence activities as they concern persons and organizations not affiliated with DoD, reference h.

(3) The PLO will be the point of contact between the ACSI and PCF. The PLO will present to the ACSI or his designated representative, a quarterly briefing on the progress of the operation. In the event the PLO receives information requiring immediate action by OACSI, the information will be released to the ACSI and the Commander, 902d MI Group. Such information will be sanitized or otherwise protected to insure continued operational viability and source utilization.

(4) Specific EEI to be pursued are:

(a) Determine the existance of espionage, sabotage, or subversion within the target or directed against the target.

(b) If espionage, sabotage, or subversion is known or suspected, identify the perpetrators, the nature and scope of their activities, their methods of operation, and the foreign or domestic organization controlling such activity.

(c) Determine the prevalence of dissident activity within the target area, identify military or civilian personnel involved, and resolve whether such activity is supported or directed by elements outside the OACSI.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1929 of 3957

~~CONFIDENTIAL~~

(d) Detect and report adverse suitability information, foreign contacts by Cables Branch military members, and other significant matters which may be exploited by hostile intelligence services.

a. The following activities and types of individuals will be subjected to continuous and intensive counterintelligence coverage:

(1) Known or suspected security risks.

(2) Persons who are known or suspected to associate with persons who are known or suspected members of hostile intelligence or subversive organizations.

c. Implementation:

(1) Overt Phase: The overt phase will begin immediately upon approval of this plan. Close liaison will be maintained with selected OACSI Staff and security personnel. The PLO will be primarily responsible for the spotting and assessment of prospective confidential sources. The spotting will be continuous throughout the operation so as to assure an adequate bank of prospective sources for possible covert utilization. The PLO will conduct the overt functions as necessary to include investigative activities and quarterly briefings concerning the status of the ICIP.

(2) Covert Phase: The covert phase will be the responsibility of the PCO with the assistance of the Alternate PCO. This phase will include the exploitation of confidential sources who have been recruited from among the military personnel. The PCO is also responsible for vetting, recruitment, targeting, training, and disposition of confidential sources. The objective of this phase will be the development of, timely reporting of credible information relating to the detection, neutralization, or exploitation of factors or individuals who pose a direct threat to the security of the Cables Branch, and thus the United States.

5. (U) ~~(C)~~ COMMUNICATIONS: (SEE ANNEX B)

a. Communications between the Project Officer and PCO/PLO will be conducted almost exclusively through personal meetings; telephone will serve as an alternate.

b. Primary communications with confidential sources will be through personal meetings at pre-selected safe sites in the Washington Metropolitan area, or the Pentagon.

c. Alternate means of communications with confidential sources will be via US Mail, using Post Office boxes in the Arlington, Virginia area. A Post Office box may also be used by the confidential source, if circumstances at his residence indicate a possibility of other persons gaining access to his personal mail.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 1930 of 3957

d. Emergency means of communications from confidential sources to PCO will be by telephone to an existing unlisted telephone number located in the office of the Special Operations Section, PCF/NCR. After duty hours, the confidential source will leave a message for the PCO at a telephone located in the PCF. This telephone is manned 24 hours a day, and night personne will be briefed concerning their actions should a source telephone and ask to speak to the PCO. The source will be asked to leave his name (cover name) and a telephone number where he may be reached. PCF night personnel will then immediately pass the information to the PCO, or if the PCO is unavailable the alternate PCO. From PCO to source, emergency communications will be by telephone call to sources home or office, as appropriate.

6. (U) ~~(C)~~ TRAINING:

Training of confidential sources will be continuing process and a portion of each meeting will be devoted to instruction. Emphasis will be placed on security of the operation and the source and reporting procedures. Observation and description, targeting, and related subjects based on source's role will also be included. Each indivudual and source involved in the conduct of the operation will be briefed on current policies and constraints pertaining to counterintelligence operations and activities as they concern persons and organizations not affiliated with DOD, Reference h. The training administered to source(s) will be in the quantity necessary to develop the maximum information from the target comensurate with the previous intelligence and experience of source(s).

7. ~~(C)~~ FINANCE AND LOGISTICS: (SEE ANNEX C)

b1

8. (U) ~~(C)~~ TERMINATION: (SEE ANNEX D)

a. Confidential sources recruited under this plan will be terminated when their usefulness to the plan ceases, when they show indicators of insecure security practices which would jeopardize the operation, are no longer amenable to control, or when the operation is terminated by proper authority. Circumstances under which termination is effected will determine whether termination is with or without prejudice.

b. The only commitments made to confidential sources employed in this operation will be assurance of personnel and job safety through anonymity, and of reimbursement of any legitimate expenses incurred during the operation.

Page 1931 of 3957

c. Knowledgeability of confidential sources will be limited to the following:

(1) Name and physical description of the PCO and Alternate PCO.

(2) Location of meeting sites as well as that of PCF.

(3) Means of alternate and emergency contact with PCO: Namely the Post Office Box number(s) and the telephone number(s) where PCO may be contacted in the event of an emergency.

(4) The approach method used by the PCO in his initial contact with confidential sources.

d. As a control factor, confidential sources will be required to sign a statement evidencing their willingness to cooperate and attesting to the fact that all facets of security will be strictly adhered to. This will not be construed to be a contractual agreement, but will be used as a physhological instrument to enhance the security of the operation.

e. Security considerations are contained in ANNEX E.

9. (U) ~~(C)~~ COORDINATION AND LIAISON:

Liaison with designated OACSI officials and other appropriate Pentagon Agencies will routinely be effected the PLO.

10. (U) REPORTING:

a. Formats for operational reports are contained in Chapter 5, Section III, USAINTC Regulation 381-100 (reference a.)

b. Production reports will be in Agent Report Format.

ANNEX A-Cover and Documentation (Ø)

ANNEX B-Communications (Ø)

ANNEX C-Finance and Logistics (Ø)

ANNEX D-Termination (Ø)

ANNEX E-Security Considerations (Ø)

ANNEX F-Knowledgeability List (U)

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

433 KENNETH R. SCHLAG
PROJECT OFFICER

Page 1932 of 3957

CONFIDENTIAL

ANNEX A - Cover and Documentation

1. (c) b1

a. b1

b. b1

c. b1

2. (c) b1

3. (c) b1

a. b1

b. b1

4. (c) Documentation:

b1

434

CONFIDENTIAL

Page 1933 of 3957

ANNEX B - Communication

1. (U) Communication:

a. Primary: The primary means of communication between the PCO and the source(s) will be personal meetings at selected safe sites in the Pentagon building or in the surrounding area of Northern Virginia or the District of Columbia. Personal meetings will be held to the absolute minimum consistent with operational requirements. Details of future meetings will be established at each meeting or through telephonic communication initiated by either the PCO or source(s) to previously exchanged telephone numbers.

b. Emergency: To establish an unscheduled meeting on a priority basis, Source will call the PCO through an unlisted commercial number on the PCF/NCR FO call director. Source(s) will identify himself through a pre-arranged code name (cover name) and ask to speak to the PCO. If the PCO is not in available at the time of the call, the message will be transmitted to the PCO by PCF personnel as soon as possible. The PCO, to establish an unscheduled meeting with source(s), will contact source(s) by a pre-established telephone number in conformance with source(s) work schedule or off duty habits.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

435

Page 1934 of 3957

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

5 USC 552 (b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 436

IAGPA-CSF Form 6-R
1 Sep 93

ANNEX D - Termination

1. (U) (C) Termination of the operation: Termination will be accomplished based upon an objective evaluation of the effectiveness of continued utilization of source towards the accomplishment of the goals of this operation, with the final decision to terminate resting with OACSI, Department of the Army.

2. (U) (C) Termination of source(s) with prejudice: In the event source(s) violate basic security practices and are terminated for that reason, they will be prosecuted for violation of the appropriate statute or directive, should such an action be deemed feasible and advisable in connection with the nature of the violation and their activities in support of the operation. Should prosecution be inadvisable, source(s) will be required to execute a debriefing statement, and detailed instructions will be given regarding the possible consequences should they reveal their MI affiliations and activities.

3. (U) (C) Termination of source(s) without prejudice: Upon termination of this operation or at such time as source(s) are considered to be of no further value within the scope of this plan, and provided source(s) have committed no flagrant violations of security, they will be paid all outstanding reimbursable expenses incurred. A detailed security briefing concerning disclosure of information concerning their MI affiliations and activities will also be administered. If deemed advisable at the time of termination, source(s) may be presented a properly sanitized letter of commendation/appreciation or other appropriate recognition for their cooperation.

4. (U) (C) Commitments: No commitments other than those relating to reimbursement of legitimate operation expenses incurred during the course of the operation will be made. Source(s) will be given assurance of personal safety and protection of careers and reputations.

5. (U) (C) Knowledgeability: Source(s), during the course of the operation will be knowledgeable of the following:

a. PCO: by name and status as Special Agent, US Army Intelligence.

b. Facilities: Source(s) will not be routinely exposed to facilities housing PCF during the course of their covert activities. However, the existence of PCF is common knowledge throughout the Pentagon, and the likelihood that source(s) will, at a minimum, know the location of PCF is unavoidable.

c. Modus Operandi: Source(s) will be exposed to modus operandi only in direct relation to the requirement levied by the PCO.

d. Location of meeting sites.

e. Means of alternate and emergency contact with PCO: Post Office

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Box numbers and locations and telephone numbers where PCO can be reached in an emergency.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

438

ANNEX E - Security Considerations

1. (U) ~~(C)~~ The activities engaged in by individuals assigned to OACSI which may be considered to be disruptive of military operations, contrary to good order and discipline, and posing a threat to military security are unknown at this time. The number of military personnel engaged in activities relative to active and/or passive resistance to the military is also unknown.

a. The inter-relationship of military and civilian community in the National Capital area is such that it can be expected to present a degree of security risk in that confidential source(s) covert activities could be revealed through indiscretions on the part of source(s) in deviating from normal routine of activities normally associated with the work environment. This risk will be substantially limited by extensive training of source(s) in the areas of personal security and operational security. Further, close monitoring of all activities of source(s) for the purpose of determining the presence of or lack of derogatory security indicators will preclude unexpected security developments and will provide a means by which source(s) may be further trained, guided, and controlled in their activities.

b. Project Control Officer/Confidential Source relationship could be revealed inadvertently by the passive element of the military establishment, thus posing a threat to the security of the operation. This possibility will be reduced by close adherence to fundamentals of security in the conduct of personal meetings, telephone calls, and all other contacts between PCO and source(s).

2. (U) ~~(C)~~ In the event that either source(s) or this operation are compromised, USAINTA will not confirm the existence of such an operation, the employment of source(s), or interest in organizations/personalities involved in alleged subversive activities. Should source(s) be compromised PCO will immediately instruct source(s) to cease all operations; activity, and will debrief in detail concerning all aspects of the possible compromise. Based upon an evaluation of the situation, source(s) may be terminated and the operation may be suspended pending an analysis of the compromise and its ramifications. All sources so terminated will be administered the appropriate security debriefing.

3. (U) ~~(C)~~ Security measures must assure:

a. Strict need-to-know restructions concerning the existence of this operation and the methods by which it is implemented will be applied. A PCF Knowledgeability list will be maintained. (See ANNEX F)

b. Briefings on the existence of this operation will be given only to the ACSI or his designated representative.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

439

ANNEX F - Knowledgeability List (U)

1.	LTC Byron W. Hunt	Commander, PCF
2.	MAJ Kenneth G. Hetzel	Operations Officer, PCF
3.	MSG Daniel W. Leber Jr	Operations NCOIC, PCF
4.	CPT Kenneth R. Schlag	PCF
5.	CW2 Shawn M. Sandlin	PCF
6.	CW2 Leonard NMN Gross	PCF
7.	SFC George E. Perry	PCF

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

REGRADED UNCLASSIFIED
ON 5 SEP 97
BY CDR USAINSCOM FOIPO
AUTH PARA 1-603 DoD 5200.1R

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

Retention of Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH
SUSPENSE:
DATE: 3 July 1975

ACTION REQUIRED
To respond to a request from the Commander, APG for continuation of ICIP.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) BACKGROUND: During the last quarter, calendar year 1974, the ACSI conducted a review of the ICIP, and based on the results of this review, he directed the termination of 12 of the 19 on-going operations. The operations terminated were those which were less productive or conducted at installations of lesser sensitivity. Among the operations terminated was GONDOLA STAR which had been conducted in the Aberdeen Proving Ground (APG)/Edgewood Arsenal (EA) area. At RED TAB B is a recommendation from the Commander, APG indorsed by the Commander, Test and Evaluation Command (TECOM) and the Commander, Army Materiel Command, that the ICIP be continued at APG/EA.

2. (U) DISCUSSION:

a. The APG request advises that they recognize information developed in GONDOLA STAR has been of limited CI value in the past, however, they consider even negative reporting to be significant. The TECOM indorsement emphasizes the probable significant increase in travel during the Bicentennial period and the proximity of APG/EA to New York and Washington would make those facilities more vulnerable to hostile intelligence agencies.

b. The ACSI reexamined the operation and advised that he would consider continuing the operation for a six-month trial period to determine if any more significant information can be developed to indicate a hostile threat to APG/EA. On 2 July 1975, the Deputy Under Secretary of the Army indorsed this proposal.

c. Letter at RED TAB A advises the Commander, APG of the ACSI's decision to continue the operation for another six months and then reassess its progress.

3. (U) RECOMMENDATION: That letter at RED TAB A be approved and signed.

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DECEMBER 2005

(Continue on plain bond)

IMPLICATIONS — CINFO: YES ☐ NO ☐ — PRIM PROGS: YES ☐ NO ☐ — SUBJECT: YES ☐ NO ☐

COORDINATIONS

OFFICE	NAME	PHONE		INITIALS	DATE
			DR		
			DIV		3 Jul 75
			DIR	MC	
			EX		3 Jul 75
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED

ACTION OFFICER *(Name, grade, phone and signature)*
R. EBERSOLE, MAJ/56074/jl R Ebersole 441

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

DAMI-DOH

11 JUL 1975

SUBJECT: Retention of Internal Counterintelligence Program (ICIP) (U)

THRU: Commander
US Army Materiel Command
5001 Eisenhower Avenue
Alexandria, Virginia 22333

Commander
US Army Test and Evaluation Command
Aberdeen Proving Ground, Maryland 21005

TO: Commander
Aberdeen Proving Ground
Maryland 21005

1. (U) Reference letter, STEAP-IN, subject as above, 17 April 1975, with indorsements.

2. (U) During the past several years, the ICIP effort has grown rapidly. Unfortunately, sufficient resources to conduct these operations have not always been available. In order to make optimum use of these scarce, highly trained resources, it became necessary to conduct a total review of the program and make adjustments. This review revealed that GONDOLA STAR was a marginal operation and I directed its termination.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 2005

~~WARNING NOTICE-SENSITIVE INTELLIGENCE~~
~~SOURCES AND METHODS INVOLVED~~

4 of 2

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

11 JUL 1975

DAMI-DOH
SUBJECT: Retention of Internal Counterintelligence Program (ICIP) (U)

3. (U) In light of your request that this operation be continued, and considering the fact that the Commander, USAINTA has advised me that new sources with improved access have been recruited, I will revalidate GONDOLA STAR for a six-month period. In January 1976, I will assess the progress of this operation and will then determine if we will be able to continue this effort.

(sgd) Harold R. Aaron

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

443

~~CONFIDENTIAL~~

Page 1942 of 3957

~~CONFIDENTIAL~~

AMCSS (17 Apr 75) 2d Ind (U)
SUBJECT: Retention of Internal Counterintelligence Program (ICIP) (U)
29 April 1975

HQ, US Army Materiel Command, 5001 Eisenhower Avenue, Alexandria, VA 22333
29 April 1975

TO: HQDA (DAMI) WASH DC 20310

Forwarded for your consideration. This headquarters supports the requests and recommends favorable consideration be given to the continuation of the program.

FOR THE COMMANDER:

ROBERT L. KIRWAN
Brigadier General, USA
Chief of Staff

WARNING NOTICE
SENSITIVE INTELLIGENCE
SOURCES AND METHODS INVOLVED

~~CONFIDENTIAL~~ 444

REGRADED UNCLASSIFIED WHEN SEPARATED
FROM Basic Trng Instr Pkt

Page 1943 of 3957

AMCSS

~~CONFIDENTIAL~~

(U)
AMSTE-SE (17 Apr 75) 1st Ind ~~(C)~~
SUBJECT: Retention of Internal Counterintelligence Program (ICIP)(U)

Headquarters, U. S. Army Test and Evaluation Command, Aberdeen Proving Ground, Maryland 21005 25 APR 1975

TO: Commander, U. S. Army Materiel Command, ATTN: AMCSS, 5001 Eisenhower Avenue, Alexandria, Virginia 22333

1. (U) I recommend that GONDOLA STAR be continued as an active counterintelligence operation in the Aberdeen Proving Ground area.

(U)
2. ~~(C)~~ The conditions set forth by the Commander of Aberdeen Proving Ground I feel support this continued operation. The recently revised ACSI EEI reveals that the weapons, tanks, and chemical defense RDT&E conducted in the Aberdeen Proving Ground area, to include Edgewood Arsenal, are of interest to Communist Bloc intelligence agents. With the advent of the Bicentennial year, Aberdeen Proving Ground will be open to significantly more tourists visits commencing on 14 June and extending throughout the Bicentennial period. During that year, the closeness of Aberdeen Proving Ground and Edgewood Arsenal to the New York City and Washington, DC areas make it vulnerable to hostile intelligence gathering agencies and their desire to exploit the situation to secure EEI. I conclude that security of USAAPG will be vulnerable and that ICIP will be of greater importance than ever during this coming period. I intend to maintain all normal internal security measures and ICIP support on a continuing basis would be a valuable supplement to these measures.

REGRADED UNCLASSIFIED
ON [illegible] -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Charles P. Brown
CHARLES P. BROWN
Major General, USA
Commanding

WARNING NOTICE
SENSITIVE INTELLIGENCE
SOURCES AND METHODS
INVOLVED

Classified by Cdr, USAINTA
Exempt from General Declassification
Schedule of EO 11652
Exemption Category 2
Declassify on 31 Dec 2005

445

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
U S ARMY ABERDEEN PROVING GROUND
ABERDEEN PROVING GROUND, MARYLAND 21005

STEAP-IN

APR 1 1975

SUBJECT: Retention of Internal Counterintelligence Program (ICIP) (U)

Commander
US Army Test and Evaluation Command

(U)

1. (U) This headquarters has been advised by your Security Officer at a meeting held on 9 April 1975 that the Internal Counterintelligence Program for Aberdeen Proving Ground, Operation GONDOLA STAR (U), is scheduled for termination. It is understood that the AMC Security Officer desires a review of the impact of such an action upon this installation.

(U)

2. (U) It is recognized that specific information of counterintelligence value developed by Operation GONDOLA STAR has been somewhat limited in the past; however, it must be acknowledged that even negative reports are significant provided that effective coverage of critical target areas has been maintained. In some cases, reports received from ICIP sources have served as useful early warnings of developing situations on which corrective action could be promptly initiated. If this operation is terminated, the sensitivity and espionage potential of this installation would remain whereas one tool for building a strong security posture would be removed.

(U)

3. (U) The importance of Aberdeen Proving Ground as an espionage target is obvious. Research and testing programs generate information of worldwide intelligence interest, and scientific personnel have frequent contacts with foreign nationals. The diversified missions of several tenant activities include projects which have been reported to have high priority among Soviet intelligence collectors. Therefore, ICIP support would be a useful supplement to our normal internal security measures.

(U)

4. (U) It is recommended that GONDOLA STAR be continued as an active counterintelligence operation and strengthened with such resources as may be feasible.

ALVIN D. UNGERLEIDER
Colonel, Armor
Commanding

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

WARNING NOTICE
SENSITIVE INTELLIGENCE
SOURCES AND METHODS INVOLVED

Classified by Cmdr, USAINTA
Exempt from General Declassification
Schedule of EO 11652
Exemption Category 2
Declassify on 31 Dec 2005.

#46

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 14 May 1975

ACTION REQUIRED: To obtain approval of the quarterly ICIP report.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) BACKGROUND:

a. By memorandum dated 8 February 1972 (BLUE TAB B), the Under Secretary of the Army requested that the VCSA, US Army, provide a quarterly report on all ICIP operations.

b. A report covering the fourth quarter, calendar year 1974 submitted in February 1975 reflected the results of a review conducted by the ACSI. Of the 19 ongoing operations, 12 were identified for termination.

2. (U) DISCUSSION:

a. During the past quarter, 11 operations were terminated. This leaves one operation pending termination. One new operation was approved by the ACSI on 4 March 1975. This operation, CANTER RIDE (U) at the US Army Missile Command, Redstone Arsenal, AL, raises the number of active ICIPs to eight at the close of the quarter.

b. Memorandum at BLUE TAB A provides information required by the USofA.

3. (U) RECOMMENDATION: That memorandum at BLUE TAB A be approved and signed.

Classified by DAMI-ZA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2005

(Continue on plain bond)

IMPLICATIONS — CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		15 May 75
			DIV		15 MAY 75
			DIR		16 May 75
			EX		
			ACSI		
			DISPATCHED (DTG)		

~~REGRADED UNCLASSIFIED ON SEP 5 1997 BY USAINSCOM FOIPA Auth Para 4-102 DOD 5200.1R~~

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

MAJ EBERSOLE/56074 K. Ebersole 447

ACSI FORM 28, 13 Sep 71

~~REGRADED CONFIDENTIAL~~ WHEN SEPARATED FROM CLASSIFIED DOCUMENT

DUSA

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

DAMI-DOH

27 MAY 1975

MEMORANDUM THRU: VICE CHIEF OF STAFF, UNITED ~~STATES ARMY~~ WTK 28 MAY 1975

FOR: ~~UNDER SECRETARY OF THE ARMY~~ NOTED - USA

SUBJECT: Internal Counterintelligence Program (ICIP) (U)--INFORMATION MEMORANDUM

1. (U) During the past quarter, action was initiated to terminate 12 ICIP operations that were considered to be relatively unproductive or located at less sensitive installations. Eleven operations have been terminated and the twelfth will be terminated in the near future.

2. (U) A new operation, CANTER RIDE, was initiated at the US Army Missile Command, Redstone Arsenal, AL, raising the total number of active operations to eight.

3. (U) Three of the ongoing operations continue to provide information which serves to enhance security at the facilities concerned. LENTIL MONKEY, at the Defense Language Institute, continues to be the most active operation, surfacing security weaknesses involving both instructor and student personnel at that facility.

4. (U) Status reports for each operation are inclosed.

8 Incl
as (~~CONFIDENTIAL~~)

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by DAMI-ZA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 2005

448 MAJ Ebersole/74087/19 May 75
Typed by J. Lukasik

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE UNDER SECRETARY

10 Jun 75

MG Harold R. Aaron
ACofS for Intelligence
Rm 2E464
Pentagon

Noted and returned.

R.P.S.

DO
Hatch
USAINTA

449

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

17 APR 1975

MIIA-SO

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOI-C)
WASH DC 20310

1. (U) ~~(C)~~ Internal Counterintelligence Program (ICIP) operations during the third quarter of FY 1975 were characterized by a large scale slow-down of activity in all operations as those operations selected for termination early in the quarter were phased out. By 31 March 1975, 11 ICIPS, with supporting confidential sources, were terminated and one additional ICIP is scheduled for termination.

2. (U) ~~(C)~~ Upon completion of the termination actions described above, seven ICIPS remained active. One new ICIP operation providing for insert of an agent in a covert status in the US Army Missile Command (USAMICOM), Redstone Arsenal, AL, was approved on 4 March 1975. The USAMICOM operation, which has the nickname CANTER RIDE (U) raises the total of active ICIPS to eight at the close of the quarter.

3. (U) Brief status reports for each ICIP operation reported upon, including both those terminated and those continued, are attached as inclosures.

FOR THE COMMANDER:

Albert N Weidhas

20 Incl
as

ALBERT N. WEIDHAS
Colonel, MI
Director of Operations

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by Cdr USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF E.O. 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 2000

450

~~CONFIDENTIAL~~

1. (U) CANARY EFFORT: (OACSI Approval - 16 Feb 72)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three sources were used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Information surfaced pertaining to the use of drugs and moral improprieties on the part of a civilian employee assigned to the Office of the Comptroller prompted a suitability investigation of the employee. The employee's access to classified information has been suspended. Adverse suitability information consisting of drug abuse, indebtedness, moral misconduct and mental instability on the part of six military policemen assigned at the Alternate Joint Command Center and Fort Ritchie was provided the Provost Marshal and the Director of Security, US Army Communications Command (USACC). Investigations of the allegations are being made. Information reported on an Army NCO assigned to the Engineering & Installation Office, USACC, alleging excessive gambling and unexplained affluence is being checked prior to requesting that a limited investigation be conducted.

e. Operational Status: On 18 Mar 75, the PIO briefed COL Donald E. Clark, interim Director, Telecommunications, on the ICIP. COL Clark is scheduled to become Commander, USACC Operations Command, after the reorganization of USACC on 1 Jul 75. On 20 March 1975, the PIO presented the Quarterly Briefing to COL Harold G. deMoya, Commander, Fort Ritchie, and COL John J. Plosay, Jr., Deputy Commander, Fort Ritchie. COL deMoya expressed his appreciation for the support provided by the ICIP at Fort Ritchie.

REGRADED UNCLASSIFIED
ON SEP 3 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1950 of 3957

2. (U) CANINE PLATE: (OACSI Approval - 18 Sep 73)

a. Location: Seneca Army Depot (SAD), Romulus, NY.

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: On 13 Jan 75, COL Alan A. Nord assumed command of Seneca Army Depot. The Commander, 902d MI Group, had scheduled a briefing on the ICIP CANINE PLATE for COL Nord in mid-March 1975. That briefing was cancelled and is now scheduled for the following quarter. Operational progress has been stalemated during this reporting period pending the briefing of the new Depot Commander. Subsequent to that briefing, it is anticipated that development of the operation can be accelerated.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

3. (C) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal (RSA), AL.

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: During the past year several significant security weaknesses surfaced at USAMICOM, prompting the USAMICOM Chief of Staff to request an ICIP operation at that facility. These weaknesses included mishandling and loss of classified documents and allegations concerning suitability of some employees. Considering the sensitivity of the facility and the evident security weaknesses, a degree of urgency in initiating this operation was apparent. Unlike previous ICIP operations, the planning for this operation envisioned the use of a trained military intelligence warrant officer, a "Great Skill" officer, as the principal confidential source in order to expedite the initiation of this operation. The source has been selected for insertion in the target area (the US Army Missile Research, Development and Engineering Laboratory (USAMRDEL)), and has been provided administrative and operational training to enable him to function in his cover capacity as an administrative officer. The source will be assigned in the target area in April 1975. On 14 March 1975, the Commander, Redstone Resident Office, 902d MI Group, briefed COL R. A. Axelson, Director, USAMRDEL, informing him that the requested counterintelligence special support had been approved on 4 Mar 75 and it was proposed to insert an agent by mid-April 1975.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

4. CANVAS TAX: (OACSI Approval - 8 Mar 74)

a. Location: Sierra Army Depot (SIAD), Herlong, CA.

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: A new Project Liaison Officer (PLO) was assigned to this operation and arrived on station in January 1975. The PLO will perform the functions of both the PLO and the Project Case Officer (PCO). The PLO has been engaged in familiarization and orientation with SIAD and will perform spotting and assessment of potential sources in the coming weeks. On 20 March 1975, the Quarterly Briefing was presented by the PLO to the supported command. Those in attendance at the briefing were COL Robert Hawlk, CDR, SIAD; LTC Bernard Render, Dep CDR, SIAD; and MAJ John Jolley, Security Officer, SIAD.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

45

~~CONFIDENTIAL~~

5. (2) ~~(C)~~ CENSUS TIME: (OACSI Approval - 5 Feb 74)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC.

b. Confidential Source Utilization: One source was used during the reporting period.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: This operation is conducted by representatives of the Pentagon Counterintelligence Force (PCF). Early in the quarter, it was necessary to divert virtually the entire strength of PCF from their normal functions to a files screening project at the Counterintelligence Analysis Detachment and the Special Security Group. Both the PLO and PCO were assigned to the files screening project and were able to devote only a limited amount of time to this ICIP operation. This precluded any significant expansion or development of the ICIP. The supported command requested that an attempt be made to obtain information on several persons assigned to PTC suspected of drug abuse. Sources have failed to surface any concrete information to date in this connection. On 1 April 1975, the PLO presented the Quarterly Briefing to COL Joseph T. Adinaro, Commander, PTC.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 1954 of 3957

6. (U) CENTAVO KID: (OACSI Approval - 18 Oct 73)

a. Location: Harry Diamond Laboratories (HDL), Washington, DC.

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: Investigation of allegations of misconduct on the part of a DAC employee of HDL while the employee was on TDY were inconclusive, but the HDL Security Officer and the employee's supervisor are continuing to monitor the employee's activities. The PLO called the attention of the HDL Security Officer to several minor security problems during the period which were corrected on the spot.

e. Operational Status: During the period approximately 400 HDL personnel were moved from the HDL offices at Connecticut and Van Ness Avenues, NW, Wash, DC, to HDL facilities in White Oak, MD. The move is part of a reorganization and centralization of US Army electronics research facilities into one organization which will be named the Harry Diamond Developmental Center. On 5 March 1975, the PLO presented the Quarterly Briefing to COL D. W. Einsel, Jr., Commander, HDL, and Mr. James F. Yeick, Security Officer, HDL.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 1955 of 3957

7. (U) ~~(C)~~ IENS HOLDER: (OACSI Approval - 7 Aug 74)

a. Location: White Sands Missile Range (WSMR), NM

b. Confidential Source Utilization: None.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None

e. Operational Status: The Project Liaison Officer (PLO) for this operation will also perform the Project Case Officer (PCO) function when Source assets are obtained. One prospective source has been identified in the Missile Electronic Warfare Technical Area (MEWTA), and recruitment is planned for the next quarter. On 18 March 1975, the PLO presented the Quarterly Briefing to Mr. William F. Arquette, Chief, Intelligence Div, WSMR. Mr. Arquette, speaking for the Commander, WSMR, expressed satisfaction with the progress of the ICIP to date.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

Page 1956 of 3957

~~CONFIDENTIAL~~

8. (C) LENTIL MONKEY: (OACSI Approval - 26 Oct 71)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Five confidential sources were utilized during the quarter.

c. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) An instructor in the Chinese-Mandarin Language Dept may have had contact with personnel of the Peoples Republic of China during a business conference in Jan 75. The instructor, who has several commercial enterprises, allegedly attended a conference in Dallas, Texas, where the Chinese were present. An effort is being made to obtain further details.

(2) Sources of the operation provided information which established the existence of contacts between an instructor of the Arabic Language Dept and officials of the Palestinian Liberation Organization. The instructor, who is a US citizen, allegedly utilizes a Lebanese passport when he travels in the Middle East. Summaries of Information containing details have been passed to the FBI and the Immigration and Naturalization Service.

(3) Sources in the project surfaced a series of reports on a USAF student, who, through his Czech language instructor, has socialized with citizens of Czechoslovakia. By USAF regulations, the NCO was to have reported promptly any contact with citizens of a Communist Bloc country. The NCO failed to make the necessary report. The information was passed to the OSI by Summaries of Information and the OSI is now conducting an investigation of the USAF student.

(4) Suitability information concerning DLI students was passed to the Security Officer, DLI.

e. Operational Status: Of the five confidential sources used in the operation, two were terminated during the period due to their graduation. The remaining three provide coverage in the Russian, Czech, and Serbo-Croatian Language Department. Prospective confidential sources are being assessed in the Russian, Czech, Polish, and Chinese-Mandarin Departments. In addition to the confidential sources, 21 conventional sources are providing coverage in ten language departments. All sources are concentrated in the Priority I language departments. The PLO provided the Quarterly Briefing on 21 March 1975 in the Office of the Director, DLI. Those

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON 13 MAR 1998
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

attending the briefing were COL James R. Koenig, Director, DLI; COL Avery Kay, Deputy Director, DLI; and MAJ Richard Erickson, Security Officer, DLI. COL Koenig stated that he believed the information gained from the ICIP had been particularly helpful and had been largely responsible for several command letters published by DLI in an effort to improve internal security at DLI. The Director also stated that as a result of information provided by the ICIP, the teaching texts and materials of all DLI courses are being reviewed to eliminate politically contentious materials from the language courses.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

459

Page 1958 of 3957

ROUTING AND TRANSMITTAL SLIP		ACTION
TO Mr. Kelly	INITIALS DATE 14 May	CIRCULATE COORDINATION
BG Kelley	INITIALS DATE	FILE INFORMATION XXX
HQS. ONLY	INITIALS DATE	NOTE AND RETURN PER CONVERSATION
EYES SOLE	INITIALS DATE	SEE ME SIGNATURE

REMARKS

The attached is forwarded for your information. This is the result of a 902nd MI Group review of five key facilities in the Canal Zone to determine if the security posture at any of the facilities warranted initiation of ICIP operations. After reviewing the package, I concur with the USAINTA recommendation that ICIP operations are not appropriate.

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM	DATE
L. A. SPIRITO, COL, GS Chief, HUMINT Division 460	14 May 75 PHONE 56074

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41 CFR) 100-11.206

1034-75

GPO: 1973 O - 526-336 5041-101

SECRET

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

26 APR 1975

MIIA-SO

SUBJECT: Evaluation of Selected Installations in Panama Canal Zone (U)

HQDA (DAMI-DOI-C)
WASH DC 20310

1. (U) (C) During a 19 Feb 75 visit by the ACSI to the 902d MI Group, the 902d was tasked to explore the possibility of the need for an ICIP operation in the Panama Canal Zone. The 902d MI Group has conducted a review of five key installations/units for evidence of past and present HoIS threat indicators.

2. (U) (C) The five installations/units which were assessed are 470th MI Group (TAB A); 193d Infantry Brigade (TAB B); USASA Det, SOUTHCOM, and 408th ASA Det (TAB C); Armed Forces Courier Station - Panama (TAB D); J-2/3 Directorates' Warning and Operations Centers - SOUTHCOM (TAB E). A threat assessment common to all activities, units, or installations in the Canal Zone is attached as TAB F.

3. (U) (C) Commanders of the installations concerned in each instance have stated that current counterintelligence support is adequate to maintain a proper security posture and an ICIP operation is not warranted at this time. The Commander, 902d MI Group concurs in this position and recommends that an ICIP operation not be initiated at any of the five units assessed. USAINTA also concurs in this recommendation.

6 Incl
1-6. TABS A thru F

WILLIAM S. WOLF
Colonel, MI
Commanding

HASSEL L. PARKER
COLONEL, MI
DEPUTY COMMANDER

Regraded CONFIDENTIAL when separated from SECRET inclosure.

Classified by Cdr, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 2025

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

461

SECRET

~~CONFIDENTIAL~~

470th MILITARY INTELLIGENCE GROUP

1. (U) GENERAL: The 470th Military Intelligence Group (MIGP) is a subordinate unit of the 193d Infantry Brigade (Canal Zone). This unit consists of 67 military and 18 civilian personnel. There are 80 personnel assigned to the Group Headquarters, Fort Amador (FA), Canal Zone (CZ), on the Pacific side of the isthmus, and 5 stationed at the Atlantic Field Office, Building 214, Fort Gulick (FG), CZ, on the Atlantic side. Due to the importance and sensitivity of its mission, the 470th MIGP is considered a CRITICAL SENSITIVE activity.

2. (U) HISTORY: The 470th MIGP was born on 12 July 1944, as a Counter-intelligence Corps Detachment. It was first picked up on the Army's active duty roles on 31 July 1944, at the post of Quarry Heights, CZ. The 470th Intel Corps Detachment was redesignated and reorganized into an Intel Corps Group in September 1964, with a Security Service Detachment, the 508th MID in support of the 193d Infantry Brigade, the 610th MID, and the 471st MID in Puerto Rico. Two years later, in 1966, the unit was renamed the 470th MIGP, its present designation.

3. (U) MISSION: The mission of the 470th MIGP is to detect treason, sedition, and disaffection; to detect, prevent, and neutralize espionage, subversion, and sabotage directed against the United States Army, its personnel and installations; to conduct counterintelligence (CI) operations; and to collect intelligence through conduct of HUMINT operations.

4. (FOUO) SECURITY HISTORY/PRESENT SECURITY POSTURE: Building 47, FA, where the headquarters, 470th MIGP is located, is a two-story masonry structure used for administrative office space. The 470th MIGP has a photographic laboratory located on the first floor of Building 46, a motor pool located in Buildings 96 and T95, a Liaison Office located at Building 49, all at FA, and an Atlantic Field Office located at Building 214, Ft Gulick, CZ. A Counterintelligence Survey was conducted on the 470th MIGP on 12 December 1966, to establish basic security requirements. Subsequent CI inspections disclosed no major deviations from requirements established in the survey. Security Assistance Visits are utilized by the 470th MIGP in maintaining a good security posture. There have been no acts of espionage, sabotage or subversion detected in the unit.

5. (U) SECURITY SUPPORT ACTIVITIES: There are several US military and civilian activities in the CZ that render direct or indirect intelligence and CI support, external physical security support, security assistance, and police services to the 470th MIGP. These support activities augment the internal security procedures of the 470th MIGP and assist it in accomplishing its mission. The units or activities which provide direct or indirect support to the 470th MIGP are as follows:

CLASSIFIED BY CDR, 902d MI GP ltr 1 Nov 75
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY II
DECLASSIFY ON 3 Dec 2005

462

REGRADED UNCLASSIFIED
ON SEP -5 --
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

a. Canal Zone Field Office (CZFO), 902d MIGP, Fort Amador, CZ: Conducts Personnel Security Investigations (PSI) in the CZ. Provides CZ based surveillance and counter-surveillance support operations. Provides Security Assistance services in support of the 470th MIGP's mission. Conducts CI surveys, inspections, technical surveys and inspections, SAEDA lectures, penetration inspections, and CI related advice and assistance in support of the Group's security objectives.

b. United States Army Security Agency (USASA) Detachment-USSOUTHCOM, Fort Clayton (FC), CZ: Provides advice and assistance on capabilities and limitations of EW and SIGINT. Evaluates intelligence requirements in terms of USASA mission capabilities and maintains a continuous estimate of the local CRYPTOLOGICAL situation. Provides COMINT during contingency situations.

c. Naval Intelligence Service, FA, CZ: Provides information of intelligence and CI interest on local hostile activities and potential threats in functioning as a member of the Delimitation Committee.

d. Office of Special Investigations, US Air Force, Howard Air Force Base, CZ: Provides intelligence and CI information regarding hostile organizations and their activities as well as threat information of interest. Functions as a local member of the Delimitation Committee.

e. Provost Marshal Office, 193d Infantry Brigade, FC, CZ: Assists in preventing unauthorized vehicle and personnel entry in and adjacent to US Army installations and structures in the CZ. Provides additional security guard and personnel restrainment force when required. Conducts Physical Security Surveys and Inspections. Maintains criminal investigation files for review and use during the conduct of PSIs. Assists in preventing overt acts of sabotage by having mobile and foot Military Police patrols.

f. Criminal Investigations Detachment, Corozal, CZ: Provides information of intelligence interest uncovered during criminal investigations. Maintains files of all investigations conducted which are available for use during the conduct of PSIs or for intelligence purposes.

g. Internal Security Office, Canal Zone Government, Balboa Heights, CZ: Maintains files which are available for review during the conduct of PSIs or for intelligence purposes. Within the constraints of DA policies, provides information regarding intelligence matters of mutual benefit on US, Panamanian, Central and South Americans, as a local security agency.

h. Immigration and Naturalization Service (IN), District Court House, Ancon, CZ: Provides information regarding citizenship status on US naturalized citizens who are DOD-affiliated and of intelligence interest or the subjects of PSIs. Provides possible threat information of interest uncovered during normal IN functions.

6. (U) THREAT: See Tab F which is classified SECRET-NO FOREIGN DISSEMINATION.

Regraded UNCLASSIFIED on
3 Dec 09
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

Page 1962 of 3957

~~CONFIDENTIAL~~

7. (U) COMMANDER'S EVALUATION: The 470th MI GP advised that current CI support rendered by the CZFO, 902d MI GP is considered adequate in maintaining a good security posture. In the event a problem develops which falls within the purview of the Internal Counterintelligence Program or any other security support operation, a request for that service will be submitted.

8. (U) ~~(C)~~ CONCLUSIONS AND RECOMMENDATION: A detailed and minute search of the files of the Security Manager, 470th MI GP, as well as our own files, failed to disclose any history or current trend of bad security practices, disaffection, espionage, sabotage or subversion within the unit. Administrative security deficiencies found during the course of routine CI inspections had been corrected. The main threats, as pointed out in paragraph 6 above, are external rather than internal in nature and are targeted against by the entire intelligence community in the CZ. The commander clearly feels that current CI support rendered is adequate and has no desire for an ICIP operation at the present time. Based on the facts presented above, it is believed that an ICIP operation is presently neither warranted nor justified in the 470th MI GP. Recommend that an ICIP operation not be instituted in the 470th MI GP at this time.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

464

~~CONFIDENTIAL~~

Page 1963 of 3957

~~CONFIDENTIAL~~

193D INFANTRY BRIGADE (CANAL ZONE)

1. ~~(C)~~ GENERAL: Within the Headquarters, 193d Infantry Brigade (Canal Zone), Fort Amador (FA), Canal Zone (CZ), and its subordinate units or elements, only the Brigade Command Group (BCG), the Directorate of Intelligence (DINTEL), the Directorate of Operations, Plan and Training (DOPT), and the 470th Military Intelligence Group (MI GP), were considered as falling in the category of CRITICAL SENSITIVE. BCG, DINTEL and DOPT are all located at Building 1, FA, and will be dealt with in this Tab. The 470th MI GP is located at Building 47, FA, and is addressed separately in Tab A.

2. (U) HISTORY: On 1 July 1917, US Army personnel in the CZ were formed into a separate command and designated as the "Panama Canal Department". With the formation of a unified Caribbean Command in November 1947, the US Army element in the CZ was designated the US Army Caribbean Command with its Headquarters located at Quarry Heights (QH), CZ. In 1949, the Headquarters was moved to FA, its present location. On 6 June 1963, the US Army Caribbean Command was redesignated the US Army Forces Southern Command (USARSO), and remained so for 11 years. With the disestablishment of USARSO on 31 October 1974, the 193d Inf Bde assumed all command functions and was redesignated Headquarters, 193d Inf Bde (CZ).

3. (U) MISSIONS:

a. BCG: The BCG, under the direction of the Commanding General, US Army Forces Command, (FORSCOM), Atlanta, Georgia, commands all subordinate US Army units and activities in the CZ; maintains a combat-ready operational posture; provides support to the unified command as directed by CINCSO; and exercises operational control over USACC Agency-Panama.

b. DINTEL: The DINTEL, manages the collection, evaluation and processing of information into intelligence and the establishment of required intelligence, counterintelligence (CI) and security programs in support of the installation command's mission.

c. DOPT: The DOPT prepares, maintains and supervises the execution of policies and directives for the tactical security and defense of the Brigade's area. Plans, directs and coordinates for the Commander all CZ defense operations required of the Brigade including joint operations. Monitors and reports operational readiness. Formulates and coordinates estimates, plans, policies and functions pertaining to force structure, organization, equipment, and training of subordinate units. Supervises and coordinates reserve component matters within the Brigade. Advises on and supervises all Army Aviation matters. Supervises the activities of the Emergency Operations Center (EOC).

CDR, 902d MI GP on 1 Apr 95

CLASSIFICATION

4

DECLASSIFY ON: 31 Dec 2005

465

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

4. (U) ~~(C)~~ SECURITY HISTORY/PRESENT SECURITY POSTURE: Building 1, FA, where the BCG, DINTEL, and the DOPT are located, is a three-story masonry structure used for administrative office space. Counterintelligence (CI) surveys were conducted on Building 1 in July 1961, and during the months of August and September 1970. At that time, Building 1 housed USARSO'S Command Group, G-2, and G-3 offices, now the BCG, DINTEL, and DOPT respectively. Subsequent CI inspections have disclosed no major deviations from the security requirements established in the CI surveys. Additionally, Security Assistance Visits are presently being conducted on the activities as requested, with formal security inspections for CI purposes scheduled locally for the remainder of Fiscal Year 75. There have been no acts of espionage, sabotage or subversion detected in the BCG, DINTEL, or DOPT.

5. (U) ~~(C)~~ SECURITY SUPPORT ACTIVITIES: There are several US military and civilian activities in the CZ that render direct or indirect intelligence and CI support, external physical security support, security assistance, and police services to the 193d Infantry Brigade (Canal Zone). These support activities augment the internal security procedures of the Brigade and assist it in accomplishing its mission. The units or activities which provide direct or indirect support to the Brigade are as follows:

a. Canal Zone Field Office (CZFO), 902d MI GP, FA, CZ: Conducts Personnel Security Investigations (PSI) in the CZ. Provides CZ based surveillance and counter-surveillance support operations. Provides Security Assistance services in support of the Brigade's mission. Conducts CI surveys, inspections, technical surveys and inspections, SAEDA lectures, penetration inspections, and CI related advice and assistance in support of the Group's security objectives.

b. 470th Military Intelligence Group, FA, CZ: Provides intelligence operations and services to detect treason, sedition and disaffection and to detect, prevent and neutralize espionage, subversion and sabotage directed against the US Army, its personnel and installations in the CZ. Conducts CI operations and collects intelligence through conduct of HUMINT operations.

c. United States Army Security Agency (USASA) Detachment-USSOUTHCOM, Fort Clayton (FC), CZ: Provides advice and assistance on capabilities and limitations of EW and SIGINT. Evaluates intelligence requirements in terms of USASA mission capabilities and maintains a continuous estimate of the local CRYPTOLOGICAL situation. Provides COMINT during contingency situations.

d. Naval Intelligence Service, FA, CZ: Provides information of intelligence and CI interest on local hostile activities and potential threats.

e. Office of Special Investigations, US Air Force, Howard Air Force Base, CZ: Provides intelligence and CI information regarding hostile

4/66

REGRADED UNCLASSIFIED
ON 3 May 1998
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

organizations and their activities as well as threat information of interest.

f. (U) Provost Marshal Office, 193d Infantry Brigade, FC, CZ: Assists in preventing unauthorized vehicle and personnel entry in and adjacent to US Army installations and structures in the CZ. Provides additional security guard and personnel restrainment force when required. Conducts Physical Security Surveys and Inspections. Maintains criminal investigation files for review and use during the conduct of PSIs. Assists in preventing overt acts of sabotage by having mobile and foot Military Police patrols.

(U) g. (C) Criminal Investigations Detachment, Corozal, CZ: Provides information of intelligence interest uncovered during criminal investigations. Maintains files of all investigations conducted which are available for use during the conduct of PSIs or for intelligence purposes.

h. (U) Internal Security Office, Canal Zone Government, Balboa Heights, CZ: Maintains files which are available for review during the conduct of PSIs or for intelligence purposes. Within the constraints of DA policies, provides information regarding intelligence matters of mutual benefit on US, Panamanian, Central and South Americans as a local security agency.

i. (U) Immigration and Naturalization Service (IN), District Court House, Ancon, CZ: Provides information regarding citizenship status on US naturalized citizens who are DOD-affiliated and of intelligence interest or the subjects of PSIs. Provides possible threat information of interest uncovered during normal IN functions.

6. (U) THREAT: See Tab F which is classified SECRET-NO FOREIGN DISSEMINATION.

7. (U) COMMANDER'S EVALUATION: The 193d Infantry Brigade (Canal Zone) advised that the current support rendered by the CZFO, 902d MI GP, is considered adequate in maintaining a good security posture for the Brigade. Should a problem arise which falls within the purview of the Internal Counterintelligence Program, or any other security support operation, a request for that service will be initiated.

8. (U) ~~(C)~~ CONCLUSIONS AND RECOMMENDATION: To gather the information necessary to make a recommendation, a complete review of the files of the BCG, DINTEL, and DOPT was made. It was determined that there was no evidence of any security problems which could not be corrected by routine CI support. The review did not disclose any trends which might lead to weakening of the security posture. Based on information and facts already stated, and the feelings of the commander that his security posture is adequate, it is felt that at the present time, an ICIP operation is neither warranted nor justified. It is recommended that an ICIP operation not be instituted at this time.

Regraded UNCLASSIFIED on
3 Dec 01
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

467

~~CONFIDENTIAL~~

Page 1966 of 3957

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

US ARMY SECURITY AGENCY DETACHMENT SOUTHERN COMMAND

AND

408TH ARMY SECURITY AGENCY DETACHMENT

1. ~~(C)~~ GENERAL: The US Army Security Agency Detachment Southern Command (USASADSC), which includes the 408th ASA Detachment is a subordinate unit of the US Army Security Agency, Arlington Hall, Virginia, and is a tenant unit in support of the 193d Infantry Brigade (Canal Zone). USASADSC has its Headquarters in Building 220, Fort Clayton (FC), CZ. Due to the extreme sensitivity of its mission, the USASADSC is considered a CRITICAL SENSITIVE activity.

2. (U) HISTORY: Headquarters, US Army Security Agency Southern Command was established in the Canal Zone in June 1949. The headquarters was located in Building 220, FC, CZ, with an operational site located at Chiva Chiva, CZ. On 31 March 1971, it was redesignated USASADSC, and the site at Chiva Chiva was closed. All operational functions were consolidated in Building 220. With the redesignation, the 408th ASA Detachment was formed to enable the headquarters to assume its increased tactical role.

3. ~~(U)~~ MISSIONS:

a. USASADSC: The USASADSC operates as the senior USASA element in Latin America for command and control purposes. Conducts liaison between local forces and USASA elements in the CZ and higher USASA Headquarters. Operates and maintains a CRITICOMM terminal station, and coordinates and furnishes advice and assistance to US Military Forces in the CZ on capabilities and limitations of EW and SIGINT. Evaluates supported command intelligence requirements in terms of USASA mission capabilities, and maintains a continuous estimate of the cryptologic situation.

b. 408th ASA Det: The 408th ASA Det. provides a separate US Army Brigade with direct communications intelligence (COMINT) during contingency situations and issues intelligence information reports to SSO, Panama. Provides, within the limits of its capabilities, COMINT information to an ASA Battalion, Group, or Theater Headquarters in support of the national intelligence effort.

4. (FOUO) SECURITY HISTORY/PRESENT SECURITY POSTURE: The USASADSC and its subordinate unit, the 408th ASA Det, are administratively and operationally located in Building 220, FC, CZ. Counterintelligence Services support is primarily the responsibility of the Technical Services Activity (TSA), US Army Intelligence Agency (USAINTA), Fort Meade, Maryland. Locally, the Canal Zone Field Office, (CZFO), 902d Military Intelligence Group (MI GP) furnishes routine investigative support and emergency technical support. The last CI Inspection/Technical Service was conducted during December 1974 by TSA and disclosed no major security problems. A check of local files and those of USASADSC did not indicate any weakness in their security posture, or trends which could lead to security weaknesses. It was found that USASADSC continuously check and upgrade the

DECLASSIFIED ... E.O. 12958 ... DEC 2005

Page 1967 of 3957

~~CONFIDENTIA~~

integrity of their security program. There have been no acts of espionage, sabotage or subversion detected in the unit's history.

5. (C) SECURITY SUPPORT ACTIVITIES: There are several US military and civilian activities in the CZ that render direct or indirect intelligence and CI support, external physical security support, security assistance, and police services to the USASADSC. These support activities augment the internal security procedures of the Agency and assist it in accomplishing its mission. The units or activities which provide direct or indirect support to the Agency are as follows:

a. (U) CZFO, 902d MI GP, Fort Amador (FA), CZ: Conducts Personnel Security Investigations (PSI) in the CZ. Provides CZ based surveillance and counter-surveillance support operations. Provides Security Assistance services in support of the USASAD's mission. Conducts CI surveys, inspections, technical surveys and inspections, SAEDA lectures, penetration inspections, and CI related advice and assistance in support of the Agency's security objectives.

b. (U) 470th Military Intelligence Group, FA, CZ: Provides intelligence operations and services to detect treason, sedition and disaffection and to detect, prevent and neutralize espionage, subversion and sabotage directed against the US Army, its personnel and installations in the CZ. Conducts CI operations and collects intelligence through conduct of HUMINT operations.

c. (U) Naval Intelligence Service, FA, CZ: Provides information of intelligence and CI interest on local hostile activities and potential threats.

d. (U) Office of Special Investigations, US Air Force, Howard Air Force Base, CZ: Provides intelligence and CI information regarding hostile organizations and their activities as well as threat information of interest.

e. (U) Provost Marshal Office, 193d Infantry Brigade, FC, CZ: Assists in preventing unauthorized vehicle and personnel entry in and adjacent to US Army installations and structures in the CZ. Provides additional security guard and personnel restrainment force when required. Conducts Physical Security Surveys and Inspections. Maintains criminal investigation files for review and use during the conduct of PSIs. Assists in preventing overt acts of sabotage by having mobile and foot Military Police patrols.

(U) f. (C) Criminal Investigations Detachment, Corozal, CZ: Provides information of intelligence interest uncovered during criminal investigations. Maintains files of all investigations conducted which are available for use during the conduct of PSIs or for intelligence purposes.

h. (U) Internal Security Office, Canal Zone Government, Balboa Heights, CZ: Maintains files which are available for review during the conduct of PSIs or for intelligence purposes. Within the constraints of DA policies, provides information regarding intelligence matters of mutual benefit on US, Panamanian, Central and South Americans as a local security agency.

Regraded UNCLASSIFIED on
3 Dec 07
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

~~CONFIDENTIAL~~

Page 1968 of 3957

h. Immigration and Naturalization Service (IN), District Court House, Ancon, CZ: Provides information regarding citizenship status on US naturalized citizens who are DOD-affiliated and of intelligence interest or the subjects of PSIs. Provides possible threat information of interest uncovered during normal IN functions.

i. United States Army Security Agency, Arlington Hall Station, Arlington, VA: CI and technical security support is provided USASADSC by scheduled visits from its higher headquarters in Arlington, Virginia.

j. TSA, USAINTA, Fort Meade, Maryland: Provides technical and oounter-intelligence services to field activities of ASA by programming and scheduling inspections worldwide. Responding to field elements in semi-critical case, to insure proper security measures are being complied with, in order to maintain field elements in a high state of operational readiness.

6. (U) THREAT: See Tab F which is classified SECRET-NO FOREIGN DISSEMINATION.

7. (U) COMMANDER'S EVALUATION: The Commander, USASADSC, advised that the CI support received from TSA, the CZFO, 902d MI GP, and his own internal security personnel is considered adequate in maintaining a good security posture. In the event a problem develops which falls within the purview of the Internal Counterintelligence Program or any other security support operation, a request for assistance would be submitted through his Headquarters.

8. (U) CONCLUSIONS AND RECOMMENDATION: A detailed search of the security files of USASADSC, to include the 408th ASA Det, failed to disclose any weakness in their security posture or indicate a trend in that direction. Past CI services by TSA indicated some minor deficiencies, but those had been corrected shortly after the service was completed. Due to the extreme sensitivity of the unit, the Commander maintains a constant check of his unit's security program. This program is felt to be adequate. The main threats, as pointed out in paragraph 6 above, are external rather than internal in nature, and are targeted against by the entire intelligence community in the CZ. In evaluating the ICIP program, the Commander asked for guidance from his Headquarters in the US. The guidance he received agreed with his determination, that he had no desire for an ICIP operation at the present time. Based on the facts presented above, it is believed that an ICIP operation is presently neither warranted nor justified, and it is recommended that an ICIP operation not be instituted in the USASADSC at this time.

REGRADED UNCLASSIFIED
ON 3MAR 1998
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

Page 1969 of 3957

~~CONFIDENTIAL~~

UNITED STATES ARMY COURIER STATION - PANAMA

1. (U) GENERAL: The United States Army Courier Station - Panama (USACS-P) is a subordinate activity of the Office of the Adjutant General, Washington, D.C., with its office located at the Air Freight Terminal, Howard Air Force Base (HAFB), Canal Zone (CZ). This activity consists of only two individuals, one officer and one NCO. Because of the activity's continuous mission of handling extremely sensitive Departments of State and Defense documents and material, it falls in the CRITICAL SENSITIVE category.

2. (U) HISTORY: On 15 January 1966, the United States Army Courier Service was organized under the jurisdiction of the Office of the Adjutant General, Washington D.C. At that time, the United States Army Courier Transfer Station, United States Army Forces Southern Command (USARSO), Fort Amador, CZ, was disestablished and the USACS-P created and located at HAFB, where it has been to present.

3. (U) MISSION: The mission of the USACS-P is the secure and expedient transportation of material authorized protected handling by courier; to provide facilities for receiving, safeguarding, processing, delivering, and dispatching such material; to provide transportation facilities for TOP SECRET and CRYPTOGRAPHIC material to US Forces in the Panama Canal Zone, the Panama Canal Company, Federal Aviation Agency, Oceanographic Representative, U.S. Embassy - Panama, ships or units of the North Atlantic Treaty Organization, the Southeast Asia Treaty Organization, and the US State Department.

4. (U) SECURITY HISTORY/PRESENT SECURITY POSTURE: The Air Freight Terminal, HAFB, where USACS-P is located is a one-story concrete block office and warehouse structure used for the storage, maintenance and administration of in-transit freight and related material. USACS-P has a steel-feinforced concrete vault facility which meets the physical security requirements for storage of TOP SECRET material. An initial CI Survey was conducted on 28 April 1966, with recommended security requirements subsequently implemented. USACS-P's most recent CI inspection was conducted on 13 April 1973, with no major deviations from recommended requirements recorded. A search of the activity's files failed to reveal any history of security violations. There is no reason to believe USACS-P personnel have been involved in any security infractions. There are no reasons to believe the security objectives of USACS-P are not being met. USACS-P is scheduled for a routine CI inspection in 1975 by its parent organization, Headquarters, Armed Forces Courier Service (AFCS), Washington D.C., 20314.

5. (C) SECURITY SUPPORT ACTIVITIES: There are several US military and civilian activities in the CZ that render direct or indirect intelligence

CLASSIFIED BY CDR, 902d MIG on 1 Apr 75
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY II
DECLASSIFY ON 31 Dec 2005

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 1970 of 3957

~~CONFIDENTIAL~~

and CI support, external physical security support, security assistance, and police services to the USACS-P. These support activities augment the internal security procedures of the USACS-P and assist it in accomplishing its mission. The units or activities which provide direct or indirect support to the USACS-P are as follows:

a. (U) Canal Zone Field Office (CZFO), 902d MI GP, Fort Amador (FA), CZ: Conducts Personnel Security Investigations (PSI) in the CZ. Provides CZ based surveillance and counter-surveillance support operations. Provides Security Assistance services in support of the USACS-P mission. Conducts CI surveys, inspections, technical surveys and inspections, SAEDA lectures, penetration inspections, and CI related advice and assistance in support of the USACS-P security objectives.

b. (U) 470th Military Intelligence Group, FA, CZ: Provides intelligence operations and services to detect treason, sedition and disaffection and to detect, prevent and neutralize espionage, subversion and sabotage directed against the US Army, its personnel and installations in the CZ. Conducts CI operations and collects intelligence through conduct of HUMINT operations.

c. (U) United States Army Security Agency (USASA) Detachment-USSOUTHCOM, Fort Clayton (FC), CZ: Provides advice and assistance on capabilities and limitations of EW and SIGINT. Evaluates intelligence requirements in terms of USASA mission capabilities and maintains a continous estimate of the local CRYPTOLOGICAL situation. Provides COMINT during contingency situations.

d. (U) Naval Intelligence Service, FA, CZ: Provides information of intelligence and CI interest on local hostile activities and potential threats.

e. (U) Office of Special Investigations, US Air Force, Howard Air Force Base, CZ: Provides intelligence and CI information regarding hostile organizations and their activities as well as threat information of interest.

f. (U) Provost Marshal Office, 193d Infantry Brigade, FC, CZ: Assists in preventing unauthorized vehicle and personnel entry in and adjacent to US Army installations and structures in the CZ. Provides additional security guard and personnel restrainment force when required. Conducts Physical Security Surveys and Inspections. Maintains criminal investigations files for review and use during the conduct of PSIs. Assists in preventing overt acts of sabotage by having mobile and foot Military Police patrols.

g. (C) Criminal Investigations Detachment, Corozal, CZ: Provides information of intelligence interest uncovered during criminal investigations. Maintains files of all investigations conducted which are available for use during the conduct of PSIs or for intelligence purposes.

Regraded UNCLASSIFIED on
3 Dec 07
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

~~CONFIDENTIAL~~

Page 1971 of 3957

h. Internal Security Office, Canal Zone Government, Balboa Heights, CZ: Maintains files which are available for review during the conduct of PSIs or for intelligence purposes. Within the constraints of DA policies, provides information regarding intelligence matters of mutual benefit on US, Panamanian, Central and South Americans as a local security agency.

i. Immigration and Naturalization Service (IN), District Court House, Ancon, CZ: Provides information regarding citizenship status on US naturalized citizens who are DOD-affiliated and of intelligence interest or the subjects of PSIs. Provides possible threat information of interest uncovered during normal IN functions.

j. Headquarters, Armed Forces Courier Service, Washington, D.C.: Provides CI services and support in forms of surveys, inspections, and visits. Provides intelligence and security information and guidance through directives, regulations, and staff visits. Coordinates with local commands for additional CI and security support when required. Provides assistance in matters of security as a higher headquarters.

6. (U) THREAT: See Tab F which is classified SECRET-NO FOREIGN DISSEMINATION

7. (U) COMMANDER'S EVALUATION: The Commander,USACS-P, advised that USACS-P consists of only two persons and that the present counterintelligence services provided USACS-P are adequate and meets his security requirements. USACS-P does not desire additional CI support at this time.

8. (FOUO) CONCLUSIONS AND RECOMMENDATION: An examination of security and administrative files failed to disclose information that USACS-P's security posture was anything but sound and secure. In addition, security checks provided by Headquarters (HQ), AFCS, revealed that USACS-P was performing its mission, to include maintaining a good security posture, in an outstanding manner. An in-depth study of the local hostile threat and the mission of USACS-P conducted with the Commander, USACS-P, failed to indicate that an on-going or potential internal security threat exists. There are no reasons to believe that the normal CI support and service provided USACS-P by HQS, AFCS, in conjunction with local intelligence and security agencies, CZ, is not adequate coverage to identify and neutralize any CI threat to USACS-P. In view of the existing CI coverage of the USACS-P, and that there are only two persons assigned to it, additional CI support is not recommended for USACS-P at the present time.

REGRADED UNCLASSIFIED
ON 3MAR1998
BY USAINSCOM FOUPA
Auth Para 4-102 DOD 5200.1R

Page 1972 of 3957

~~CONFIDENTIAL~~

J-2/3 DIRECTORATES' WARNING AND OPERATIONS CENTER

1. (U) ~~(C)~~ GENERAL: The J-2/3 Directorates' Warning and Operations Center (J-2/3 DWOC) is a subordinate joint activity of the J-2 and J-3 Directorates, United States Southern Command (USSOUTHCOM), Quarry Heights (QH), Canal Zone (CZ). The J-2/3 DWOC is housed in Building 81, "The Tunnel", a building that is tunneled into a hillside in QH, and is a combined service activity manned by US Army, Navy, and Air Force personnel. Because of its communication capabilities and functions within USSOUTHCOM, and its support to the JCS, the J-2/3 DWOC is considered a CRITICAL SENSITIVE facility.

2. (U) HISTORY: Caribbean Command, a Unified Command under the JCS, had its genesis in the World War II Caribbean Defense Command which was organized in early 1942 and was composed of the Panama Canal and Puerto Rican Departments of the Army, the 10th and 15th Naval Districts of the Navy, the Trinidad Base Command, and the Panama Canal. The Caribbean Command was established at QH, CZ, on 1 November 1947, by authority of the JCS. The Component forces assigned to Caribbean Command consisted of the Army and Air Force elements of the Caribbean Defense Command and, with the exception of certain fleet facilities and bases, of the Navy's Caribbean Sea Frontier. On 6 June 1963, the Caribbean Command was redesignated USSOUTHCOM.

3. (U) ~~(FOUO)~~ MISSIONS:

a. J-2 Warning Center: The J-2 Warning Center supports the Director of Intelligence through the operation of the Warning Branch by preparing and disseminating current intelligence and warning indications and through the preparation of current and long range estimates, studies and assessments. Provides supervision and personnel for the J-2 element of the Battle Staff and the Emergency Relocation Site (ERS) when activated.

b. J-3 Operations Center: The J-3 Operations Center implements JCS emergency action procedures within USSOUTHCOM; prepares, coordinates, and disseminates USSOUTHCOM Emergency Action Procedures (EAP) in support of the JCS. In addition, prepares, coordinates, disseminates and implements USSOUTHCOM Control of Civil Disturbance Posture, USSOUTHCOM EAP, VOL III. Supervises the manning and operation of the emergency actions section of the Joint Operations Center and the ERS. Prepares, reviews, coordinates and supervises plans within the USSOUTHCOM command and control system to insure interface and capability with the Worldwide Military Command and Control Systems.

4. (U) ~~(FOUO)~~ SECURITY HISTORY/PRESENT SECURITY POSTURE: Building 81, the Tunnel, where the J-2/3 DWOC is located, is constructed of steel reinforced concrete embedded in sub-strata rock in Ancon Hill, QH, CZ, with

CLASSIFIED BY CDR, 90th MI GP on 1 Nov 75
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 11
DECLASSIFY ON 31 Dec 2005

474 REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

the building extending through the hill. The entrance to the tunnel is manned by armed guards and unauthorized access to it could result in exceptionally grave danger to the US. The J-2/3 DWOC is a highly sensitive operational activity and is the coordination nerve center of USSOUTHCOM. A CI Security Survey was conducted on the tunnel in 16 June 1961, to determine the security measures necessary to limit or deny unauthorized access to it. Subsequent CI inspections and Security Assistance Visits have been conducted to insure compliance with the procedures established in the Security Survey. There are no known on-going internal threats in the J-2/3 DWOC.

5. (U~~C~~) SECURITY SUPPORT ACTIVITIES: There are several US military and civilian activities in the CZ that render direct or indirect intelligence and CI support, external physical security support, security assistance, and police services to the J-2/3 DWOC. These support activities augment the internal security procedures of the J-2/3 DWOC and assist it in accomplishing its mission. The units or activities which provide direct or indirect support to the J-2/3 DWOC are as follows:

a. Canal Zone Field Office (CZFO), 902d MI GP, Fort Amador (FA), CZ: Conducts Personnel Security Investigations (PSI) in the CZ. Provides CZ based surveillance and counter-surveillance support operations. Provides Security Assistance services in support of the J-2/3 DWOC mission. Conducts CI surveys, inspections, technical surveys and inspections, SAEDA lectures, penetration inspections, and CI related advice and assistance in support of the Group's security objectives.

b. 470th Military Intelligence Group, FA, CZ: Provides intelligence operations and services to detect treason, sedition and disaffection and to detect, prevent and neutralize espionage, subversion and sabotage directed against the US Army, its personnel and installations in the CZ. Conducts CI operations and collects intelligence through conduct of HUMINT operations.

c. United States Army Security Agency (USAS) Detachment-USSOUTHCOM, Fort Clayton (FC), CZ: Provides advice and assistance on capabilities and limitations of EW and SIGINT. Evaluates intelligence requirements in terms of USASA mission capabilities and maintains a continuous estimate of the local CRYPTOLOGICAL situation. Provides COMINT during contingency situations.

d. Naval Intelligence Service, FA, CZ: Provides information of intelligence and CI interest on local hostile activities and potential threats.

e. Office of Special Investigations, US Air Force, Howard Air Force Base, CZ: Provides intelligence and CI information regarding hostile organizations and their activities as well as threat information of interest.

475

REGRADED UNCLASSIFIED
ON 3 MAR 1998
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

Page 1974 of 3957

~~CONFIDENTIAL~~

f. (U) Provost Marshal Office, 193d Infantry Brigade, FC, CZ: Assists in preventing unauthorized vehicle and personnel entry in and adjacent to US Army installations and structures in the CZ. Provides additional security guard and personnel restrainment force when required. Conduct Physical Security Surveys and Inspections. Maintains criminal investigation files for review and use during the conduct of PSIs. Assists in preventing overt acts of sabotage by having mobile and foot Military Police patrols.

(U) g. (C) Criminal Investigations Detachment, Corozal, CZ: Provides information of intelligence interest uncovered during criminal investigations. Maintains files of all investigations conducted which are available for use during the conduct of PSIs or for intelligence purposes.

h. (U) Internal Security Office, Canal Zone Government, Balboa Heights, CZ. Maintains files which are available for review during the conduct of PSIs or for intelligence purposes. Within the constraints of DA policies, provides information regarding intelligence matters of mutual benefit on US, Panamanian, Central and South Americans as a local security agency.

i. (U) Immigration and Naturalization Service (IN), District Court House, Ancon, CZ: Provides information regarding citizenship status on US naturalized citizens who are DOD-affiliated and of intelligence interest or the subjects of PSIs. Provides possible threat information of interest uncovered during normal IN functions.

6. (U) THREAT: See Tab F which is classified SECRET-NO FOREIGN DISSEMINATION.

7. (U) COMMANDER'S EVALUATION: The CINC, USSOUTHCOM, advised that CI support presently being received from the CZFO, 902d MI GP, together with the internal security programs and checks, are adequate in maintaining a good security posture. If at any future date, problems develop which would be considered within the purview of the Internal Counterintelligence Program or any other security support operation, a formal request for assistance would be submitted.

8. (U) ~~(C)~~ CONCLUSIONS AND RECOMMENDATION: After completing a review of the files concerning the J-2/3 DWOC security situation, it was determined that the security posture of the J-2/3 DWOC was adequate. No espionage, subversion or sabotage activities have been detected, and no trends seem to be developing which would lead to weakening the security posture. Taking into consideration the sensitivity of the area and the strict controls utilized by personnel of the activities, it is felt that the routine CI support now being given J-2/3 DWOC is adequate. Based on the information and facts stated, an ICIP operation in the DWOC at the present time is neither warranted nor justified. It is recommended that an ICIP operation not be instituted in the J-2/3 DWOC at this time.

Regraded UNCLASSIFIED on
3 Dec 07
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

476

~~CONFIDENTIAL~~

~~SECRET~~ NO FOREIGN DISSEM

THREAT

(S/NFD) THREAT: A current assessment of the threat to the Canal Zone (CZ) is as follows:

a. b1

b. b1

c. b1

d. b1

e. b1

f. The ever-present controversy over Canal negotiations provides a hostile threat from dissatisfied US employed local nationals. Their dissatisfaction might cause disaffection and subversion among US personnel sympathetic to the Panamanian cause.

CLASSIFIED BY COL 902d MIGP on 1 Nov 75
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 11
DECLASSIFY ON 31 Dec 2002

477

16

902-024-75

~~SECRET~~ NO FOREIGN DISSEM

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER	
OFFICE SYMBOL: DAMI-DOI-C	SUSPENSE:
DATE: 6 March 1975	

SUBJECT: CANTER RIDE (U)

ACTION REQUIRED: To inform the CDR, USAINTA subject OPLAN (ICIP) approved by ACSI, DA.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (W) BACKGROUND:

a. By letter dated 25 February 1975, subject as above (ORANGE TAB B), CDR, USAINTA (MIIA-SO), forwarded to DAMI-DOI-C for review and approval ~~of~~ 902d MI Group Operation Plan OP-001-75-902, subject: Internal Counterintelligence Program (ICIP)(U), (Project Canter Ride)(U).

b. By Memorandum Thru DAMI-DO for ACSI, DA, subject as above, dated 28 February 75 (ORANGE TAB C), DAMI-DOI recommended that the OPLAN be approved. On 4 March 1975, the ACSI, DA approved the OPLAN.

2. (U) DISCUSSION: By 1st Indorsement to USAINTA letter, DAMI-DOI advises the CDR, USAINTA that the ACSI, DA approved subject OPLAN on 4 March 1975.

3. (U) RECOMMENDATION: The attached 1st Indorsement to USAINTA (ORANGE TAB A) be approved and signed.

Classified by AR 381-102
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2005

(Continue on plain bond)

IMPLICATIONS — CINFO: YES ☐ NO ☐ | PRIM PROGS: YES ☐ NO ☐ | BUDGET: YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		7 MAR 75
			DIV		7 Mar 75
			DIR		7 Mar 75
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER (Name, grade, phone and signature)
M. BRANNAN/53501/bh

478

C/ Branch Record Copy

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

Page 1977 of 3957

~~CONFIDENTIAL~~

DAMI-DOI-C

MEMORANDUM THRU: BRIGADIER GENERAL KELLEY /3 Mar 75

FOR: MAJOR GENERAL AARON

SUBJECT: CANTER RIDE (U)

1. (C)

b1

2. (C) Most of the personnel assigned to ASD are scientifically oriented, and it is this scientific orientation that has been considered the primary cause for an uncooperative and lackadaisical attitude toward security. This attitude, coupled with prevailing unfavorable opinions of intelligence personnel in general, results in an environment not suitable to a conventional ICIP operation.

b1

3. (U)(C) A Sensitive Activity Vulnerability Estimate dated 5 February 1974, conducted at the US Army Missile Command, surfaced a number of security shortcomings. Other investigative efforts at this facility have revealed alleged questionable suitability activities on the part of some individuals assigned to ASD.

4. (U)(C) A review of the Sensitive Installation listing reveals that all activities at Redstone Arsenal (with the exception of the US Army Missile and Munitions Center and School) are considered "highly sensitive." A review of the Hostile Intelligence EEI maintained at CIAD revealed that information on missile technology continues to be a high priority Hostile Intelligence EEI.

Classified by DAMI-DO
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2005

479

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DAMI-DOI-C
SUBJECT: CANTER RIDE (U)

5. It is recommended that the attached OPlan be approved.

1 Incl
as (CONFIDENTIAL)

LEONARD A. SPIRITO
Colonel, GS
Chief, Counterintelligence
and Collection Division

Approved 14 MAY 75

Disapproved_____

See Me_____

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

480

~~CONFIDENTIAL~~

Page 1979 of 3957

~~CONFIDENTIAL~~

DAMI-DOI-C (25 Feb 75) 1st Ind
SUBJECT: CANTER RIDE

HQDA (DAMI-DOI-C), WASH DC 20310

TO: Commander, US Army Intelligence Agency, ATTN: MIIA-SC, Fort Meade, Maryland 20755

The attached OPLAN, subject as above, was approved by the ACSI on 4 March 1975.

FOR THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE:

2 Incl
nc

EUGENE KELLEY, JR.
Brigadier General, GS
Director of Intelligence Operations

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Upon removal of enclosures this document is Classified

~~CONFIDENTIAL~~

CONFIDENTIAL

DEPARTMENT OF THE ARMY
HEADQUARTERS
U.S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

25 FEB 1975

MIIA-SO

SUBJECT: CANTER RIDE (U)

HQDA (DAMI-DOI-C)
WASH DC 20310

1. (U) ~~(C)~~ Forwarded for your review and approval is 902d MI Group Operation Plan OP-001-75-902, subject: Internal Counterintelligence Program (ICIP) (U), (Project CANTER RIDE (U)) (TAB A).

2. (C) b1 This specialized counterintelligence support was requested by CG, USAMICOM, to enhance the security of the Directorate and determine the extent, if any, of hostile intelligence penetration of Redstone Arsenal. A feasibility study is at TAB B and provides additional detailed background information.

2 Incl
as

WILLIAM S. WOLF
Colonel, MI
Commanding

Classified by AR 380-380
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 2005

CONFIDENTIAL 482

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS, 902D MILITARY INTELLIGENCE GROUP
FORT MEADE, MARYLAND 20755

MIIA-GPB-AC(SP) O P E R A T I O N P L A N DATE:

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

REPORT NO: OP-001-75-902

PROJECT: CANTER RIDE (U)

(U) REFERENCES:

a. AR 380-13, Acquisition and Storage of Information Concerning Non-affiliated Persons and Organizations, 30 September 1974.

b. USAINTA Regulation 381-100-1, Counterintelligence Special Operations, 8 February 1974.

c. Memorandum, Redstone Resident Office, 902d MI Group, Subject: Request for Counterintelligence Special Operations, 23 September 1974.

d. LTR, AMSMI-X, Headquarters, US Army Missile Command (USAMICOM), Subject: Request for Special Counterintelligence Support, 30 September 1974.

e. Feasibility Study, MIIA-IA-O, Subject: CANTER RIDE Feasibility Study (U), 12 November 1974.

f. See Annex A (Doctrinal References for references relating to doctrine, modus operandi and operational restrictions.)

~~WARNING NOTICE: SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED~~

1. (C) MISSION:

a. Requirement: The 902d MI Group, with the assistance of the Composite Intelligence Activity (COMPIA), USAINTA, will develop and implement an Internal Counterintelligence Program (ICIP) operation [b1] The operation is designed to provide special counterintelligence support to the Commanding General, US Army Missile Command (USAMICOM), Redstone Arsenal (RA), Alabama, in response to reference d above. The 902d MI Group will be responsible for the planning, operational control and monitorship of the operation while COMPIA will provide for the [b1]

Classified by AR 380-102
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 2005

483

~~CONFIDENTIAL~~

OP-001-75-902
SUBJECT: Internal Counterintelligence Program (ICIP)

b1

Further information pertaining to the target is contained at Annex I (Target Information).

b. Objective:

(1) To enhance the security of the directorate by identifying those activities, practices and personnel employed within the target area which have been, and may continue to be, involved in the existent security weaknesses affecting the security of classified defense information within USAMRDEL. Further information pertaining to existent security weaknesses of the target area is contained at Annex J (Security Weaknesses).

(2) To determine the extent, if any, of Hostile Intelligence Service (HoIS) penetration of Redstone Arsenal. Any information pertaining to this subject developed by the operation will be expeditiously passed to the appropriate office of the US Army Intelligence Agency for possible exploitation under the provisions of AR 381-47.

c. Base of Operation: Redstone Arsenal, AL

d. Each individual and source involved in the conduct or control of the operation will be briefed on current policies and constraints pertaining to counterintelligence operations and activities as they concern persons and organizations not affiliated with the Department of Defense.

e. The scope of the operation will not be expanded to cover off-post targets not affiliated with the Department of Defense without prior approval IAW provisions of Appendix B, AR 381-13, dated 30 September 1974, Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations.

2. (C) PERSONNEL:

a. Agent Personnel: [See Annex B (Agent Personnel)]

b1

b. US Army MI Personnel: [See Annex C (Knowledgeability List)]

(1) Case Officer: A "Great Skills" member of the Military Intelligence Officer Excepted Career Program (MIOCP) utilized under the provisions of AR 614-115, dated 1 November 1974, is required.

(2) Alternate Case Officer: Commander, Redstone RO, 902d MI Group.

OP-001-75-902
SUBJECT: Internal Counterintelligence Program (ICIP)(U)

3. (C) COVER AND DOCUMENTATION: [See Annex D (Cover and Documentation)]

a. b1

b. b1

c. b1

4. (C) EXECUTION:

a. Itinerary:

(1) b1

(2) b1

b. b1

(1) b1

OP-001-75-902
SUBJECT: Internal Counterintelligence Program (ICIP)(U)

b1

(2)

b1

c. Security Considerations:

(1)

b1

(2)

b1

5. (U) ~~(C)~~ COMMUNICATIONS:

a. This OPlan provides for the use of personal meetings, US Postal Service and telephonic contacts to effect necessary communications. The communications system will be designed to assure a continuous and secure means for the transmission of information and will provide for a primary, alternate and emergency channel as follows:

OP-001-75-902
SUBJECT: Internal Counterintelligence Program (ICIP)(U)

(1) Primary: Used for normal requirements.

(2) Alternate: Used to prevent overloading of the primary system or in the event that the primary channel cannot be used.

(3) Emergency: Used only in such instances which require the urgent transmission of information when the primary or alternate systems will not suffice.

b. Details of the communications systems are contained in Annex E (Communications) to this OPlan.

6. (U)(C) TRAINING: The source will be trained jointly by the 902d MI Group and COMPIA in the skills necessary to accomplish his assigned tasks in a secure and effective manner. Source training will be continuous and will be dictated by the experience and background of the source and the operational situation within the target area. Specific minimal training requirements to include the provisions of AR 380-13 and standard Essential Elements of Information (EEI) are contained in Annex F (Training) to this OPlan.

7. (C) b1

8. (C) TERMINATION:

a. Termination with or without prejudice: The source recruited for this operation will be terminated when his usefulness to the operation ceases, he shows indications of insecure practices which could compromise the operation, he is no longer amenable to control, or the operation is terminated. Circumstances under which termination is effected will determine whether termination is with or without prejudice. The terms "with or without prejudice" do not indicate the manner in which the source will be terminated, but rather whether or not the source would be considered for use in future operations of this nature. Circumstances under which termination is effected are outlined in Annex H (Termination) to this OPlan.

b. Commitments: The only commitments to be made to the source will be assurance of personal security and reimbursement for expenses incurred at the direction of the C/O. At termination a severance statement will be obtained from the source in the appropriate format and will include a provision that the source has no further claim.

c. Knowledgeability: b1

Page 1986 of 3957

OP-001-75-902
SUBJECT: Internal Counterintelligence Program (ICIP)(U)

b1

b1

9. (U) ~~(C)~~ COORDINATION AND LIAISON:

a. Coordination between Headquarters, 902d MI Group; the Atlanta Field Office; Redstone Resident Office; COMPIA, USAINTA and appropriate personnel at RA has been established and will be maintained on a continuing basis.

b. Coordination and liaison between COMPIA and DA personnel assignments branches has been established to ensure the identification and procurement of a suitable agent for utilization in the operation.

c. Coordination with additional personnel at RA may be determined to be necessary in the accomplishment of the operation. Consideration is presently being made to the possible briefing of the Chief, COMPACT, RA, to ensure proper assignment of the agent. However, as the operation will be conducted under strict "close-hold" rules, the briefing of additional personnel at RA will be accomplished only when deemed absolutely necessary, and upon the approval of the 902d MI Group Commander.

10. (U) ~~(C)~~ Reports:

a. Source administration, operational reports and periodic status reports will be submitted in accordance with reference b.

b. Appropriate USAMICOM representatives will be informed of the information gleaned from the operation as it is developed.

ANNEXES:

A - Doctrinal References
B - Agent Personnel
C - Knowledgeability List
D - Cover and Documentation
E - Communications
F - Training
G - Finance and Logistics
H - Termination Plan
I - Target Information
J - Security Weaknesses
K - b1 Plan

CONFIDENTIAL

Annex A (Doctrinal References) to OPlan OP-001-75-902

(C) References contained in this Annex are those which affect the administration and conduct of the operation, as opposed to those which establish the requirements for the operation and are listed under REFERENCES in the heading of this OPlan.

1. Defense Intelligence Agency Manual (DIAM) 58-11, Vol II.

2. Field Manual (FM) 30-17, Counterintelligence Operations, January 1972.

3. FM 30-17A, Counterintelligence Special Operations, February 1973.

4. Army Regulation (AR) 381-141, Provisions for Administration, Supervision, Control and Use of Intelligence Contingency Funds (U), 22 November 1965 with changes 1 through 4.

5. AR 614-115, Assignments, Details and Transfers - Military Intelligence Officer Excepted Career Program (U), 1 November 1974.

6. USAINTA Regulation 381-1, Provisions for Administration, Supervision, Control and Use of Intelligence Contingency Funds (U), 20 August 1974.

7. USAINTA Regulation 381-100, Counterintelligence Activities and Procedures, 13 February 1974.

8. 902d MI Group OPlan QUIZ TALK (U).

9. LTR, AGAM-P(M), ACSI, DSCI, Subject: Availability of Special Counter-intelligence Support, dated 17 September 1965, and Chapter 5, Subject: b1 (C) to AR 381-102 (S), Subject: Intelligence Cover and Operational Support Activities (U), November 1974.

CONFIDENTIAL 489

Page 1988 of 3957

~~CONFIDENTIAL~~

Annex C (Knowledgeability List) to OPlan OP-001-75-902

1. US Army Missile Command:

   a. MG Vincent H. Ellis, Commanding General

   b. COL Arthur G. Lange, Jr., Chief of Staff

   c. Dr John L. McDaniel, Director, USAMRDEL

   d. COL R. A. Axelson, Deputy Director, USAMRDEL

2. 902d MI Group: (Additional personnel of the 902d MI Group will be briefed on the operation only upon the approval of the Group Commander).

   a. COL Albert N. Stubblebine III, Commander

   b. LTC Dale L. Hartig, Deputy Commander

   c. LTC Alton R. Westrick, Operations Officer

   d. MAJ Hugh W. Fitzpatrick, Jr., Asst Operations Officer

   e. CW4 Edward P. Clark, Special Investigations Desk

   f. CW2 Benjamin W. Struchen, Special Operations Desk

   g. CPT Rodney J. Sollenberger, CDR, Atlanta Field Office

   h. CPT Bobby E. Gipson, CDR, Redstone Arsenal Resident Office

3. Case Officer Personnel:

   a. Primary: (to be determined)

   b. Alternate: CPT Bobby E. Gipson

~~REGRADED UNCLASSIFIED~~
~~ON~~ SEP 5 1997
BY USAINSCOM FOIPA
~~Auth Para 4-102 DOD 5200.1R~~

~~CONFIDENTIAL~~ 490

Page 1989 of 3957

~~CONFIDENTIAL~~

APPENDIX I to ANNEX C, OPLAN OP 001-74-902 DATE: 29 January 1975

PROJECT NAME: CANTER RIDE (U)

SUBJECT: Knowledgeability List

1. The following personnel have full knowledge of the operation:

a. 902d MI Group Personnel

(1) CW4 William Johnson, Chief, Liaison Branch, Pentagon Counterintelligence Force.

(2) SGT Dave Horn, Liaison Branch, Pentagon Counterintelligence Force.

b. USAINTA Personnel

(1) COL William S. Wolf, CDR.

(2) COL Hassel L. Parker, DCDR.

(3) COL William T. Singleton, Chief, CI Div.

(4) LTC Donald B. Grimes, Chief, Special Ops Br.

(5) James Hession, GS-13, Chief, Intel Div.

(6) Gordon Huff, GS-13, Exec Asst to Chief, COMPIA.

(7) Les Hime, GS-12, Civ Adv to Chief, Special Ops Br.

(8) Rocco Melo, GS-13, Civ Adv to Chief, Special Ops Br.

(9) MAJ Joseph S. Kieffer, Chief, COMPIA.

(10) CPT Lawrence A. Edell, Chief, Svcs Sec, COMPIA.

(11) CPT Richard A. Govoni, Chief, Ops Sec, COMPIA.

(12) 1LT James A. Holliday, Svcs Sec, COMPIA.

(13) CW2 Mellberth Bowling, Alternate Project Officer, COMPIA.

(14) CW2 John McNulla, Ops Sec, COMPIA.

(15) WO1 Donald J. Rander, Project Officer, COMPIA.

491

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

~~CONFIDENTIAL~~

(16) Dolores J. Crounse, GS-5, Admin Sec, COMPIA.

(17) Judy C. Howard, GS-5, Admin Sec, COMPIA.

(18) SFC James D. Blessing, Admin Sec, COMPIA.

(19) SFC Robert J. Snyder, Ops Sec, COMPIA.

(20) SSG William R. Quinton, Svcs Sec, COMPIA.

(21) SP5 Douglas B. Miller, Svcs Sec, COMPIA.

c. Other MI Personnel

CW3 Ralph W. Ochs, Assignments Officer, MI Br, OPD, MILPERCEN.

2. The following personnel have limited knowledge of the operation:

a. USAINTA Personnel

(1) Autmer Ackley, Jr., GS-12, b1 Mgmt Officer.

(2) CPT Noel Jones, Special Ops Br.

(3) CW3 Robert J. Finch, USAASD.

(4) CW2 Paul B. Maison, USAASD.

b. Other Personnel

(1) COL Ransom Barber, Chief, MI Br, OPD, MILPERCEN.

(2) CAPT Donald B. Polatty, USN, Dir, Personnel & Administration Div, DNA.

(3) LTC C. P. Joiner, Jr., CDR, 901st MI Det.

(4) LTC Floyd W. Cox, Jr., Chief, Admin Services Div, DNA.

(5) MAJ David A. Harrison, Chief, Mil Pers Div, DNA.

(6) CPT Doneld Howell, Chief, Mail & Records Br, DNA.

(7) CW3 Darrell Graf, Assignments Officer, AG Br, OPD.

CONFIDENTIAL

Page 1992 of 3957

(8) CW3 Charles B. Decker, Deputy Chief, US Army Staff Officer Personnel Div, TAG.

(9) SGM Edward J. Doucette, Jr., US Army Staff Officer Personnel Div, TAG.

(10) MSG Larry C. Duke, F&AO, Fort Myer, VA.

(11) LTC C. F. Fry, USAINTA Liaison officer to the Army Material Command.

Inclosure
Security Oaths

REGRADED UNCLASSIFIED
ON SEP 5,1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

Page 1992 of 3957

Annex D (Cover and Documentation) to OPlan OP-001-7 02

1. (C) C/O Cover and Documentation:

a. b1

b. b1

c. Documentation:

(1) b1

(2)
(a)
(b)
(c) b1

Annex D (Cover and Documentation) to OPlan OP-001-75-902

2. (C) b1

a. b1

b. b1

Page 1994 of 3957

(c) b1

1. (c) b1

a. b1

b. b1

(1) b1

(2) b1

c. b1

2. (c) b1

a. b1

b. b1

(1) b1

(2) b1

c. b1

Annex E b1

3. (c) b1

a. b1

b. b1

c. b1

4. (c) b1

a. b1

(1) b1

(2) b1

b. b1

(1) b1

Page 1996 of 3957

(2) b1

b1

c. b1

(1) b1

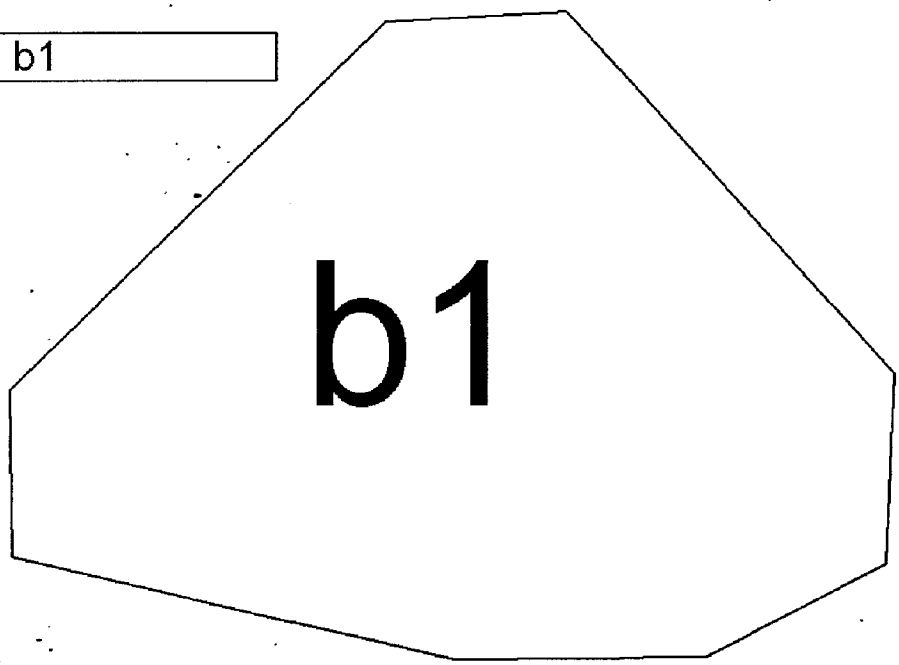
(2) b1

(3) b1

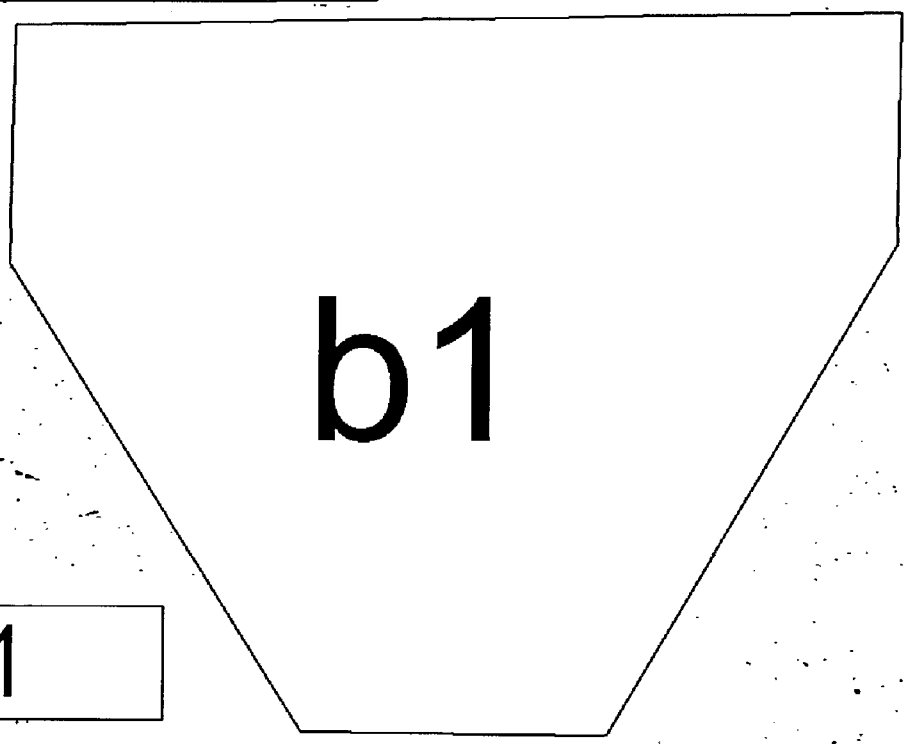
5. (c) b1

Appendix 1 (Commun ations Diagram) to Annex E (C unications) to OPlan OP-001-75-902

1. b1



2. b1



b1

CONFIDENTIAL

499

Appendix 1 to Annex E

1. ~~(C)~~ b1

2. ~~(C)~~ b1

a. b1

b. b1

c. b1

d. b1

e. b1

f. b1

3. ~~(C)~~ b1

Page 1999 of 3957

Appendix 1 (Standard Essential Elements of Information) to Annex F (Training) to OPlan OP-001-75-902.

1. b1

2. b1

3. b1

4. b1

5. b1

6. b1

7. b1

8. b1

9. b1

10. b1

Page 2000 of 3957

Appendix 2 (Specific Essential Elements of Information) to Annex F (Training) to OPlan OP-001-75-02

1. b1
2. b1
3. b1
4. b1
   a. b1
   b. b1
   c. b1
   d. b1
   e. b1
   f. b1
   g. b1
5. b1
6. b1
7. b1
8. b1

CONFIDENTIAL

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

5 USC 552 (b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 503-504

IAGPA-CSF Form 6-R
1 Sep 93

CONFIDENTIAL

1. (c)

b1

2. (U) (C) The source may be terminated with or without prejudice, which indicates a recommendation for future utilization only.

a. A source may be terminated with prejudice for any of the following reasons:

(1) Control by HoIS.

(2) Complete ineptitude.

(3) Unwillingness to accept direction or guidance from the C/O, or continuous disregard for security instructions.

(4) Compromise as a result of his own actions, in violation of the C/O's instructions.

(5) Deliberate distortion or fabrication of information.

(6) Habitual law violation.

(7) Inability to give satisfactory explanations for long absences or suspicious actions.

b. A source may be termin ated without prejudice for any of the following reasons:

(1) Compromise through no fault of his own.

(2) Loss of placement and/or access.

(3) Desire of the source to terminate for non-operational reasons.

(4) Deterioration of health of the source to a degree that he cannot continue his efforts.

(5) Recruitment of other assets who have better placement and/or access.

(6) Termination of the operation.

CONFIDENTIAL

Page 2003 of 3957

3. (c) b1

a. b1

b. b1

c. b1

d. b1

e. b1

4. (c) b1

a. b1

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

5 USC 552 (b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 507-508

IAGPA-CSF Form 6-R
1 Sep 93

Annex I (Target Information) to OPlan OP-001-75-902

1. (U) The initial specific target of the operation is the Optical Guidance Technology Office (OGTO), which is an office within the Advanced Sensor Directorate (ASD) located in Building 5400, a restricted area located on Redstone Arsenal (RA). Mr J. Ducote is the director of OGTO and Mr W. J. Linberg is the director of ASD. Neither of these persons is aware of the operation. ASD is one of several directorates under the US Army Missile Research, Development and Engineering Laboratory (USAMRDEL) which is responsible for developing concepts for new missiles. Dr J. McDaniel, Director USAMRDEL, and COL R. A. Axelson, Deputy Director USAMRDEL, have been briefed on the operation. USAMRDEL is, in turn, one of nine directorates which are collectively responsible for the developing, testing and procurement of missiles for the US Army Missile Command (USAMICOM). The CG, USAMICOM, Major General Vincent H. Ellis and the CofS, COL Arthur G. Lange Jr., are aware of the operation.

2. (U) Further information pertaining to RA, USAMICOM, Huntsville and a map of RA are provided in Appendices to this Annex.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2006 of 3957

THE COMMANDS

U.S. Army Missile Command (MICOM)
U.S. Army Missile and Munitions Center and School (MMCS)
U.S. Army Medical Department Activity (MEDDAC)
Ballistic Missile Defense Systems Command (BMDSCOM)
U.S. Army Engineer Division, Huntsville
Ballistic Missile Defense Advanced Technology Center (BMDATC)
Redstone Readiness Group

Redstone Arsenal is a combination of two U.S. Army arsenals established in 1941, for the production of artillery shells. Today it is the nerve center of the Army's missile and rocket programs.

The 38,650 acres were designated the center of research and development activities for rockets and related items in October, 194 Recruitment of technical and professional personnel began in January, 1949, and a Research and Development Division was establishe the next month.

Redstone Arsenal was declared an active installation by the Department of the Army on June 1, 1949. Some of the Army's rocket exper who had been working at Ft. Bliss, Texas were moved to Redstone in April, 1950. This included the team of scientists and engineer headed by Dr. Wernher von Braun.

Six major Army agencies are now located on Redstone and in neighboring Huntsville. Based on the arsenal are the U.S. Army Missi Command and the U.S. Army Missile and Munitions Center and School. The George C. Marshall Space Flight Center of the Nation Aeronautics and Space Administration is also sited on the arsenal as well as a government-owned, contractor-operated facility engaged i rocket propellant research and manufacture — the Huntsville Division of Thiokol Chemical Corporation.

In nearby Huntsville are the Army's Ballistic Missile Defense Systems Command and Ballistic Missile Defense Advanced Technology Center, The U.S. Army Engineer Division, Huntsville, and the Redstone Readiness Group.

The arsenal's land area includes three minor mountains, 94 miles of railroads, more than 330 miles of roads and more than 2,00 buildings. There is a jet length airfield and modern cargo docks on the Tennessee River, the arsenal's southern boundary. Army buildin and equipment at Redstone are valued at more than $330 million.

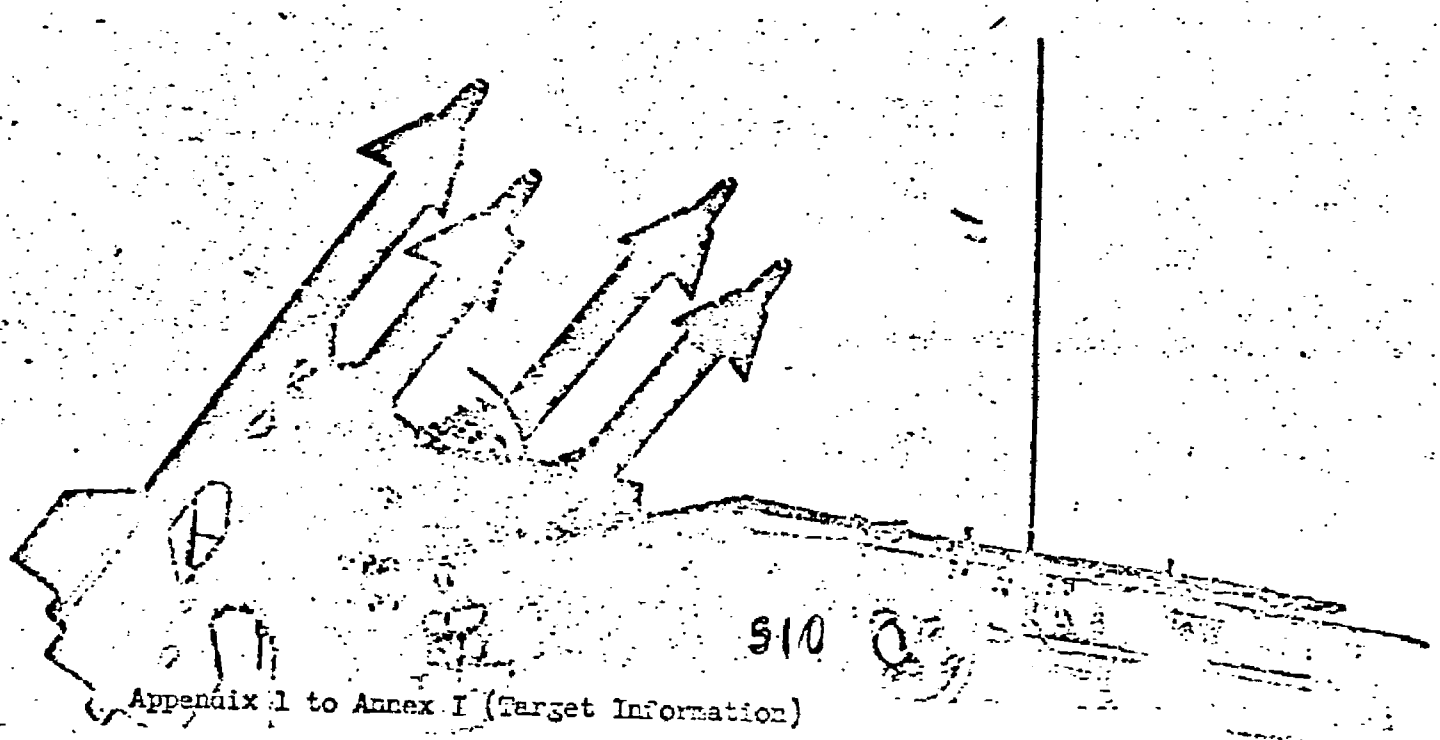
An average of 20,000 vehicles pass through Redstone's gates each day. In an average month, some 8,000 transient visitors are badge through the control facilities to do business or tour one or more of the government agencies on the installation.

The arsenal has a daily government and contractor working population of about 25,000. Although no civilians live on the arsenal, mo than 1,000 military families reside in government quarters. Approximately 1,500 children of military personnel residing on the installati attend schools in Huntsville.

Civilian employees working for the Department of the Army at Redstone and in Huntsville number about 10,000. Approximately 4,0 soldiers are assigned to the various Army commands and agencies. The total Army payroll at Redstone and in Huntsville exceeds $2 million.

Nearly $2 billion was spent last year by the Army at Redstone and in Huntsville. About 85 percent of the amount went to Americ industry, principally through contracts to companies for missile system research, development and production.

This is an excerpt from Redstone Arsenal, dated 1974, an unofficial guide published by Military Publishers, a private firm in no way connected with the Department of the Army.



Appendix 1 to Annex I (Target Information)

[illegible] a major command of the U.S. Army Materiel Command, has its headquarters at Redstone Arsenal and also runs the installation.

MICOM is responsible for missiles and rockets and the supporting equipment required to field them as weapon systems. The command's mission includes research, development, engineering, testing, procurement, production and logistics support of operational missile and rocket systems.

Activated in 1962, MICOM combines the facilities, personnel and missions of several predecessor Army organizations which, at the same location, have directed the Army's expanding missile and rocket activities at Redstone Arsenal for more than 25 years.

Its predecessors fielded the Army's first generation missile and rocket systems and made major contributions in the late 1950's to early American space exploration efforts — including the launching of our first scientific earth satellite. NASA's major space vehicle development organization, the Marshall Space Flight Center, also located at Redstone, was activated in 1960 from a nucleus of former Army civilian employees at Redstone. The Safeguard ABM system also began as a research and development program managed by one of MICOM's predecessors.

MICOM's programs today include a full spectrum of weapon systems ranging from man portable ground-to-air and anti-tank missiles to the 400-mile range Pershing Missile. Its research and development team pioneered the emerging technology of "smart" or precision guided munitions, artillery shells, bombs, rockets and missiles that home on their targets.

MICOM is also the center of Army effort to advance high energy laser technology.

Although the command's responsibilities are worldwide, most of its experienced team of about 7,000 soldiers and civilians are at Redstone Arsenal. The command's test ranges, laboratories, buildings and highly specialized equipment comprise a total investment of about $400 million. Its annual budget averages more than one billion dollars including funds covering acquisition of missiles and rockets for the U.S. Army as well as many allied nations which also employ U.S. Army missiles and rockets.

Missiles and rockets are not manufactured at Redstone Arsenal. Traditionally, the Army has turned to American industry and business for their manufacture, a task managed by MICOM.

MICOM supports an Army Materiel Command element based at Redstone Arsenal: the project office directing the SAM-D advanced air defense system. Soldiers at Redstone Arsenal work with some of the most advanced equipment in the Army. Their daily tasks may range from a research project to training new members of the Army how to repair components of the missile systems. Here, the soldiers perform the technical side of their job and contribute their part toward making their Army truly modern.

This is an excerpt from Redstone Arsenal, dated 1974, an unofficial guide published by Military Publishers, a private firm, in no way connected with the Department of the Army.

511

Appendix 2 to Annex I (Target Information)

HUNTSVILLE . . .

A Good Place to Live

Huntsville, growing from a town of about 20,000 persons to more than 140,000 since 1950, [illegible] many neighborhood environments with both pleasant [illegible]. The [illegible] and blend with the old. The city's [illegible] in the past, yet it is a vital part of the challenging future. With activities for every age. It is a stimulating and [illegible] place to live. The city itself is progressive, fast growing, beautiful and [illegible] to the pulsating space age. Located in the Alabama Tennessee Lakes section, it is convenient to one of the foremost [illegible] in the South. For the history enthusiast, the nature lover, the hunter, the fisherman, the student, the engineer, the businessman, the club woman — it is the place to be and the place to live.

Many military families reside in the city. Assistance to the new family moving into town is available in the Housing Referral Office at Redstone Arsenal. The office maintains files of rentals and homes for purchase in Building 5666. Phone [illegible]. With this referral assistance, the new family can get settled rapidly.

Huntsville offers schooling through college level, as well as special education classes through high school for those who require it. There are three colleges in Huntsville and a soldier can work toward a degree by the many night courses offered.

This is an excerpt from Redstone Arsenal, dated 1974, an unofficial guide published by Military Publications, a private firm, in no way connected with the Department of the Army.

Appendix 3 to Annex I (Target Information)

512

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

5 USC 552 (b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 5/3

IAGPA-CSF Form 6-R
1 Sep 93

~~CONFIDENTIAL~~

Annex J (Security Weaknesses) to OPlan OP-001-75-902

1. (U) ~~(C)~~ Colonel Arthur G. Lange, Jr., Chief of Staff, US Army Missile Command (USAMICOM) has requested a counterintelligence operation be initiated within USAMICOM to ensure the security of that command with emphasis on security of classified defense information. The chain of event, list of persons involved, and allegations which fostered the request are as follows:

a. Chain of Events:

(1) On 14 May 1974, a SECRET document entitled "Vunerability Assessment of Army Electro Optical Missile Systems (U)", copy 7, dated 7 December 1973, was determined to be missing and has not been found. Compromise was not considered remote.

(2) On 16 May 1974, a CONFIDENTIAL document entitled "Internal Technical Note RE72-35, Digital Simulation of the Texas Instrument's Cannon Launched Guided Projectile (U)", dated 24 October 1972, was found in a desk drawer of Mr b6, a member of OGTO. The document was found in the desk during an after-hours check for SECRET material referred to in para 1a(1) above. The classification markings had been excised from the document. During the investigation for this incident, b6 admitted in his sworn statement that he had found another CONFIDENTIAL document in his desk on 12 June 1974.

(3) During the week of 20 September 1974 another SECRET document entitled "Laser countermeasures/counter counter measures (U)", Progress Report, Pitman Dunn Laboratory, Frankfort Arsenal, was found to be missing and could not be accounted for. The investigation is ongoing and it is anticipated that b6 will be considered responsible and may receive a letter of reprimand and/or a day's loss of pay.

b. Personnel within OGTO and ASD who may be of counterintelligence interest include the following:

(1) b6, GS15, Supervisor, OGTO.

(2) b6, GS12, Physicist, formerly assigned OGTO,

(3) b6, GS14, Aerospace Engineer, OGTO.

(4) b6 nee: b6, GS4, Typist.

(5) b6, GS14, Engineer, OGTO.

(6) b6, GS15, Physicist, OGTO.

(7) b6, GS12 (formerly 1LT), Engineer, OGTO.

(8) b6, Nee: b6, GS5, Clerk, OGTO.

(9) b6, GS11, Electronics Technician, OGTO.

514

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP 5,1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

~~CONFIDENTIAL~~

Annex J (Security Weaknesses) to OPlan OP-001-75-902

c. During an investigation into the loss of documents listed above, certain allegations were made which reflected adversely on persons assigned to OGTO, ASD and USAMICOM. In general, the allegations are as follows:

(1) b6 and b6 had a romance although each was married.

(2) b6 conducted herself in a manner to suggest that she was "available" or as a practical joke by sitting in b6 and b6 lap during office meetings.

(3) b6 was so mad that he claimed he would "kill" b6 for "screwing his girl" in reference to b6.

(4) b6 believes b6 placed CONFIDENTIAL documents in b6 desk because of jealousy.

(5) b6 alleges there is a meeting place for sexual activities by b6 and other members of the office.

(6) Pornographic films shown in this meeting place during office lunch hours.

(7) b6 and b6 took two secretaries to this meeting place during lunch.

(8) Office calls and contacts with a Marge Cleveland, now deceased, who was called "Bucking Bronco".

(9) Homosexual tendencies by b6.

(10) b6 intoxicated on the job.

(11) b6 used to place persons under obligation.

(12) b6 and b6 procuring secretaries for sex.

(13) Someone placed sugar in the gas tank of b6's truck and dameged the motor. b6 alleges that it was b6.

2. (U) Further information to include sworn statements are on file at Headquarters, 902d MI Group, and COMPIA, USAINTA.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

515

~~CONFIDENTIAL~~

Page 2012 of 3957

CONFIDENTIAL

ANNEX K to OPLAN 001-74-902 DATE: 29 January 1975

PROJECT NAME: CANTER RIDE (U) PROJECT NUMBER: IA-74-001

SUBJECT: b1

1. (U) AUTHORITY/REFERENCE:

OPLAN OP 001-74-902, dtd 21 Nov 74, Subject: Special Counterintelligence Support, and references cited therein.

2. (c) BACKGROUND/OBJECTIVES:

a. b1

b. b1

c. b1

3. (c) CONCEPT OF OPERATION:

a. b1

516

CONFIDENTIAL

CLASSIFIED BY CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2

~~CONFIDENTIAL~~

b1

b. b1

c. b1

(1) b1

(2) b1

(3) b1

(4) b1

(5) b1

~~CONFIDENTIAL~~

Page 2014 of 3957

CONFIDENTIAL

MIIA-IA-O 12 November 1974

SUBJECT: CANTER RIDE Feasibility Study (U)

1. (U) References:

a. Letter, Redstone Resident Office, Redstone Arsenal, Alabama, 902d Military Intelligence Group, MIIA-GPR-RS, dated 23 September 1974, Subject: Request for Counterintelligence Special Operation (U), with inclosures.

b. Letter, Headquarters, US Army Missile Command, Redstone Arsenal, Redstone, Alabama, AMSMI-X, dated 30 September 1974, Subject: Request for Special Counterintelligence Support (U), with 1st indorsement, Headquarters, 902d Military Intelligence Group, Fort Meade, Maryland, dated 9 October 1974.

c. Discussions between representatives of the 902d Military Intelligence Group and the Composite Intelligence Activity (COMPIA), on 27 September and 4 October 1974.

d. Chapter 5, AR 381-102 (S).

2. (C) Section I. Purpose of Study. During the period 16 to 17 October 1974, COMPIA Project Officers, Mr. Mellberth Bowling and Mr. Donald J. Rander, visited the Redstone Resident Office, 902d MI Group, Redstone Arsenal, Huntsville, Alabama, for the purpose of compiling the necessary information

b1

into the Optical Guidance Technology Office (OGTO), Advanced Sensors Directorate (ASD), US Army Missile Research, Development and Engineering Laboratory (USAMRDEL), US Army Missile Command (USAMICOM), Redstone Arsenal, Alabama. In addition, the study was conducted to determine the feasibility of providing assistance to the Commander, USAMICOM, through the use of a b1 to improve the security posture of the Command.

3. (C) Coordination.

b1

CLASSIFIED BY CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 3
DECLASSIFY ON

518

CONFIDENTIAL

CONFIDENTIAL

MIIA-IA-O 12 November 1974
SUBJECT: CANTER RIDE Feasibility Study (U)

b1

4. (U) ~~(C)~~ Section II. Findings.

a. USAMICOM, a subordinate command of the US Army Materiel Command (AMC) is commanded by Major General Vincent H. Ellis, and has been classified as a "Highly Sensitive" Class II Installation by the Department of Army. In addition to the requisite Table of Organization and Equipment, logistical, and administrative support elements, USAMICOM consists of various US Army Missile Systems project offices, a contingent of missile systems Liaison Offices with foreign allied military forces to include Senior Staff Technical Representatives stationed at CONUS and OCONUS installations, a complement of special activities, such as the US Army Metrology and Calibration Center and the Missile Intelligence Agency, and six sensitive Directorates, three of which are considered "critically sensitive" by USAMICOM. This category applies to the USAMRDEL, the Directorate for Procurement and Development (DPP), the Directorate for Product Assurance (DPA), and the Missile Intelligence Agency (MIA). The mission of these Directorates is directly related to the crucial phases of research and development of all current and future missile systems in the US Army and to the contracting to appropriate firms for production. The Advanced Sensors Directorate (ASD) of the USAMRDEL is of specific interest to this study as indicated in references listed in paragraph 1, above.

b. USAMICOM has a significantly large number of civilian employees and assigned military personnel, who by the nature of their duties, require access to critically classified defense information and material. Suitability shortcomings such as drug and alcohol abuse, possible homosexuality and immoral activity, and excessive indebtedness, all of which have been alleged against USAMRDEL personnel, serve to create a fertile field for Hostile Intelligence (HoIS) offensive intelligence operations against the Command. The human element of USAMICOM, therefore, must be considered particularly vulnerable to the security of the Command. The desirability of advanced knowledge of the US Army missile systems must be considered lucrative to HoIS. By obtaining this type of information, the efficiency of these systems in a future battlefield environment could be impaired and thereby adversely affect the national defense of the United States. In a Sensitive Activity Vulnerability Estimate (SAVE), dated 5 February 1974, conducted at USAMICOM, a number of violations and shortcomings were noted in the above critical directorates. A synopsis of the SAVE and other incidents which have occurred in USAMRDEL subsequent to the SAVE, follows:

5 9

CONFIDENTIAL

Page 2016 of 3957

CONFIDENTIAL

MIIA-IA-O 12 November 1974
SUBJECT: CANTER RIDE Feasibility Study (U)

(1) In MIA, SECRET material was discovered in containers which also contained unclassified material. SECRET documents were also stored in unauthorized security containers. Accountability for classified documents in MIA is maintained on Automatic Data Processing (ADP) equipment which is also used extensively for routine office functions. This practice has been continued despite the fact that the classified document custodians are not properly trained in ADP security procedures.

(2) Most document custodians are not knowledgeable of the provisions of DoD Regulation 5200.1-R or AR 380-5 and other AMC and USAMICOM security regulations.

(3) Personnel of USAMICOM are not receiving proper security indoctrination instructions in accordance with applicable regulations. There is a general lack of security consciousness throughout the Command, but is especially evident amongst the civilian, scientific-oriented personnel, who refuse to properly wear and display their security badges or assist in sound security practices and procedures.

(4) Conference rooms utilized to discuss classified information are not properly secured and maintained. No record of CI Technical inspections for sensitive areas and conference rooms was available.

(5) There is an inadequate number of qualified Security Support Specialists assigned to USAMICOM. USAMRDEL shares such a support officer with three other Directorates or project offices.

(6) Classified Document Custodian duties within USAMRDEL are normally assigned as an "extra duty". This practice fosters resentment of the responsibility on the part of personnel assigned the task. This has resulted in poor administration of the control of classified documents, a factor which significantly contributed to the loss of seven SECRET documents in USAMRDEL. In each case, it was determined that the fault was an administrative error on the part of the custodian. Subsequent to the above incidents, on 14 May and 20 September 1974, two more classified documents were discovered missing from OGTO, the office within USAMRDEL referenced in 1a, above. The 14 May violation was discovered during a non-duty hours check. In this instance, a CONFIDENTIAL document was found in a desk. The classified markings had been removed. The 20 September incident occurred after a 100% inventory and resulted in a reprimand and possible loss of one day's pay for b6 b6 GS-15, upon whom the responsibility for the loss was fixed.

520

CONFIDENTIAL

REVIEWED UNCLASSIFIED
ON SEP 5, 1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

Page 2017 of 3957

~~CONFIDENTIAL~~

MIIA-IA-O 12 November 1974
SUBJECT: CANTER RIDE Feasibility Study (U)

(7) Uncleared personnel have access to Building 5400, a RESTRICTED AREA, which houses in part USAMRDEL and in particular, the Advanced Sensors Directorate and OGTO. The Building's Cafeteria employees do not have security clearances yet they have entrance badges. These badges do not identify the bearer since they have neither the picture nor the name of the individual. No roster is maintained of these personnel.

Singularly, the above infractions and violations do not justify the use of a SCOPI asset. Collectively, however, these security problems constitute a serious threat to the security of the Command as similar situations exist in most of the other critically sensitive Directorates. In addition to the above security problems, the Request for Special CI Support, reference in 1b, above, outlines a serious suitability problem which allegedly involves the entire office staff of OGTO.

5. (U) ~~(C)~~ Analysis.

a. Based upon the Findings as outlined above, a SCOPI is believed to be the most advantageous investigative tool to assist the requestor Command because the local Military Intelligence personnel are highly visible in the area and do not have at their disposal the resources necessary to provide the Commander of USAMICOM indepth CI support. The RRO has two enlisted agent personnel and one MI Officer present for duty. This office conducts 36 CI Inspections and Checks of USAMICOM and the US Army Munitions School and Center units annually. The inspected elements have an aggregate of over 100,000 SECRET documents and approximately three linear miles of CONFIDENTIAL material. About 350 classified document custodians routinely maintain these documents. In addition to being tasked to conduct SAVE studies, the RRO is tasked with normal liaison contact, suitability investigations, incident investigations, occasional PSI investigations, and security indoctrination briefings when time permits. Even though these accumulative services benefit the Commander in terms of CI Support, RRO personnel have noted that corrective follow-up actions concerning reported infractions have proven to be of a temporary nature. This has been evidenced by the recurrence of similar violations and infractions during a short period of time following the conduct of CI services. The local CI effort has been hampered by the existence of a large number of uncooperative and apathetic scientifically oriented personnel in the Command. The attitude of these personnel toward sound security practices and procedures can only be described as uncooperative and lackadaisical. It is therefore considered highly unlikely for the RRO to be successful in conducting an ICIP operation in the area. Additionally, past intelligence related investigations concerning USAMICOM personnel has fostered an unfavorable attitude toward intelligence personnel in general. The following details the procedures through which personnel are acquired in USAMRDEL.

521

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP 5,1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

~~CONFIDENTIAL~~

MIIA-IA-O 12 November 1974
SUBJECT: CANTER RIDE Feasibility Study (U)

b. There are 162 civilian personnel assigned to the Advanced Sensors Directorate. The director is Mr. William J. Lindberg, GS-15. Seven of these civilians normally perform duties in the Optical Guidance Technology Office, which is the specific target area of the requested support as outlined in above references, under the supervision of Mr. b6 GS-15. The General Schedule rating of the Directorate's employees range from GS-1 to GS-16. The majority of ASD personnel perform duties related to research and development which are highly technical in nature. When deemed necessary, all personnel of USAMRDEL are subject to being required to perform functions in other Directorates and Offices to fulfill specific project requirements. However, in instances wherein additional manpower must be procured from resources outside of USAMICOM, the request for Personnel Action (SF Form 52) may be initiated by the respective office supervisor or the Director of the Directorate concerned. The request must be staffed through the appropriate chain of command within the Directorate to the Civilian Personnel Office (CPO), USAMICOM. The request is then reviewed by the CPO Technical Services Branch, where it is recorded in the Personnel Control Roster. Following this action, the request must be reviewed by the CPO Position/Pay Management Branch, where it is closely reviewed to determine the correctness of the pay grade and job description. From that Branch, the request is forwarded to the Recruiting and Placement Branch for recruitment action. In any event, positions are normally filled from personnel listed on the DoD Stopper List, local RIF lists, internal promotion, lateral transfer or direct hire.

c. Requisitions for military and civilian personnel for assignment to USAMICOM are unique in terms of routine requisition assignments in other commands of the US Army. All assignments to USAMICOM are dictated on the basis of current and future project requirements which fluctuate according to the mission, necessity, and special qualifications of desired personnel. This system is known as Project REFLEX. It provides authority to fill temporary or permanent positions for the duration of a specific project at the completion of which the individual may be reassigned or shifted to another office within USAMICOM.

d. There are only three authorized military positions within the Advanced Sensors Directorate. One of these positions is a LTC, MOS 2157 (Research and Development Coordinator), located at White Sands Missile Range, New Mexico. The remaining two, a 2LT, MOS 7302 (Physicist) and a CPT, MOS 7601 (Electrical Engineer) are assigned to Redstone Arsenal. These positions are currently filled. Requisitions for US Army personnel assigned to ASD or the USAMRDEL are submitted by the Consolidation of Military Personnel Activities (COMPACT), USAMICOM to AMC on a Projected Requisition Authority (PRA). The need for personnel is determined by COMPACT, who subtracts or adds gains and losses using current personnel strength figures which are compared with the

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

522

~~CONFIDENTIAL~~

CONFIDENTIAL

MIIA-IA-O 12 November 1974
SUBJECT: CANTER RIDE Feasibility Study (U)

PRA account. Should it be determined that a shortage of personnel exists, COMPACT may then submit the requisition to AMC who, in turn, submits the request to DA. Personnel can be assigned either directly to the USAMRDEL, or to COMPACT on DA orders for further assignment within the Command.

e. As a minimum, a SECRET security clearance is required for all civilian and military personnel assigned to USAMRDEL. Upon arrival of military personnel in the Command, the Clearance and Intelligence Branch, Internal Security Division, COMPACT reviews the individual's 201 file, Medical and Dental Records. This is a routine procedure conducted to determine the person's eligibility for a security clearance. The individual must fill out a locator card, a request for security clearance statement, and a local office personnel data card. COMPACT determines the degree of clearance required, based on the sensitivity of the position to which the individual is to be assigned. If a valid DA Form 873 (Certificate of Clearance and Security Determination) is in the individual's file, and no derogatory information is revealed in the files review, a SECRET clearance is normally granted. Should the file not contain a valid 873 form, appropriate action is initiated for verification of security clearance data through USAIRR. Although contrary to routine procedures, the USAIRR Dossier may be requested for review.

f. Due to the highly technical nature of the civilian positions within ASD it is not considered feasible to [b1] into any of these positions. Because the three authorized military positions within ASD are currently filled, an alternate military position must be considered for [b1] The viability of utilizing a SCOPI asset in ASD under the guise of a Classified Document Control Officer (CDCO) appears highly favorable since the Command plans to centralize the classified document control unit within ASD and acquire a properly trained classified document custodian to maintain the documents. This position has Command sanction as it would serve to decrease the recurrent difficulties experienced by the Command in the control of classified material and would be widely accepted by ASD personnel because of their dislike for performing the extra duties as a CDCO. Through the use of Project REFLEX,

b1

523

CONFIDENTIAL

CONFIDENTIAL

MIIA-IA-O 12 November 1974
SUBJECT: CANTER RIDE Feasibility Study (U)

b1

(1) Age: 35 to 40 years.

(2) Marital Status: Unmarried.

(3) Race: Caucasian.

(4) Ethnic background: Preferably born in the Southern region of the United States.

(5) b1

(6) b1

(7) Rank: WO, CW2 or CW3.

(8) Training and experience:

b1

As most of the local personnel are Caucasian and from the Southern region of the United States, these characteristics are deemed beneficial to mission accomplishment. Operational control of the SCOPI will be executed by the 902d MI Group, who will be responsible for writing the Operations Plan. A CI Inspection of ASD is currently in progress by the RRO, 902d MI Group. Significant findings will be reported to COMPIA if deemed relevant to the proposed requested Special CI Support.

6. (C) Conclusions. In view of the collective security shortcomings noted in the Command, the highly sensitive nature of the mission of the Command,

524

CONFIDENTIAL

7

CONFIDENTIAL

MIIA-IA-0 12 November 1974
SUBJECT: CANTER RIDE Feasibility Study (U)

and the severely limited options available to local MI activity in the area,

b1

7. (C) Recommendation. b1

RICHARD A. GOVONI
CPT, MI
Chief, Operations Section, COMPIA

525

CONFIDENTIAL

DISPOSITION FORM

For use of this form, see AR 340-15; the proponent agency is the Adjutant General's Office.

CONFIDENTIAL

REFERENCE OR OFFICE SYMBOL	SUBJECT
MIIA-IA-O	CANTER RIDE (U)

TO: b1
ATTN: Mr. Ackley

FROM: Chief, COMPIA

DATE: 3 Feb 75
Rander/dic/6364

1. Your attention is invited to paragraph 1, Annex G; and paragraph 6, Annex K of OP001-75-902.

2. Request your concurrence and recommendations.

1 Incl
Ltr 902d MI Gp 21 Nov 74 w/incl

JOSEPH S. KIEFFER
MAJ, MI
Chief, Composite Intelligence Activity

b1

b1
TO: Chief, COMPIA

FROM: b1 Office

DATE: 4 Feb 75 CMT 2

1. Concur with the proposed utilization of b1

a. b1

b. If payment of partial per diem is considered essential in this instance, then it must be authorized by classified orders and paid through CPT Denny's office.

c. It is true that partial per diem is authorized for duty in excess of 10 hours per day away from a persons normal duty station; however, it is suggested that the daily training time be adjusted so as to reduce the overall time to less than 10 hours per day.

2. Funds are available to support this project for the remainder of FY 75.

1 Ind
MC

AUTMER ACKLEY JR.
DAC, GS-12
b1 Management Officer

Regraded CONFIDENTIAL
ON 5 SEP 1997
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

526

REGRADED UNCLASSIFIED

DAMI-ZA

04 FEB 1975

MEMORANDUM THRU: VICE CHIEF OF STAFF, UNITED STATES ARMY

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

1. (U) This is in response to your Memorandum on 17 January 1975 to the Vice Chief of Staff in regard to subject and serves as the Quarterly ICIP Report for the 2d Quarter, FY 2975.

2. (U) (C) On 2 October 1974, I directed a review of the entire ICIP program with a view towards the elimination of those no longer considered of sufficient merit to warrant retention. The criteria used in evaluating each ICIP operation was: (a) The sensitivity of the installation/activity is such that some type of special counterintelligence support is required or (b) There is a known threat of sufficient magnitude to the installation/activity to warrant a need for some type of special counterintelligence support and (c) The information desired cannot be obtained except through the use of confidential sources.

3. (U) (C) Based on this review and considering your 17 January guidance, I directed the termination of 12 ICIP operations at the following headquarters:

a. Hq, US Army Communications Command, Fort Huachuca, Arizona (CANAL ROPE).

b. Dugway Proving Ground, Utah (CANARY STONE).

c. US Army Air Defense Center, Fort Bliss, Texas (CANTINA ARCH).

d. Umatilla Army Depot Activity, Hermiston, Oregon (CANYON ROSTER).

e. US Army Mobility Equipment Research and Development Center, Fort Belvoir, Virginia (CENTAUR SALE).

Regraded CONFIDENTIAL when Separated from CLASSIFIED Inclosures

527

Classified by DAMI-ZA

EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652

EXEMPTION CATEGORY 2

DECLASSIFY ON 31 Dec 2005

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

J. Branch
Richard Cavoy

DAMI-ZA
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

f. Hq, US Army Electronics Command, Fort Monmouth, New Jersey (CENTRAL TAXI).

g. US Army Management Systems Support Agency, The Pentagon, Washington, DC (CENTURY SQUAD).

h. US Army Electronics Proving Ground, Fort Huachuca, Arizona (GONDOLA FLAG).

i. Aberdeen Proving Ground, Aberdeen, Maryland (GONDOLA STAR).

j. Defense Language Institute East Coast, Washington Navy Yard, Washington, DC (LANYARD MOOD).

k. Picatinny Arsenal, Armament Command, Dover, New Jersey (LEND TONE).

l. US Army War College, Carlisle Barracks, Pennsylvania (LENIENT CLOUD).

4. (U) The remaining seven ICIPs are worthy of retention as they meet your criteria. Reviews of these seven operations are attached at Incl 1. Reviews of the 12 to be terminated are at Incl 2.

(Sgd) Harold R. Aaron

2 Incls
as

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

REGRADED UNCLASSIFIED
ON SEP 5
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

528

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP (U)

OFFICE SYMBOL: DAMI-DOI-C

SUSPENSE:

DATE: 31 January 1975

ACTION REQUIRED: To respond to tasking from the USofA pertaining to ICIP.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. BACKGROUND:

a. At the direction of the USofA quarterly reporting of ICIP has been furnished to him through the VCSA since February 1972. In a memorandum to the VCSA (RED TAB B), the VSofA suggests that in more than half of the ongoing operations, no useful information was developed. He directed a detailed review of the benefits derived through the program over the last two years.

b. On 29 January 1975, the ACSI directed the termination of 12 of the 19 ongoing operations. They will be terminated on a time phase basis with all 12 being terminated by 31 March 1975.

2. DISCUSSION: At RED TAB A is a memo through the VCSA to the USofA replying to the comments of USofA and providing the requested information pertaining to the program.

3. RECOMMENDATION: That the memo at RED TAB A be approved and signed.

(Continue on plain bond)

IMPLICATIONS — CINFO: YES ☐ NO ☐ | PRIM PROGS: YES ☐ NO ☐ | BUDGET: YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR	[illegible]	3 Feb 75
			DIV	[illegible]	[illegible]
			DIRECTOR	[illegible]	[illegible]
			EX		
			ACSI	[illegible]	
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*

MAJ EBERSOLE/56074/th [signature] 529

[signature] Record Copy

ACSI FORM 28, 13 Sep 71

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

DEPARTMENT OF THE ARMY
OFFICE OF THE UNDER SECRETARY
WASHINGTON, D.C. 20310

17 January 1975

MEMORANDUM FOR: VICE CHIEF OF STAFF, U.S. ARMY

SUBJECT: Internal Counterintelligence Program (ICIP)

I have received and reviewed the latest quarterly report of ICIP operations during 1974 as requested. In 1972 the Under Secretary authorized a trial run of this subject program. Judging from this report, the program has grown considerably and includes installations that I did not appreciate were considered sensitive. A cursory review of the data presented suggests that in more than half the cases, no useful information was obtained.

It would appear to me appropriate to review the results of this experiment to date in order to establish that the program is in fact of such a value that it should be continued in the future.

I would therefore appreciate a detailed report documenting all of the benefits, information, etc., that have been obtained through this program over the last two years. It would also be helpful to have a statement for each listed installation of the sensitive character of the mission that necessitates an ICIP operation. Finally, I would appreciate an indication of your subjective judgment as to how many of the issues that arose from these ICIP efforts would not have otherwise come to our attention.

Herman R. Staudt
Under Secretary of the Army

Inclosure
Memo, 29 Nov 74,
Subj: ICIP Operations

REGRADED FOR OFFICIAL USE ONLY
WHEN SEPARATED FROM
CLASSIFIED INCLOSURES

530

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, D.C. 20310

29 November 1974

MEMORANDUM FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) Operations (U)

1. (U) Reference is made to memorandum, Under Secretary of the Army, dated 8 February 1972, subject as above.

2. (C) During the third quarter of CY 1974, the ICIP at Edgewood Arsenal Maryland (CANAL LOOP) was combined with the Aberdeen Proving Ground ICIP (GONDOLA STAR). The nickname GONDOLA STAR was retained.

3. (C) With the subsidence of anti-military activity at Fort Lewis, Washington and in the absence of a specific on-post threat, the Commanding General, 9th Infantry Division requested that the Fort Lewis ICIP (CENTAUR RACE) be terminated. This ICIP was inactivated on [illegible] 74. During the same time frame, LENS HOLDER, a new ICIP developed at White Sands Missile Range was approved on 7 Aug 74. With the implementation of this ICIP, the total number of active ICIP operations at close of the quarter was 19. Brief status reports are attached.

4. (C) After briefing you on 25 September 1974 on the status of the program, the Assistant Chief of Staff for Intelligence personally viewed and revalidated each on-going operation. Each operation will be revalidated on an annual basis hereafter. Additionally, MI Army has initiated a systematic review of all source dossiers to insure that sources possess sufficient maturity and stability to enable them to function efficiently and effectively in ICIP operations.

1 Incl
as (CONFIDENTIAL)

WALTER T. KERWIN, JR.
General, United States Army
Vice Chief of Staff

Classified by DAMI
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 2004

531

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

MAJ Ebersole/[illegible]

CONFIDENTIAL

OFFICE OF THE UNDER SECRETARY
WASHINGTON, D.C. 20310

17 January 1975

MEMORANDUM FOR: VICE CHIEF OF STAFF, U.S. ARMY

SUBJECT: Internal Counterintelligence Program (ICIP)

I have received and reviewed the latest quarterly report of ICIP operations during 1974 as requested. In 1972 the Under Secretary authorized a trial run of this subject program. Judging from this report, the program has grown considerably and includes installations that I did not appreciate were considered sensitive. A cursory review of the data presented suggests that in more than half the cases, no useful information was obtained.

It would appear to me appropriate to review the results of this experiment to date in order to establish that the program is in fact of such a value that it should be continued in the future.

I would therefore appreciate a detailed report documenting all of the benefits, information, etc., that have been obtained through this program over the last two years. It would also be helpful to have a statement for each listed installation of the sensitive character of the mission that necessitates an ICIP operation. Finally, I would appreciate an indication of your subjective judgment as to how many of the issues that arose from these ICIP efforts would not have otherwise come to our attention.

Herman R. Staudt
Under Secretary of the Army

Inclosure
Memo, 29 Nov 74,
Subj: ICIP Operations

CONFIDENTIAL

22 Jan 75 (DATE) | DAVIS (NAME) | 22866 (CASE NUMBER) | WH/SUSPENSE NO. | CONF (CLASSIFICATION)

WHITE HOUSE CASE ☐ | OCSA CASE XX | SMA CASE ☐

SUMMARY
USofA Memo for VCSA, dated 17 Jan 75, Subject: Internal Counterintelligence Program (ICIP)

SUSPENSE
OCSA 4 Feb 1975
USofA 4 Feb 1975
OSD

ROUTING	A-Action	I-Information			
DCSOPS	ACSFOR	COE	CMH	CLL	
DCSPER A	ACSI	TSG	TAG	MILPERCEN	
DCSLOG	ACSC-E	TJAG	TPMG	CUSAA	
COA	CORC	CNGB	CAR		
CRD	TIG	CINFO	CCH		

REMARKS 532

ACTION
XX DIRECT REPLY WITH 1 COPY(IES) TO OCSA to USofA
☐ CITE WHITE HOUSE CONTROL NUMBER
☐ PREPARE (DRAFT) (FINAL) REPLY FOR SIGNATURE OF
☐ PROVIDE ASSISTANCE AS REQUIRED

THIS MUST REMAIN T O P D O C U M E N T

DOSSIER NO. ZF011946W
Vol 5 of 7 Vols

As of 18 Sep 85 (Date) all material included in this file conforms with DA policies currently in effect.

Delmar Smith 18 Sep 85
(Signature) (Date Signed)

Delmar Smith GS5
(Printed Name) (Grade)

Reviewed for Retention
Criteria UP AR 381-10
Reviewer P. Gaines Date 4 Jan 92

THIS MUST REMAIN T O P D O C U M E N T

IA (HQ) Form 2214
(1 Sep 78)

Replaces MIIA Fm 315, 1 Jun 75, which may be used until supplies are exhausted.

533

CONTENTS

TAB	TITLE	DATE
A	ICIP Gondola Star - Approval	20 Jan 76
B	ICIP Careless Token - Approval	25 Feb 76
C	ICIP Quarterly Report	1 Apr 76
D	ICIP Canary Effort - Terminated	11 May 76
E	ICIP Canter Ride - Terminated	11 May 76
F	ICIP Unnamed OPLAN USAREUR to HQUSASA for Review	12 May 76
G	ICIP Careless Token (USAREUR) to HQUSASA for Comment-concurrence	12 May 76
H	ICIP Careless Token (USAREUR) Terminated	27 May 76
I	ICIP (unnamed OPLAN) (USAREUR) Approved	27 May 76
J	ICIP's Canine Plate (U), Census Time (U), and Centavo Kid (U) - Terminated	8 June 76
K	ICIP - Quarterly ICIP Report	2 June 76
L	ICIP - USAINTA Ltr (MIIA-SO-SA)	25 June 76
M	ICIP - Careless Token (U) various items	

Page 2031 of 3957

JOINT MESSAGE M

SECURITY CLASSIFICATION [redacted] LIMDIS

PAGE	DRAFTER OR RELEASER TIME	PRECEDENCE ACT	PRECEDENCE INFO	LMF	CLASS	CIC	FOR MESSAGE CENTER/COMMUNICATIONS CENTER ONLY DATE - TIME	MONTH	YR
01 OF 03	1625Z	RR	RR		CCCC				

BOOK NO

MESSAGE HANDLING INSTRUCTIONS SECRET 171Z

FROM: SSO ACSI DA WASH DC

TO: SSO HEIDELBERG GERMANY

INFO: SSO INTEL AGENCY FT MEADE MD

~~CONFIDENTIAL LIMDIS WDC~~ 35775 TOPIC

DCSI, USAREUR FOR COL LADEROSA, CH CI DIV; USAINTA FOR LTC GRIMES, CDR SO DET

FROM COL HEISS, CHIEF HUMINT DIV

SUBJECT: INTERNAL COUNTERINTELLIGENCE PROGRAM (ICIP) (U)

A. HBG 1691 TOPIC 021525Z Apr 76.

B. HBG 0072 TOPIC 061755 Jan 76.

C. AEAGB-CI (SO) OPLAN 1-75, 5 May 75, with 5th Ind, ACSI, DA, 25 Feb 76 (ICIP CARELESS TOKEN (U)).

1. (U) The impact of Executive Order 11905 on Counterintelligence Operations and the Army General Counsel's interpretation of the EO by memorandum dated 5 Mar 76, has temporarily delayed implementation of DA policy on the Internal Counterintelligence Program (ICIP). The OACSI and USAINTA staffs are currently preparing recommendations for the ACSI to consider whether any or all of the various ICIP projects should be continued.

XXXXXXXXXXX

LTC Haendle

6 5 4 3 2 1 0

DISTR:

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR INSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

DRAFTER TYPED NAMED, TITLE, OFFICE SYMBOL AND PHONE
K.V. Haendle, LTC(P), DAMI-DOH/56159

RELEASER
TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE
J. L. HEISS III, COL, GS/DAMI-DOH/56074

SIGNATURE

536

SPECIAL INSTRUCTIONS

SECURITY CLASSIFICATION [redacted] LIMDIS

DD FORM 1 JUL 68 173 REPLACES DD FORM 173, 1 NOV 63 AND DD FORM 173-1, 1 NOV 63, WHICH ARE OBSOLETE.

~~CONFIDENTIAL LIMDIS~~

02 of 03

2. (U) Of the operations cited in Ref B above, only CARELESS TOKEN (U) appears to meet the concept of the ICIP as a security service in support of an installation's (or command's) security program. Ref C forwarded the ACSI's approval for this ICIP. We concur with the views expressed in Ref B that CARDINAL FLIGHT (U) and CAREFREE TALENT (U) are defensive CE operations which are not within the scope of the ICIP.

3. (U) Request you provide a summary of the ICIP CARELESS TOKEN (U) for the next ICIP quarterly report by 20 Apr 76 in the following format:

10. (U) CARELESS TOKEN (ACSI Revalidation 25 Feb 76)

A. LOCATION:

B. CONFIDENTIAL SOURCE UTILIZATION: (NUMBER OF SOURCES USED)

C. INFORMATION OBTAINED OR REPORTED ON NON-AFFILIATED CIVILIANS: (NORMALLY "NONE")

D. USEFUL INFORMATION OBTAINED:

(1)

(2) ETC

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

537

~~CONFIDENTIAL LIMDIS~~

~~CONFIDENTIAL~~ ~~LIMDIS~~

03 of 03

(Contains a summary of information obtained in the operation which should not exceed two pages. Content varies by project, but numbers and types of incidents/occurrences reported by sources such as poor security practices, suitability of personnel, suspicious activities and other CI indications are normally included. Names of individuals are not included unless particularly significant.)

E. Operational Status: (Source lead development, results of briefings to supported commanders, anticipated or past changes in the operation, etc).

4. (U) A copy of the summary as rewritten by this office and approved by the ACSI will be returned to you for future guidance.

XGDS-2 31 Dec 2006, AR 381-47.

REGRADED UNCLASSIFIED
ON SEP 5 2007
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~ ~~LIMDIS~~

01 02 RR RR -0000-

HO

SSO ACSI DA WASH DC

SSO HEIDELBERG GERMANY

INFO: SSO INTEL AGENCY FT MEADE MD

-CONFIDENTIAL LIMDIS XGDS- TOPIC

ACSI, USAINTA FOR COL LABERDSA, CH CI DIV; USAINTA FOR LTC GRIDER, CDR SO DET

FROM COL HEISS, CHIEF HUMINT DIV

SUBJECT: INTERNAL COUNTERINTELLIGENCE PROGRAM (ICIP) (U)

A. HDG 1691 TOPIC 021525Z Apr 76.

B. HDG 0672 TOPIC 061755 Jan 76.

C. AEAGB-CI (SO) OPLAN 1-75, 5 May 75, with 5th Ind, ACSI, DA, 25 Feb 76 (ICIP CARELESS TOKEN (U)).

1. (U) The impact of Executive Order 11905 on Counterintelligence Operations and the Army General Counsel's interpretation of the EO by memorandum dated 5 Mar 76, has temporarily delayed implementation of DA policy on the Internal Counterintelligence Program (ICIP). The OACSI and USAINTA staffs are currently preparing recommendations for the ACSI to consider whether any or all of the various ICIP projects should be continued.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

K.V. Haendle, LTC(P), DAMI-DOH/56159

J. L. HEISS III, COL, GS/DAMI-DOH/56074

539

02 of 03

2. (U) Of the operations cited in Ref B above, only CARELESS TOKEN (U) appears to meet the concept of the ICIP as a security service in support of an installation's (or command's) security program. Ref C forwarded the ACSI's approval for this ICIP. We concur with the views expressed in Ref B that CARDINAL FLIGHT (U) and CAREFREE TALENT (U) are defensive CE operations which are not within the scope of the ICIP.

3. (U) Request you provide a summary of the ICIP CARELESS TOKEN (U) for the next ICIP quarterly report by 20 Apr 76 in the following format:

1. (U) CARELESS TOKEN (ACSI Revalidation 25 Feb 76)

A. LOCATION:

B. CONFIDENTIAL SOURCE UTILIZATION: (NUMBER OF SOURCES USED)

C. INFORMATION OBTAINED OR REPORTED ON NON-AFFILIATED CIVILIANS: (NORMALLY "NONE")

D. USEFUL INFORMATION OBTAINED:

(1)

(2) ETC

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

540

~~CONFIDENTIAL~~

03 of 03

(Contains a summary of information obtained in the operation which should not exceed two pages. Content varies by project, but numbers and types of incidents/occurrences reported by sources such as poor security practices, suitability of personnel, suspicious activities and other CI indications are normally included. Names of individuals are not included unless particularly significant.)

E. Operational Status: (Source lead development, results of briefings to supported commanders, anticipated or past changes in the operation, etc).

4. (U) A copy of the summary as rewritten by this office and approved by the ACSI will be returned to you for future guidance.

XGDS-2 31 Dec 2006, AR 381-47.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

541

~~CONFIDENTIAL~~

[redacted]

D'MI-DOH (10 Jun 75)
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

M D', Office of the 'CofS for Intelligence, Washington, DC 20310

TO: Commander, US 'rmy Europe and Seventh 'rmy, 'TTN: DCS for Intelligence, 'PO New York 09403

1. (U) The Operations Plan for ICIP C'RELESS TOKEN (U) in support of Detachment M, US 'rmy Security 'gency, Field Station, 'ugsburg, FRG is approved.

2. (U) 's indicated in earlier correspondence, a Memorandum to the Under Secretary of the 'rmy is prepared quarterly by the Office of the 'ssistant Chief of Staff for Intelligence, D' Staff which includes a brief summary of each ongoing ICIP. Field input is requested by the 15th of the month following the end of the quarter. ' copy of the previous quarterly report is attached as an added enclosure to this correspondence.

2 Incl
'dded 1 Incl
as

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

542

[redacted]

ACTION COPY

ACTION (Action for Handle (DOH)
Peggy Jim Kelly is Cook

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

[redacted]

Best Copy Available

543

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

(d)

(d)

Best Copy Available

544

[redacted]

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOIPO
AUTH PARA 1-603 DoD 5200.1-R

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 12 July 1976

ACTION REQUIRED: To obtain Actg ACSI approval for termination of three and retention of one ICIP.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) Background:

-- Para 3, DAMI-DOH ltr, 8 June 76 (TAB B) and USAINTA reply, MIIA-SO-SA ltr, 25 Jun 76 (TAB C).

2. (U) Discussion:

-- (U) Cdr, 902d MI Group reviewed ICIP, GONDOLA STAR and requested termination effective 30 June 76.

o (U) Confidential sources used in GONDOLA STAR terminated.

o (U) Supported commanders, Edgewood Arsenal/Aberdeen Proving, briefed and concurred in termination. Commanders will be supported by 902d MI Group under DSCCP.

-- (U) Cdr, 525th MI Group reviewed CANVAS TAX (Sierra Army Depot), LENS HOLDER (White Sands Missile Range), and LENTILE MONKEY (Defense Language Institute) to determine possible termination and/or replacement with a program similar to DSCCP.

(U) Cdr, 525th recommends termination CANVAS TAX and LENS HOLDER effective on 31 Aug 76. A DSCCP will be established for Sierra Army Depot and White Sands Missile Range by them.

-- (U) Present techniques used by LENTIL MONKEY best suited to provide required support to Defense Language Institute. LENTIL MONKEY continues to be productive.

(U) LENTIL MONKEY revalidated effective 1 July 76.

3. (U) Recommendation: That ltr (TAB A) to USAINTA be approved and signed.

(Continue on plain bond)

IMPLICATIONS — CINFO: YES ☐ NO ☐ — PRIN PROGS: YES ☐ NO ☐ — BUDGET: YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
USAINTA	MR William Jennings	8-923-6795	BR		
MIIA-SO	MR Paul Clifford	8-923-5103	DIV	G	13 Jul 76
			DIR	[illegible]	14 July 76
			EX		
			ACSI	J	14 JUL 76
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

Classified by CDR, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

ACTION OFFICER (Name, grade, phone and signature)
M. Brannan/53501 M. Brannan 545 7302-76

ACSI FORM 28, 13 Sep 71

CONFIDENTIAL

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

14 JUL 1976

DAMI-DOH

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Commander
US Army Intelligence Agency
ATTN: MIIA-SO
Fort Meade, MD 20755

1. References:

a. Letter, MIIA-SO-SA, USAINTA, dated 25 June 1976, subject as above.

b. Letter, DAMI-DOH, dated 8 June 1976, subject as above.

2. Your recommendation, reference a, paragraph 4, to terminate ICIP, GONDOLA STAR (U), effective 30 June 1976, is approved.

3. Your recommendation, reference a, paragraph 6, to terminate ICIP, CANVAS TAX (U) and LENS HOLDER (U) effective 31 August 1976, is approved.

4. ICIP, LENTIL MONKEY (U) is revalidated effective 1 July 1976.

(s/d) John A. Smith, Jr.

JOHN A. SMITH, JR.
Brigadier General, GS
Acting ACofS for Intelligence

546

FOR OFFICIAL USE ONLY

~~CONFIDENTIAL~~

~~UNCLASSIFIED~~ ACTION SHEET

CONTROL NUMBER

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

OFFICE SYMBOL	SUSPENSE
DAMI-DOH	

DATE: 2 June 1976

SUBJECT: Army Counterintelligence Program (ICIP) (U)

ACTION REQUIRED

To obtain formal ACSI approval for termination of three ICIP operations.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) Background:

Contained in USAINTA's 3d Quarter, FY 1976, ICIP Operations Report, 11 May 76, was recommendation to terminate three operations: CANINE PLATE (U) at Seneca Army Depot; CENSUS TIME (U) at Pentagon Telecommunications Center and CENTAVO KID (U) at Harry Diamond Laboratories.

-- USAINTA recommendation based on 902d MI Group review of ICIP's to determine advisability to terminate these ICIP's and replace them by an overt direct support comprehensive CI program.

2. (U) Discussion:

-- After a thorough review of the ICIP report on these operations, it is determined that they can be terminated with no adverse affect on the installations served. Installations concurred.

-- Increased overt liaison with additional security support will be provided the installations by the 902d MI Group. 902d MI Gp Pamphlet No. 381-3, dated 22 Apr 76, outlines the Direct Support Comprehensive Counterintelligence Program (DSCCP) (TAB C) outlines overt liaison procedures without employing confidential sources.

-- ICIP Reports on CANINE PLATE (U), CENSUS TIME (U) and CENTAVO KID (U) are attached at TAB B.

-- With the termination of these ICIP's, there remains four active CONUS ICIP operations.

-- Ltr to USAINTA at TAB A, furnishes formal termination of these ICIP's and instructs USAINTA to conduct review of the remaining four ICIP's to determine need for continuance, and to forward results and recommendations to this office NLT 21 June 1976.

(Continue on plain bond)

IMPLICATIONS CINFO YES ☐ NO ☐ PRIM PROGS YES ☐ NO ☐ BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DEV		
			DIR		6 June 76.
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

Classified by DCSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXEC ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

ACTION OFFICER (Name, grade, phone and signature)
M. Brannan/GS-13/53501 547

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

DOWNGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

DAMI-DOH
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

3. (U) Recommendation: That ltr TAB A be approved by the ACSI and signed.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

548

~~CONFIDENTIAL~~

Page 2044 of 3957

~~CONFIDENTIAL~~

8 JUN 1976

DAMI-DOH

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Commander
US Army Intelligence Agency
ATTN: MIIA-SO
Fort Meade, Maryland 20755

1. (U) Reference, 3d Quarter, FY 1976, ICIP Operations Report, wherein you recommendad termination of three ICIP operations.

2. (U) ICIP operations, CANINE PLATE (U), CENSUS TIME (U), and CENTAVO KID (U) are formally terminated as recommended.

3. (U) Request that a full review of the remaining four active CONUS ICIP operations be conducted to determine the need for their continuance or discontinuance, and the results, with your recommendations, be forwarded to this office NLT 2[illegible] June 76.

(SGD) Harold R. Aaron

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

Gondola Star
Canvas Tax
Lens Holder
Lentile Monday
} four additional ICIPs

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

549

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(U) CANINE PLATE: (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD), Romulus, NY.

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76: There was no significant information obtained during the period and there were no indications of any overt threat to the installation.

d. Operational Status: CANINE PLATE was first approved by OACSI, DA, for implementation on 18 Sep 73. During the reporting period 400 manhours were expended in the ICIP. However, there were no reports submitted, no funds expended, neither TDY nor ICF. There were no confidential sources utilized, only conventional sources.

e. Comments: The installation's mission remains the same, a supply depot for missile and artillery weapons systems with a nuclear capability. The Depot is considered a critical and sensitive installation; therefore, remains as a potential target for HOIS. However, there was no information reported to indicate the presence of any overt threat to the installation. The MI Group has been conducting a thorough review of the ICIP to determine the advisability of terminating the operation.

f. Recommendation: That the ICIP CANINE PLATE be terminated but that increased overt liaison with additional security support be provided the installation commander.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by CDR USAINSCOM
DECLASSIFY ON: 31 DEC 06

550

[redacted]

ICIP REPORT

1 April 1975 to 31 March 1976

(U) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC.

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During the Period 1 April 1975 to 31 March 1976:

(1) An ICIP source reported that a PTC civilian employee was transferred from the coding and decoding section because he had coded an obscene message that was to be sent to an overseas user. Additionally, the ICIP source provided information concerning possible security violations involving the employee. Because of the employee's questionable suitability characteristics and conduct he was assigned to a job in PTC requiring minimum contact with classified information. Supervisors will continue to monitor his conduct and activities.

(2) An Army NCO assigned to PTC attempted to commit suicide by slashing his wrists. As a result of the information gained concerning the suicide attempt a Limited Investigation was initiated. The NCO was assigned to the Logistics Branch, PTC, pending results of the investigation. The investigation revealed that the NCO has a large number of outstanding debts, has lied on loan applications, and had ordered a 1976 automobile which cost in excess of five thousand dollars. Interviews concerning the NCO revealed alleged drug usage and homosexuality. The Limited Investigation was completed and referred to PTC for adjudication. The decision was made not to revoke the NCO's security clearance since he left the service on 9 April 1976 and will not be allowed to re-enlist.

(3) Adverse suitability information was reported on two additional NCOs assigned to PTC. Based on medical reports and rebellious attitudes one NCO was released from the Army by board action. The second NCO after a night of heavy drinking began hitting his wife when she tried to arouse him after he had "passed out." The wife filed assault charges with the Military Police but withdrew them later. The PTC commander counselled the NCO on his drinking and marital problems and assigned him duties where he has no access to classified information.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by [redacted]
[redacted]
[redacted]
[redacted]
DECL

551

(4) During the course of an investigation of an enlisted WAC member of PTC who was away-without-leave (KAWOL Investigation), it was discovered that the CID was also investigating her for theft and trafficking in drugs. The MI representative and CID agents coordinated their mutual investigations. PTC has suspended the WAC's access to classified material pending completion of the investigation.

d. Operational Status:

(1) CENSUS TIME was first approved by OACSI, DA, for implementation on 5 Feb 74.

(2) During the period of 1 April 1975 to 31 March 1976, 726 manhours were expended, no TDY nor ICF funds were used. The operation produced seven information reports. One confidential source was used during the period but was terminated during the latter part of the period.

e. Comments: The PTC operations include an extremely high volume of multimedia ultra sensitive compartmented classified traffic processed at the highest level of the military establishment command group being served, and includes the cryptographic operation, maintenance and logistical mission and support rendered to the JCS, the NMCC, departments and executive agencies of the government allied embassies, and the United Nations Building in New York. The installation remains as a potential target for HOIS; however, there was no information reported to indicate the presence of any overt threat to the installation. The MI Group has been conducting a thorough review of the ICIP to determine the advisability of terminating the operation and implementing an overt direct support comprehensive counterintelligence program. In view of the above the continuation of an ICIP is not warranted at this time.

f. Recommendation: That the ICIP CENSUS TIME be terminated and an increased overt liaison with additional direct security support be provided the installation commander.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2048 of 3957

[redacted]

ICIP REPORT

1 April 1975 to 31 March 1976

(U) ~~(S)~~ CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories, (HDL), Adelphia, MD

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 - 31 Mar 76:

(1) Information was received that a First Secretary at the USSR Embassy, Washington, DC had visited HDL on two occasions. On one occasion he attended a meeting of the Institute of Electrical and Electronics Engineers, INC., a professional society for engineers which was held in the auditorium of HDL. The subject matter presented during the meeting was unclassified. At a second meeting of the society the Soviet Embassy official was denied entry. A report of the incidents were provided to the FBI and the Commander, HDL, made a determination that the society could no longer hold meetings at HDL in order to preclude any potential security threat.

(2) On two occasions an unidentified light aircraft flew over the test site, Woodbridge Research Facility (WRF), HDL, where a series of tests on foreign equipment under the Range Emory program was in progress. In both instances the aircraft circled over the Range Emory test cite for about 5-7 minutes. The overflights are being investigated in coordination with the FBI.

(3) An employee, HDL, made allegations of immoral activities by members of the HDL Security Office and a group at the Van Ness Avenue Facility, HDL. The employee claimed that she was being followed by members of the HDL Security Office. After investigating the employee's story, the Commander, HDL, believed that she was suffering from psychiatric problems and would have her visit a psychiatrist for a complete evaluation.

(4) Suitability information concerning an employee of the Woodbridge Research Facility (WRF) a branch of HDL located in Woodbridge, VA, involved a problem of alcohol abuse. After counseling, the employee participated in a rehabilitation program.

[redacted]

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

(5) A courtesy penetration test of HDL's Adelphi Facility was conducted and revealed several security weaknesses which were corrected by the supported command. As a result of the test a number of security guards were transferred and guard procedures were changed. In addition a new magnetic coded badge was approved for purchase in FY 77. As a follow-up implementation of "Lessons Learned" in the penetration test the ICIP Project Liaison Officer (PLO) and the HDL Security Officer prepared and delivered a series of lectures and classes to the HDL guard force on the penetration test. Additionally, the PLO delivered lectures on the penetration test to the faculty and students of the Counterintelligence Dept, US Army Intelligence Corps School, Fort Huachuca, AZ.

d. Operational Status

(1) During the reporting period 880 manhours were expended, 18 information reports were submitted and 41 memorandums were prepared and provided to the supported commander.

(2) No TDY or ICF funds were expended.

e. Comments

(1) ICIP CENTAVO KID was approved by OACSI, DA, 18 Oct 73 and the supported commander was briefed on the implementation of the operation on 12 November 1973.

(2) The mission of the HDL includes critical sensitive research and development activities in support of the US Army. Some of the more sensitive activities include research into the hardening of communications equipment against nuclear weapons radiation; tests of nuclear warhead and missile systems to determine their ability to withstand nuclear weapons radiation; develop fuses for use with nuclear warheads and conducts development and testing of radiation hardened systems for Minutemen and Poseidon Missiles.

(3) The installation remains a potential target for HOIS and the hostile intelligence service have an interest in the research and development activities of the type conducted at HDL. However, the amount of significant information surfaced by the ICIP does not warrant the expenditure of manhours at this time to continue the ICIP.

(4) The MI Group is reviewing the ICIP with a view of terminating the program and instead implementing an overt direct support counterintelligence program.

f. Recommendation: That the ICIP CENTAVO KID be terminated and an overt direct support counterintelligence program be implemented.

REGRADED UNCLASSIFIED
ON
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

554

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
Headquarters, 902d Military Intelligence Group
Fort George G. Meade, Maryland 20755

902d MI Group Pamphlet
No. 381-3

22 April 1976

Military Intelligence

DIRECT SUPPORT COMPREHENSIVE COUNTERINTELLIGENCE PROGRAM (DSCCP) (U)

1. (U) REFERENCES: See APPENDIX A.

2. (U) PURPOSE: This pamphlet establishes policy, guidance, and standardized procedures for the conduct of all-source, multi-discipline counterintelligence support within the 902d MI Group's area of operation.

3. (U) GENERAL:

a. The Commander, 902d MI Group, has the responsibility to notify commanders of Army installations and units in the group's area of operation when:

(1) Any situation or condition exists that poses a threat to the internal security of that Army element.

(2) Any situation exists that might adversely affect the commander's capability to perform his mission.

(3) Information indicates a probable employement of military resources to counter a threat to the installation.

In order to acquire information of situations or conditions that may pose a threat to the supported commander, field elements must aggressively seek it and not wait for it to be reported through normal sequence of events. This is particularly essential for those units/installations declared to be critical sensitive.

b. The DSCCP is one of a series of graduated intensity counterintelligence programs designed to provide the proper coverage based on the security vulnerability of a particular installation. In relationship to other graduated counterintelligence programs listed in USAINTA Regulation 381-100, the DSCCP would, in certain instances, serve as a means of identifying the need for programs of greater intensity such as SVAs, or SAVEs, or, in other instances, may serve as follow-up support subsequent to such intensified services. It provides the broad spectrum of coverage to include a multi-discipline approach with provisions that the information gathered be reported expeditiously to the responsible commander. The program systematically focuses on providing threat information on the most critical area within the target installation in order to provide the required information to the supported commander.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

555

CLASSIFIED BY: CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY: 2
DECLASSIFY ON: 31 DECEMBER 2000

~~CONFIDENTIAL~~

c. This program is not synonymous with, nor is it identifiable with, the Internal Counterintelligence Program, Special Operations as defined in FM 30-17A, or the Special Covert Operational Personnel Insertion (SCOPI) as defined in USAINTA Regulation 381-100.

4. (U) CONCEPT:

a. The Direct Support Comprehensive Counterintelligence Program (DSCCP) is an overt, dedicated counterintelligence security support program with the objective of detecting or anticipating situations and factors from any source (HUMINT/SIGINT/PHOTINT) which are or may become detrimental to the security posture of the supported installation. It employs a Direct Support Special Agent (DSSA) in an overt continuous role of acquiring information and providing it to the commander in a timely manner, while concurrently providing sound recommendations for the reduction and/or elimination of security hazards, vulnerabilities, or threats posed by hostile factors.

b. The DSSA obtains the required information from overt investigative activities and from a number and variety of sources and contacts within and in the vicinity of the supported installation. Confidential sources are not utilized. He is fully supported in this task by the intervening echelons at Field Offices, Group, and USAINTA.

c. The DSCCP is a complementary service provided to the supported commander to assist him in improving the security posture of his installation. It is not intended to duplicate nor to usurp the functions and responsibilities of the G-2 or of the Security Manager.

5. (U) RESPONSIBILITIES:

a. The Commander, 902d MI Group, is the approving authority for all DSCCP operations conducted within the group's area of operation.

b. The S3, 902d MI Group is responsible for the following:

(1) Coordinating the selection of units/installations as candidates for DSCCP with the appropriate USAINTA staff elements.

(2) Monitoring DSCCP operations on a continuing basis and periodically informing appropriate USAINTA staff elements of their progress.

(3) Conducting an annual review of each DSCCP operation to determine if it is still necessary and if so, to asure that it remains viable.

c. Field Office Commanders are responsible for the following:

(1) Initiating proposed DSCCP operations for installations located within their areas of operation.

(2) Conducting DSCCP operations within their area after approval by the Group Commander and coordination with the supported commanders.

(3) Designating the DSSA for each DSCCP operation, providing follow-up support, and arranging for DSSA clearance and access to compartmented information as required.

(4) Briefing of the supported commanders on the results of DSCCP operation at regular intervals per mutual agreements.

(5) Establish procedures to maintain continuity of the program during absences of the DSSA. When possible, an alternate DSSA will be assigned.

6. (U) PROCEDURES AND SCOPE:

a. (U) The designation of installations or Army elements as candidates for the DSCCP will be a coordinated action between the Field Office Commander and the supported commander. In some cases, the action may be directed by the Group Commander or USAINTA following a request for special counterintelligence support from a major commander. Regardless of the origin of the request, DSCCP operations will always be conducted with the full consent and knowledge of the supported commander.

b. (U) The selection of installations to be considered for the DSCCP must be discriminatory and based on a genuine need for this manpower intensive service in order to avoid over-commitment of assets. The target installation must be one that is on the ACSI Sensitive Installation and Unit List (SIUL) and one that is a potential or actual target of hostile intelligence services. It is recognized that some field offices and resident offices have numerous sensitive installations in their area, many of which may be categorized as critical. Therefore, it is essential that each FO/RO maintain a listing of these installations in order of priority. In determining the order of priority, factors such as mission sensitivity, and impact of compromise on the security of the United States, etc., will all have to be analyzed and a value judgement must be made based upon actual knowledge of the local conditions, as to which installation has a greater need for special support. The installations heading the list will get first consideration.

c. (U) Proposed concept will be submitted to the Group Commander by letter for approval. The letter will indicate the installation commander's concurrence in the program. The concept will contain a listing of missions, sensitivities, and those internal and external factors which may pose a threat to the installation. Vulnerabilities to human sources,

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2053 of 3957

[redacted]

communications intercept, overhead and ground photography, and other appropriate technical/scientific factors will be included if known. This information will be extracted from the target analysis (Para 7a) or from the SVA if one has been completed. The concept must address actions to be taken to detect and counter these threats.

d. (U) Occasional expenditures of ICF in support of this program is authorized and will be processed in compliance with the provisions of AR 381-141 and USAINTA Regulation 381-1. Recurring expenditures will be supported by a formal request for authority if such expenditures are anticipated.

e. (U) The conduct of investigations of and storage of information concerning persons and organizations not affiliated with the Department of Defense are prohibited unless authorized under the provisions of AR 380-13.

7. (U) GUIDELINES:

The actions listed below are considered to be minimum essential for the implementation of this program and are not to be considered as all-encompassing. They should be modified as appropriate to meet situations and needs peculiar to the supported installation. Common sense and experience will likely dictate additional or supplementary means to be employed in order to successfully attain the objective.

a. (U) Conduct a target analysis of the unit/installation to identify, in order of priority, the most critical and vulnerable areas and the multi-discipline threats to which they are exposed. Reference will be made to the following: USAINTA Security Support Bulletins, "THREAT" Manuals, completed SVA/SAVE Reports, CI Survey and Inspection Reports, FBI/MP Crime Statistics and Incident Reports, and Communications Security Reports, when available and applicable. The original copy of the analysis will be maintained at the FO/RO level. Appropriate data will be extracted and included in the initial Quarterly Progress Report. The analysis should be reviewed and updated periodically in subsequent Quarterly Progress Reports.

b. (U) Assign a mature, experienced MI Special Agent as a Direct Support Special Agent (DSSA) to provide all-source direct support to the supported commander or his designated representative. The DSSA must become intimately knowledgeable of the supported command's mission, functions, security status and vulnerabilities. As the program will be overt in nature, the DSSA will be known as the primary USAINTA point of contact to all within the supported units/installations. The DSSA will require a TOP SECRET clearance and an SI/SAO special access.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

c. (U) The task of the DSSA is to develop a sufficient number of sources of information to provide the best possible coverage to the unit/installation and personnel of the element to detect security vulnerabilities, and make sound recommendations for their reduction and/or elimination. The DSSA should work closely with the security manager to coordinate appropriate matters and to avoid duplication of effort. However, care should be taken not to duplicate or usurp functions and responsibilities rightfully assigned to the security manager.

(1) Human sources of information will include Conventional Sources (Incidental, Casual, and Official) and Liaison Contacts as described in Chapter 6, FM 30-17. Confidential Human Sources will not be utilized. Anonymity may be provided through the provisions of the Privacy Act of 1974 when the source so requests. The association between the DSSA and Conventional Sources or Liaison Contacts will not normally be classified.

(2) Maximum use will also be made of Documentary and Technical/Materiel Sources to include, but not be limited to, SATRAN Messages, Department of the Army intelligence publications and/or bulletins; USAINTA Security Support Bulletins and "THREAT" Manuals; SAVE/SVA reports; Military Police Reports, and Serious Incident Reports. Special attention should be paid to message traffic concerning alerts, advisories or warnings concerning events or situations affecting the supported command.

d. (U) A contact card file will be maintained at the supporting office to identify conventional sources and liaison contacts. This file will be integrated into the existing contact card file already established for use in the routine mission of the FO/RO. It must be readily available for DSSA personnel at all times. Individual cards will be annotated when the contact is in support of a specific DSCCP operation. LACs will be conducted on casual sources with the results reflected in the contact card file.

e. (U) Consideration should be given to conducting a systematic review of the dossiers of personnel occupying key and sensitive positions to insure that all such personnel have been properly cleared and to determine if unresolved security matters exist. This issue will be discussed with the supported commander if such a review is deemed necessary, the DSSA should recommend that the commander undertake the action. If the commander requests that the review be conducted by the DSSA, then the matter will be referred to group headquarters where resolution will be made in conjunction with the appropriate USAINTA staff elements. The DSSA may assist the supported command in the review of dossiers but may not take any investigative action to resolve issues. He will advise the supported command to submit requests to USAINTA whenever investigative action is indicated.

[redacted]

Page 2055 of 3957

f. (U) ~~(C)~~ Reporting of Information:

(1) (U) To the local commander: Information of counterintelligence interest affecting the security posture of the unit/installation will be reported to the supported commander or his designated representative in a timely and complete manner. The information may be reported orally, by Agent Report format, or by Summary of Information (SOI) format, as appropriate. While most items of information will be passed on an oral basis only, there may be certain instances when the commander will desire written reports from the DSSA to be later attached as backup information to his Request for Investigation. In these instances, APRs containing the adverse allegation may be passed when the full consent of the sources of the information has been obtained. However, when a source of information desires confidentiality, to protect the source, the DSSA can then pass in the information only on an oral basis or by SOI format. Regardless of the manner in which the information was passed to the supported command, a report of the information provided to the supported command will be summarized in the Quarterly Progress Report to this headquarters with an indication of the actions taken by the supported command (see Para 7h below).

(2) (U) Other: Information of counterintelligence interest to the intelligence community or other agencies will be reported in accordance with established procedures utilizing normal reporting vehicles such as oral reports, Agent Reports, Spot Reports or Summaries of Information as appropriate. Information reports will be classified according to their content. Such reports will indicate when and to whom the information was passed and what action the command has taken or plans to take. Subject blocks, special warning notices and Privacy Act caveats, etc., will be those utilized in established investigative activity procedures. (AR 381-20 and USAINTA Reg 381-100).

(3) (U) When fragmentary information of counterintelligence interest is initially surfaced, the DSSA will attempt to determine whether or not the information is credible prior to reporting it to the supported Commander. Preliminary checks may be made only to the extent authorized in para 3-6, USAINTA Reg 380-100. Should this prove to be insufficient to establish the credibility of the information, the DSSA will then refer the matter to group headquarters for coordination with USAINTA. Credible information concerning a member of the supported command should be used to support a formal Request for Investigation to USAINTA.

(4) (U) The supported commander or his designated representative will be orally briefed on all items of threat information concerning his command, or be provided written reports as appropriate. Examples of the types of threat information include satellite overflights, Soviet bloc

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

22 April 1976

country commercial overflights, communications intercept capabilities/ vulnerabilities from air, ground or water, personnel security vulnerabilities and others as listed below. Depending upon the source of the information and its previous distribution within the intelligence community, the information may be passed laterally or to higher echelons in accordance with established reporting requirements. All information gleaned from the operation will be briefly summarized in the Quarterly Progress Report.

g. (U) A list of EEI will be developed by the DSSA in order to focus specialized coverage on the specific requirements of the local situation and the supported commander. Examples of EEI are attached at APPENDIX B. It should be noted that the EEI contain items of specific interest to the supported commander and other items that pertain to lead material for use by the US Army intelligence community. A copy of the developed EEI list will be attached to the initial Quarterly Progress Report.

h. (U) A Quarterly Status Report in the format contained at APPENDIX C will be submitted to Group Headquarters no later than 10 working days following each calendar quarter. The first report will be due after the completion of the first full quarter of operation after initiation. The report should reflect the developments and progress of the operation, problems encountered, information obtained during the reporting period, future actions contemplated and lessons learned or recommendations as appropriate.

8. (U) Reducing Vulnerabilities: Once a security weakness or hazard has been identified, the DSSA then has the responsibility to make sound recommendations for corrective actions to be taken by the supported commander to reduce or eliminate them. In making these recommendations, the DSSA must use good judgement based upon his background and experience, cost verses absolute security, knowledge of similar instances, common sense, and an intimate knowledge of those technical and/or specialized security services and/or investigations available to the supported commander from other USAINTA elements. Each corrective action must be viable, made on its own merit, be practical and be within the capability of the supported command. USAINTA Security Support Bulletins contain excellent examples of "quick-fix" solutions. In those rare instances when corrective actions cannot be accomplished due to cost restrictions or limited resources available to the command, the commander must be made aware of, and accept the possible security risk(s) involved.

9. (U) It is visualized that situations, incidents or conditions may be uncovered which could have serious deleterious effect on the security

REGARDED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

posture of the installation and could not be resolved through the techniques of the DSCCP. In these cases, the matter should be expeditiously referred to Group Headquarters where it will be brought to USAINTA's attention for resolution, considering JCIPs, SCOPEs, Special Operations, or other more sophisticated methods.

10. (U) The application of the DSCCP to a supported installation is a special effort and will probably require the services of the DSSA on a near full time basis with additional manhours of support furnished by FO and Group Headquarters. Consequently, FO Commanders and RO SAICs should proceed with caution in offering this service to commanders to prevent over-extending their resources. Nevertheless, the DSSA approach of the DSCCP is sound and could well be applied to other installations in the area of operations but to a much lesser degree than in the DSCCP. This should be done as a routine matter and no formal approval is required. Thus, one MI Special Agent could become the DSSA to several installations of lower priority.

11. (U) This pamphlet provides policy and guidance for 902d MI Group personnel in the conduct of all-source, multi-disciplined counterintelligence support within the area of responsibility of the 902d MI Group. It complements existing US Army Regulations, USAINTA Regulations and USAINTA policy and guidance. Nothing in this pamphlet shall be construed to contravene or to be in conflict with existing US Army or USAINTA policy. In the event that possible conflicts may arise, the provisions of existing US Army and/or USAINTA policy will apply. Any questions pertaining to possible conflict of the provisions of this pamphlet with existing policy will be addressed to this headquarters, ATTN: MIIA-GPS-AC, for further staffing with appropriate USAINTA staff elements. Comments and recommendations are encouraged and should be submitted on DA Form 2028 (Recommended Changes to Publications) to this headquarters for consideration and staffing.

HASSEL L. PARKER
Colonel, MI
Commanding

3 Incl
Appendix A - References
Appendix B - EEI
Appendix C - Quarterly Report

DISTRIBUTION:
B plus
10-S3, 902d MI Group
1-MIIA-SO
1-EARCOM LNO
1-USASA LNO
1-USAINSCOM LNO
1-Cdr, 525th MI Group
1-MIIA-ADM
2-MIIA-CI
1-MIIA-IN
1-USACC LNO
1-HSC LNO
1-TRADOC LNO
1-Cdr, 901st MI Det

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

562

APPENDIX A TO 902D MI GROUP PAMPHLET 381-3

REFERENCES

1. Army Regulations:

a. AR 18-7, Army Information and Data Systems, Data Processing Installation Management, Procedures, and Standards.

b. AR 190-13, the Army Physical Security Program

c. AR 340-21, Office Management, The Army Privacy Program.

d. AR 380-5, Security, Department of the Army Supplement to DOD 5200.1-R (DODISPR).

e. (C) AR 380-10, Department of the Army Policy for Disclosure of Military Information to Foreign Governments (U).

f. AR 380-13, Security, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations.

g. AR 380-150, Access to and Dissemination of Restricted Data.

h. (S) AR 381-3, Signals Intelligence (SIGINT) (U).

i. AR 381-11, Military Intelligence, Threat Analysis.

j. AR 381-12, Subversion and Espionage Directed Against US Army and Deliberate Security Violations (Short Title: SAEDA).

k. (C) AR 381-12-1, Processing of SAEDA Incidents (U).

l. (C) AR 381-14, Counterintelligence - Technical Surveillance Countermeasures (U).

m. (C) AR 381-15, Military Intelligence, Domestic Exploitation Program (U)

n. AR 381-20, Military Intelligence, US Army Counterintelligence (CI) Activities.

o. (C) AR 381-141, Military Intelligence, Provisions for Administration, Supervision, Control and use of Intelligence Contingency Funds (ICF) (U)

563

A1

p. (C) AR 530-1, Operational Security (U).

q. (C) AR 530-2, Communications Security (U).

r. (C) AR 530-3, Electronics Security (U).

s. (C) AR 530-4, Control of Compromising Emanations (U).

t. AR 604-5, Clearance of Personnel for Access to Classified Defense Information and Material.

u. AR 604-10, Military Personnel Security Program.

2. DOD Publications:

a. DOD 5200.1-R, Information Security Program Regulation.

b. (SI) DOD 5200.1F (M-2) Special Security Manual

c. DOD 5200.28-M, ADP Security Manual

d. DOD 5220-22-M, Industrial Security Manual for Safeguarding Classified Information.

e. DIAM 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities.

3. Field Manuals:

a. FM 19-30, Physical Security.

b. FM 30-17, Counterintelligence Operations.

4. ACSI, DA Publications.

a. OACSI Sensitive Installation and Unit List (SIUL).

b. AARGRAMs (as applicable).

5. USAINTA Publications.

a. USAINTA Reg 10-2, Organization and Functions Manual.

b. (C) USAINTA Reg 381-1, ICF (U)

c. USAINTA Reg 381-100, Counterintelligence Activities and Procedures.

d. (S) USAINTA Security Support Bulletins (U).

564

A2

e. (S) USAINTA Security Support Program Manual "THREAT" (U)

f. (C) USAINTA Security Support Program Manual "Operations" (U)

g. USAINTA Security Support Program Computer Security Manual.

h. USAINTA Daily Operational Reports (as applicable).

i. USAINTA Supplement to AR 380-5.

6. 902d MI Group Publications:

a. (S) 902d MI Group Pamphlet 380-2, Security, SATRAN Reports (U).

b. 902d MI Group Daily Operational Reports (as applicable).

Page 2061 of 3957

APPENDIX E TO 902D MI GROUP PAMPHLET 381-3

ESSENTIAL ELEMENTS OF INFORMATION (EEI)

1. (U) GENERAL: In devising EEI applicable to the supported installation, each one of the multi-discipline threats must be examined in conjunction with the mission and situation of the particular target. The actual or potential vulnerabilities thereby conceived become EEI affecting the supported installation. Since each installation has its own specific situation, it is imperative that the DSSA work very closely with a representative of the supported installation in order to arrive at an EEI listing tailored to the specific needs of the command. The references listed at APPENDIX A provide background information and guidance in devising EEI. Many of the areas covered by these references, which heretofore have been of little concern to the Special Agent, are now essential elements of knowledge to the DSSA if he is to successfully accomplish his mission under the DSCCP concept. This is particularly necessary in the areas of SIGINT, PHOTINT, OPSEC and Computer Security. Listed below are sample EEI for each category. These EEI are basic and are only a partial listing provided as an aid in developing a list peculiar to the supported command. Some of the items may not be germane to every DSSA but are included as nuclei for possible development of new or related ideas. The final EEI list prepared by the DSSA should include the source or sources that can provide the required information.

2. (U) HUMINT: The following elements are those normally attributed to collection or exploitation by human intelligence sources. This information will usually be obtained by various HUMINT sources, personal observation by the DSSA and liaison contacts:

a. HOIS subscriptions or regular acquisition of local and post newspapers and periodicals. Sources: LEO contacts and USAINSCOM.

b. Deliberate compromise of classified information or unauthorized release of military information to representatives of foreign governments (ARs 380-5, 380-10, 381-12 and 381-12-1)

c. Public information releases and local newspaper articles revealing unclassified but useful (to HOIS) information regarding the command.

d. Theft, suspected theft, or unauthorized reproduction of classified documents and or material.

e. Reported or suspected blackmail or coercion of individuals employed within the supported command.

REGRADED UNCLASSIFIED
ON 5 SEP 1997
BY USAINSCOM FOIPA
Auth Para 4-102 DOD 5200.1R

Page 2062 of 3957

CONFIDENTIAL

f. Actual or attempted physical breaches of restricted area perimeter security, external or internal.

g. Early detection of persons whose activities and/or character weaknesses may render them vulnerable to hostile intelligence exploitation. Suitability factors may include:

(1) Excessive indebtedness or recurring financial difficulties.

(2) Unexplained affluence.

(3) Conduct rendering the individual vulnerable to pressure, such as homosexual, criminal or immoral acts.

(4) Excessive use of alcoholic beverages or improper use of drugs or narcotics.

(5) Mental or emotional instability or history thereof.

(6) Those who attempt to commit suicide.

(7) Drastic changes in behavior to indicate possible unexplained pressures being brought to bear.

h. Personnel who regularly and voluntarily work during non-duty hours when unobserved access to classified data is possible.

i. Sudden unexplained or inadequately explained absences from work.

j. Membership in, or association with members of organizations constituting a local threat against the US Army as defined in AR 380-13.

k. Unsolicited correspondence from individuals, organizations or addressees known to be a threat to the US Army.

l. Allegations or denunciations of espionage or sabotage on the part of sensitive installation personnel.

3. (U) PHOTINT: This pertains to intelligence obtained by means of photography, mainly through HOIS satellites or HOIS commercial aircraft. Also included must be threats posed by hand-held cameras operated from low-flying private aircraft and ground-level photography conducted from areas outside the perimeter of the installation. Photography from sea-borne platforms should be considered at installations located near international waters. Sources of information for this type of data are documentary sources such as SATRAN messages, schedules of tests, operations and troop movements, as well as results of liaison contacts and personal observations. Some sample EEI are as follows:

REGARDED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

CONFIDENTIAL

Page 2063 of 3957

a. Following activities during periods of scheduled overflights by HOIS satellites and commercial aircraft:

(1) Large and significant training exercises.

(2) Testing of equipment and/or techniques in the open.

(3) Uncamouflaged new or sensitive equipment.

(4) Other significant movements and activities.

(5) Concentration of transportation equipment, i.e., transports, etc.

b. Build up of major item stockpiles in the open.

c. Gradual build up of facilities at a test site.

d. Repeated violation of air restricted zones by commercial/private planes.

e. Appearance of private aircraft during classified, or significant tests/demonstrations.

f. Placing, operating or testing of new, significant or classified equipment in areas exposed to the public.

g. Sudden appearance of camera-carrying "tourists" in the vicinity, coinciding with the scheduling of new, unusual and/or classified activity.

h. Unobstructed windows and apertures in areas where classified matters are handled, permitting observation and photography from uncontrolled areas.

i. Foreign vessels, particularly from East Bloc Countries, appearing off-coast of installations near international waters.

4. (U) SIGINT: Signal intelligence is derived from the intercept and analysis of communications, COMINT, and from communications electromagnetic radiations, ELINT. HOIS SIGINT collection against US facilities is accomplished from air-borne, sea-borne, and land-based platforms. HOIS capabilities in this field are described in the USAINTA Threat Manual and additional information as to specific threat to the supported installation may be found in reports of SVAs and SAVEs and/or requested from USAINTA. The field of SIGINT is a very complex and specialized one. Adequate protection of a command/installation from HOIS SIGINT collection requires

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

568

the application of Signal Security (SIGSEC) which includes Communications Security (COMSEC), and Electronic Security (ELSEC). COMSEC measures are applied to telecommunications systems and has four components; crypto security, physical security, transmission security and emission security. ELSEC pertains to protective measures applied to electromagnetic radiations of non-communications equipment and systems to prevent the interception, analysis or exploitation of those radiations by foreign intelligence. The DSSA must become sufficiently familiar with the above subjects in order to recognize vulnerabilities, and know when to recommend a request for technical assistance. References 1h, 1, p, q, r, s, and 5d and e in APPENDIX A will provide additional information. Furthermore, the DSSA must work closely with the staff element having responsiblity for SIGSEC of the supported installation. The EEI selected will be the type that can be fulfilled by human sources, preferably located in communication/electronics work areas. Some EEI common to SIGINT are located in para 1c, Appendix to AR 530-1. Other sample EEI follow:

a. Conducting tests on new or sensitive radars and other non-communication emmitters within range of land based, air-borne or sea-based HOIS ELINT platforms.

b. Installing and operating electrically operated, information-processing equipment which handles classified information without the application of compromising emanations control measures.

c. Poor telephone security to include:

(1) Discussion of classified matters over Autovon and commercial telephone systems.

(2) Discussions of upcoming events which can provide tipoffs to classified activities.

(3) Use of double talk in reference to classified messages.

(4) Reading/quoting verbatim portions of classified matters.

5. (U) OTHER EEI: The following items are of interest to the US Army intelligence community and will be forwarded to this headquarters by Agent Report format for appropriate action. A statement in Agents Notes will indicate if and how the information has been reported through other appropriate channels. As the information will be passed to USAINSCOM for possible exploitation bt the Special Operations Detachment or the Director of Operations as appropriate, the Agent Reports will be classified CONFIDENTIAL-NO FOREIGN DISSEM. Normally this information is not passed to the local commander other than to insure that other proper reporting

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

procedures are being followed by the command.

a. Identification and extent of foreign contacts of military and DOD civilian personnel, with emphasis on Soviet bloc countries.

b. Intended foreign travel of military or DOD civilian personnel to Soviet bloc countries or attendance at social or official functions at which Soviet bloc countries are present.

c. Foreign business or professional connections and the extent thereof of military and DOD civilian personnel and their families, with emphasis on Soviet bloc countries.

d. Solicitation by foreign national or organizations of personal or official information through official or unofficial channels.

e. Invitations by non-US Government organizations or individuals to members of the supported command to participate in conferences or symposia or to submit papers for publications in professional journals on activities related to their government employment.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

570

APPENDIX C TO 902d MI GROUP PAMPHLET 381-3

DSCCP QUARTERLY PROGRESS REPORT

1. (U) IDENTIFY: (Name of 902d MI Group Field Element providing support).

2. (U) SUPPORTED COMMAND: (The activity(ies) receiving the support and the major command(s) involved.)

3. ( ) TARGET ANALYSIS: (In the initial report summarize the results of target analyses conducted for all activities, installations, or separate elements designated and included in the program, by order of priority of support. Subordinate elements large enough to be designated sub-targets will be listed in subparagraphs. In subsequent reports, indicate only changes as they occur.)

4. ( ) QUARTERLY BRIEFING OF SUPPORTED COMMAND

a. Circumstances: In brief narrative form, cite date(s), identities of all persons present, and subjects discussed and results of the briefing(s).

b. Recapitulation of Operational Progress During the Period: In as many subparagraphs as may be required, cite significant developments as pertain to development of the program, improvements in target coverage, and any operational readjustments made during the period. In citing specific items of interest, identify each by making reference to the appropriate reports made during the reporting period which contained details of the topic discussed with the commanders, if applicable.

c. Significant Counterintelligence Information Developed: In as many subparagraphs as may be required, cite identities of personalities, incidents, or groups discussed with reference to the report previously submitted.

5. ( ) INFORMATION SUBMITTED:

a. To the local commander and actions implemented or taken as a result:

Subject	Type Information Developed	Action Taken	Date of Action

b. To the intelligence community:

Subject	Type Information Developed	To whom reported

6. ( ) COMMENTS, REMARKS AND RECOMMENDATIONS:

In this paragraph, indicate any general remarks or indications of special

571

Page 2067 of 3957

interest shown by the supported command that are not covered in above paragraphs. These remarks should reflect the commander's assessment of the viability of the program, whether it is meeting the objectives and achievements as he sees them, and any problems and/or recommendations. Also indicated the extent with which the commander or his representative has cooperated with the FO/RO and/or this group and any pertinent remarks which could serve to improve the DSCCP support to the command. Where problem areas have been encountered, findings and recommended solutions will be provided. Lessons learned should be included to assist in the planning and implementation of other operations. A statement will be entered as to whether any information concerning non-affiliated DOD civilians or organizations was reported (AR 380-13). If affirmative, reference specific report or attach copy. Utilize subparagraphs to explain or amplify information or data reported.

NOTE: Classify each paragraph according to its content. Because of the distribution of this report, care must be taken to insure that the contents of the report do not reveal SI/SAO access material. An example of this would be to include the Statement "three items of PHOTINT information, reference messages _____, _____, and _____, were received and passed to the supported command. Appropriate actions were taken", without revealing the SI/SAO information contained within the reference messages.

572

Page 2068 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

MIIA-SO-SA

JUN 25 1976

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

HQDA (DAMI-DOH/Miss Brannan)
WASH DC 20310

1. (U) References:

a. Letter, MIIA-SO-SA, USAINTA, subject: Report of Internal Counterintelligence Program (ICIP) Operations (U), 11 May 76.

b. Letter, DAMI-DOH, subject as above, 8 Jun 76.

2. (U) Recommendations concerning the current four active ICIP operations are submitted in compliance with paragraph 3, reference 1b.

3. (U) The 902d MI Group requested that its sole remaining ICIP at Aberdeen Proving Ground, GONDOLA STAR (U) be terminated effective 30 June 1976. Confidential sources utilized in the ICIP have been terminated. Supported commanders at Edgewood Arsenal and Aberdeen Proving Ground were briefed on the termination of the ICIP and the concept of direct, overt, all-source counterintelligence support which the 902d will provide under the Direct Support Comprehensive Counterintelligence Program (DSCCP).

4. (U) Recommend that GONDOLA STAR be terminated effective 30 June 1976.

5. (U) The 525th MI Group reviewed each of its three active ICIPS, CANVAS TAX (Sierra Army Depot), LENS HOLDER (White Sands Missile Range), and LENTIL MONKEY (Defense Language Institute) for consideration of possible replacement with a program similar to the DSCCP of the 902d MI Group. As a result of this review the CDR, 525th MI Group believes that a program similar to the DSCCP can be established which would provide requisite support to Sierra Army Depot, CA and White Sands Missile Range, NM, which will permit termination of ICIPS at

Classified by CdR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 06

~~CONFIDENTIAL~~

Page 2069 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

MIIA-SO-SA

JUN 25 1976

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

HQDA (DAMI-DOH/Miss Brannan)
WASH DC 20310

1. (U) References:

a. Letter, MIIA-SO-SA, USAINTA, subject: Report of Internal Counterintelligence Program (ICIP) Operations (U), 11 May 76.

b. Letter, DAMI-DOH, subject as above, 8 Jun 76.

2. (U) Recommendations concerning the current four active ICIP operations are submitted in compliance with paragraph 3, reference 1b.

3. (U) The 902d MI Group requested that its sole remaining ICIP at Aberdeen Proving Ground, GONDOLA STAR (U) be terminated effective 30 June 1976. Confidential sources utilized in the ICIP have been terminated. Supported commanders at Edgewood Arsenal and Aberdeen Proving Ground were briefed on the termination of the ICIP and the concept of direct, overt, all-source counterintelligence support which the 902d will provide under the Direct Support Comprehensive Counterintelligence Program (DSCCP).

4. (U) Recommend that GONDOLA STAR be terminated effective 30 June 1976.

5. (U) The 525th MI Group reviewed each of its three active ICIPS, CANVAS TAX (Sierra Army Depot), LENS HOLDER (White Sands Missile Range), and LENTIL MONKEY (Defense Language Institute) for consideration of possible replacement with a program similar to the DSCCP of the 902d MI Group. As a result of this review the CDR, 525th MI Group believes that a program similar to the DSCCP can be established which would provide requisite support to Sierra Army Depot, CA and White Sands Missile Range, NM, which will permit termination of ICIPS at

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by ...Adj Manual...
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 06

~~CONFIDENTIAL~~ - 575

~~CONFIDENTIAL~~

MIIA-SO-SA
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

those locations. Because of the transitory nature of the military community and the makeup of the civilian community at DLI, the present techniques used in ICIP LENTIL MONKEY are believed best suited to provide the necessary support to the commander. LENTIL MONKEY has been very productive under existing operational concepts and should continue to provide significant developments in the future.

6. (U) The 525th MI Group recommends that, based on the above, CANVAS TAX and LENS HOLDER be terminated on 31 Aug 76 at which time a substitute support program will become effective. The 525th MI Group further recommends that, based on the above and the yearly analysis submitted with reference 1a, LENTIL MONKEY be revalidated and permitted to remain in effect.

7. (U) USAINTA concurs in the recommendations of the 525th MI Group.

WILLIAM I. JENNINGS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

576

~~CONFIDENTIAL~~

M. Brennan/DAMI-DOH/53501

~~CONFIDENTIAL~~

~~ROUTING AND TRANSMITTAL SLIP~~ ACTION X

1 TO (Name, office symbol or location) MG Aaron, ~~DAMI-ZA~~	INITIALS	CIRCULATE
	DATE	COORDINATION
2	INITIALS	FILE
	DATE	INFORMATION
3	INITIALS	NOTE AND RETURN
	DATE	PER CONVERSATION
4 SUBJECT: Response to DAMI-ZA question, "Why so much TDY for Canter Ride?"	INITIALS	SEE ME
	DATE	SIGNATURE

REMARKS

1. The Commander, 902d MI Group made the decision that the Project Control Officer (the individual who handles the sources) for Canter Ride be located at HQ 902d MI Group at Fort Meade, Maryland, and not at Redstone Arsenal.

2. The Operations Plan for Canter Ride specifically specified funding for the Project Control Officer to be located at Fort Meade, Maryland. The OPLAN was approved at this level.

3. The Commander's decision undoubtedly based on sensitivity of certain activities of employees at MICOM.

~~CONFIDENTIAL~~

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM (Name, office symbol or location) COL WEISS 577 Chief, DAMI-DOH	DATE
	PHONE 74087

OPTIONAL FORM 41 5041-101-01
AUGUST 1967
GSA FPMR (41CFR) 101-11.206

* GPO 1973 O-498-218

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

REGRADED UNCLASSIFIED ON BY CDR USAINSCOM FOIPO AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 2 June 1976

ACTION REQUIRED: To obtain approval of the Quarterly ICIP Report.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) Background: On 8 Feb 72, the Under Secretary of the Army requested that the VCSA provide a quarterly report on all ICIP operations. On 1 Apr 76, the Under Secretary of the Army requested, "On next quarter's review, please provide an analysis (of each ICIP for the past year) to include statistics." (TAB B).

2. (U) Discussion:

-- During the 3d Quarter two ICIP's were terminated, CANTER RIDE at Redstone Arsenal and CANARY EFFORT at Fort Ritchie. USAINTA will continue to provide overt CI support to these installations.

-- At close of 3d Quarter, seven ICIP's were active. Summaries of each ICIP, plus the two which were terminated, attached as Inclosure 1, TAB A.

-- In compliance with the Under Secretary's request, an analysis of each ICIP for the past year is attached as Inclosure 2, TAB A. Attached as Inclosure 3, TAB A, are the statistics for the ICIP's referred to in Inclosure 2.

-- USAINTA recommended in May 76 that three more ICIP's be terminated: CANINE PLATE (U) at Seneca Army Depot, CENSUS TIME (U) at Pentagon Telecommunications Center, and CENTAVO KID (U) at Harry Diamond Laboratories. Formal ACSI termination is being handled by separate action. (Decision: 6 Jun 76) Remaining four to be presented to ACSI by 26 Jun 76.

-- Information Memorandum at TAB A transmits summaries of ICIP operations through the VCSA to the Under Secretary of the Army for third quarter FY 76.

3. (U) Recommendation: That the Information Memorandum at TAB A be approved and signed by the ACSI.

Why so much TDY for Canter Ride?

(Continue on plain bond)

IMPLICATIONS	CMPO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR	[illegible]	8 Jun 76
			DIV	[illegible]	"
			BTR	[illegible]	"
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

ACTION OFFICER (Name, grade, phone and signature)
Mildred Brannan 578
M. Brannan/GS-13/53501

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~ 232-76

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

REPLY TO ATTENTION OF: DAMI-DOH

16 JUN 1976

MEMORANDUM THRU: VICE CHIEF OF STAFF, US ARMY

FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) (U) -- INFORMATION MEMORANDUM

1. (U) During the 3d Quarter, January-February-March 1976, two of the on-going ICIP operations, CANTER RIDE at Redstone Arsenal, Alabama, and CANARY EFFORT at Fort Ritchie, Maryland, were terminated effective 31 March 1976. Although these operations were terminated, the United States Intelligence Agency will continue to provide overt counter-intelligence support to the sensitive elements at Redstone Arsenal and Fort Ritchie.

2. (U) The total number of active ICIP operations at the close of the 3d Quarter was seven. Summaries for each of these operations, plus the two which were terminated, are attached as Inclosure 1.

3. (U) The Under Secretary of the Army commented on our 1 April 1976, 2d Quarter ICIP Information Memorandum that an analysis of each ICIP operation for the past year, to include statistics, be provided with this quarterly review. In compliance with this requirement, an analysis of each ICIP operation has been made for the past year and is attached as Inclosure 2. Also, attached as Inclosure 3, are the statistics for the ICIP operations referred to in Inclosure 2. These statistics provide a recapitulation of pertinent production, costs and manhours for these operations.

4. (U) After reviewing the 2d Quarter ICIP Report, I have directed that three more operations be terminated: CANINE PLATE (U) at Seneca Army Depot, Romulus, New York; CENSUS TIME (U) at Pentagon Telecommunications

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

579

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DAMI-DOH
SUBJECT: Internal Counterintelligence Program (ICIP) (U) --
INFORMATION MEMORANDUM

Center; and CENTAVO KID (U) at the Harry Diamond Laboratories, Adelphi, Maryland. Overt counterintelligence support will continue to be provided these installations by elements of the appropriate Military Intelligence units. Before the end of June 76, the four remaining cases will be reviewed again for retention.

5. (U) Our goal is to assist the Army commander in improving the operations security (OPSEC) posture of his installation through the use of the complete spectrum of counterintelligence services. I am expanding the use of overt counterintelligence services and want to use the ICIP very selectively to ferret out espionage activities of hostile intelligence services.

HAROLD R. AARON
Major General, GS
ACofs for Intelligence

3 Incl
as (C)

DOWNGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Miss Brannan/53501
Typed by: G. Rivera

~~CONFIDENTIAL~~

Page 2075 of 3957

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

(U)

1. ~~(C)~~ CANARY EFFORT: (OACSI Revalidation - 4 Feb 75)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) On 15 January 1976, the Project Liaison Officer (PLO), as a result of a liaison visit with the Baltimore Division of the Federal Bureau of Investigation obtained data on the presence of Sino-Soviet Bloc personnel travelling within the environs of the target areas and information on those Sino-Soviet Bloc personnel residing temporarily in the environs of the target area.

(2) On 28 January 1976 a member of the 572d Military Police Co, Ft Ritchie, was approached by an unidentified individual at Hagerstown Junior College, Hagerstown, MD, who claimed to be employed at Site R. The individual described Site R in general terms, but made no attempt to elicit information from the soldier. Investigative efforts failed to identify the individual. All available information was provided the Hagerstown Resident Office of the FBI. A USAINTA investigation of the incident is continuing.

(3) On 28 January 1976, an unidentified individual approached a soldier assigned to the US Army Communications Command East Coast Telecommunications Center (USACCECTC) and requested a tour of that facility. The individual appeared interested in the antenna configuration of Satellite Communications/Direct Communication Links (SATCOM/DSL). The request for the tour was denied. All available information was provided the Hagerstown Resident Office of the FBI. USAINTA investigation of the incident is continuing.

(4) During the reporting period information was developed on a Non-Appropriated Fund (NAF) employee who is a bartender employed at the Ft Ritchie NCO Club. The bartender allegedly told the patrons that she was in the employ of both "Military Intelligence" and the "CIA." An investigation is being conducted by USAINTA.

(5) On 18 March 1976, a US Army NCO assigned sensitive duties in the Alternate National Military Command Center (ANMCC) volunteered information concerning his entering into correspondence with an agency of the East German Government. The NCO, who has been researching his family history for the last six years, was attempting to obtain a record of the military service of his great-great grandfather in the period circa 1810. In the course of an inquiry to the Federal Republic of

Classified by Cdr, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652

~~CONFIDENTIAL~~

CONFIDENTIAL

Germany (FRG) Ambassador in Washington and the FRG Government, he was advised to contact the German Historical Central Archives in East Germany. The NCO volunteered the information to make it a matter of official record. He was given a SAEDA briefing under the provisions of AR 381-12 with special emphasis on reporting procedures. The NCO will inform Army Intelligence should he be contacted by any East Germany Agency and will provide copies of any correspondence he receives. At present the exploitation opportunities are unknown, pending any East German Intelligence Service overture. The Chief, ANMCC was briefed on the incident.

e. Operational Status:

(1) In February 1976, the 902d MI Group selected Operation CANARY EFFORT for termination. Supported commanders were briefed on the termination in conjunction with the scheduled quarterly briefings. All confidential sources used in this ICIP have been terminated. The effective termination date for CANARY EFFORT is 31 March 1976.

(2) During the quarter, the PLO presented 21 SAEDA/Threat/Security Awareness briefings to personnel assigned to supported activities at Fort Detrick and Fort Ritchie.

(3) The PLO presented the Quarterly Progress Briefing to LTC Dale S. Cockle, CDR, USACC ECTC, on 30 March 1976.

(4) The PLO, on 1 April 1976, presented the Quarterly Progress Briefing to COL John S. Eberle, CDR, US Army Communications Command (USACC) Site R.

(5) On 5 April 1976, the PLO gave the Quarterly Progress Briefing to the supported command, HQ, 7th Signal Command and Fort Ritchie, with the following officials present: COL Harold G. deMoya, CDR, Ft Ritchie; COL John J. Plosay, Jr., Deputy CDR, Ft Ritchie and Mr. Joseph J. Carroll, Acting Assistant Chief of Staff, Intelligence and Security, 7th Signal Command and Ft Ritchie.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

2. ~~(C)~~ CANINE PLATE (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD), Romulus, NY

b. Confidential Source Utilization: None

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status:

Five conventional sources are contacted on a recurring basis by the Project Liaison Officer (PLO) in this operation; one of these plans retirement in July 1976. One newly contacted official source is in a position to assist in spotting potential new sources. No threat information was surfaced during this quarter. On 5 March 1976 the PLO provided the Quarterly Briefing to LTC Earl Hain, Acting Depot Commander. LTC Hain was designated by COL Alden Cox, CDR, SAD, to receive the briefing during the absence of COL Cox.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

583

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2

~~CONFIDENTIAL~~

3. (U) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal, AL.

b. Confidential Source Utilization: One

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status:

On 18 February 1976, COL Hassel Parker, CDR, 902d MI Group, with the Project Liaison Officer (PLO) in attendance, provided a special briefing on this operation to MG Turnmeyer, CDR, USAMICOM. COL Lange, USAMICOM Chief of Staff, was also present during the briefing. As a result of the briefing, it was agreed by the participants that since the operation had accomplished its objective it should be terminated and the insert source should be extracted to reduce the risk of compromise. The CDR, USAMICOM expressed his deep appreciation for the information provided by the operation and concurred with the suggested termination. The source used in this operation has been debriefed and reassigned. The effective termination date for CANTER RIDE is 31 March 1976.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

584

~~CONFIDENTIAL~~

Classified by C/r, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2026

~~CONFIDENTIAL~~

4. (U) CANVAS TAX: (OACSI Revalidation - 4 Feb 75)

a. Location: Sierra Army Depot (SIAD), Herlong, CA

b. Confidential Source Utilization: Two

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status:

(1) The two confidential sources are providing coverage of the Priority I activities of SIAD which are Exclusion Areas I and II. Two conventional sources and one casual source cover the Priority II activities which are the staff and security organizations of the Depot. One individual assigned to the Special Weapons Section, Exclusion Area II is under assessment as a potential source.

(2) The Quarterly Progress Report for the 2d Quarter, FY 76, which had been postponed at the request of the CDR, SIAD, was presented by the Project Liaison Officer (PLO) on 13 Feb 76 to the following SIAD officials: COL Robert Hawlk, CDR, SIAD; LTC Robert Render, Deputy CDR; MAJ Robert Folster, Security Officer; CPT Wayne Heringer, Intelligence Officer and Mr. Anthony Tornabene, Assistant Intelligence Officer. The following personnel from the 525th MI Group also attended the briefing: COL Donald Bradbury, CDR; LTC Arthur McQueen, Operations Officer, and MAJ Trevor Bissey, CDR, San Francisco Field Office.

(3) ICIP Sources have been tasked to report any significant counter-intelligence EEI or indicators of hostile intelligence activity impacting on Operation Rocking Force (U), a special weapons project presently in progress at SIAD.

(4) The Quarterly Progress Briefing for the 3d Quarter, FY 76, will be presented by the PLO on or about 30 April 1976 to the SIAD officials listed in paragraph 4e(2), above.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

585

~~CONFIDENTIAL~~

Classified by Cdr, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

~~CONFIDENTIAL~~

5. (C) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC

b. Confidential Source Utilization: None

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) The Limited Investigation reported in the last quarter on the PTC NCO who had attempted suicide and allegedly had involved himself in financial troubles, drugs, and homosexuality was completed and referred to PTC for adjudication. The decision was made not to revoke the NCO's security clearance since he left the service on 9 April 1976 and will not be allowed to re-enlist.

(2) During the course of an investigation of an enlisted WAC member of PTC who had a SECRET security clearance and who was Absent-Without-Leave, it was discovered that Criminal Investigation Command (CID), Ft Meyer was also investigating her for theft and trafficking in drugs. The Project Liaison Officer (PLO) and CID agents coordinated their mutual investigations. Drug charges are pending the results of laboratory tests of substances purchased from the WAC by CID informants. PTC has suspended the WAC's access to classified material pending completion of the investigation.

(3) The PLO arranged with appropriate 902d MI Group elements to present formal SAEDA briefings to all PTC personnel, including the PTC elements in the Hoffman and Forrestal Buildings. This project is scheduled for completion in the next quarter.

e. Operational Status:

(1) The Hoffman Telecommunications Center has been brought under coverage of this ICIP, as requested by COL Donald E. Clark, PTC Commander, in the previous quarter.

(2) On 24 March 1976, the PLO presented the Quarterly Progress Briefing to COL Clark, CDR, PTC. CW2 Leonard Gross, Alternate PLO, was also present at the briefing.

Regraded UNCLASSIFIED on
3 Dec 07
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

586

~~CONFIDENTIAL~~

Classified by C4, USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY
DECLASSIFY ON

~~CONFIDENTIAL~~

6. (U) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories (HDL), Adelphi, MD

b. Confidential Source Utilization: None

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) As a follow-up implementation of "Lessons Learned" in the courtesy penetration test conducted at HDL's Adelphi Facility in the previous quarter, the Project Liaison Officer (PLO) and the HDL Security Officer prepared and delivered a series of lectures and classes to the HDL Guard Force on the penetration test. The Guard Force is operating under new instructions designed to thwart attempted penetrations. A new HDL Badge and Pass System, utilizing a magnetic coded badge and a computer control device, will be started in mid-1976.

(2) The PLO delivered lectures on the penetration test conducted at HDL to the faculty and students of the Counterintelligence Dept, US Army Intelligence Corps School, Fort Huachuca, AZ, on 20 and 21 January 1976.

(3) The PLO, assisted by other 902d MI Group personnel conducted several technical inspections at HDL. The PLO provided advice and assistance at several design meetings concerning new buildings at HDL.

(4) Other security advice was provided by the PLO to the Woodbridge Research Facility (WRF), Woodbridge, VA, and the Gaithersburg Test Site (GTS), Gaithersburg, MD. The PLO assisted in devising Operational Security techniques at these sites, the only HDL facilities at which outdoor testing takes place.

e. Operational Status:

On 16 March 1976, the PLO presented the Quarterly Briefing to MAJ Kenneth F. Keller, Executive Officer, HDL, and Mr. James F. Yeick, Security Officer, HDL.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

587

Classified by Cdr, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

[redacted]

7. (U) GONDOLA STAR: (OACSI Revalidation - 11 Jul 75)

a. Location: Aberdeen Proving Ground (APG), and Edgewood Arsenal, Aberdeen, MD

b. Confidential Source Utilization: Eight

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

A confidential source identified an individual in the Biomedical Laboratory, Edgewood Arsenal, as an alien enlistee. Project personnel briefed the appropriate security personnel and a background investigation, to include a polygraph examination, was initiated. The investigation had not been concluded at the close of the quarter.

e. Operational Status:

(1) On 23 March 1976, the PLO presented the Quarterly Progress Report to COL Alvin D. Ungerleider, CDR, APG, on those activities pertaining to the Aberdeen area. Mr. Harry A. Mencke, Installation Intelligence Officer, APG, was present also.

(2) On 25 March 1976, the PLO presented the Quarterly Progress Report on Edgewood Arsenal activities to COL Kenneth L. Stahl, CDR, Edgewood Arsenal, with CPT Vincent J. Falconio, Chief, Security Office, Edgewood Arsenal, also present.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 06

588

[redacted]

~~CONFIDENTIAL~~

8. (U) ~~(C)~~ LENS HOLDER: (OACSI Revalidation - 4 Feb 75)

a. Location: White Sands Missile Range (WSMR), NM

b. Confidential Source Utilization: Two

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) A confidential source reported that unknown persons had attempted on 11 January 1976 to penetrate the TRADOC Systems Analysis Activity (TRASANA). On 12 January 1976, it was reported that an unidentified individual claiming to be a colonel had been permitted to enter the TRASANA Compound. These incidents were reported immediately to the Security Officer, TRASANA. An investigation by TRASANA security personnel disclosed that there was no substance to the 11 January report and the person in the second incident of 12 January was identified and found to be a legitimate entrant into the facility. The incidents did serve to illustrate the security awareness of the source and the personnel involved.

(2) A source surfaced information on 4 February 1976 that two enlisted soldiers at TRASANA were engaged in drug trafficking, but in separate individual operations. Local on-post investigation resulted in apprehension of one of the individuals. All available information on the second individual was reported to the Sixth Region, US Army Criminal Investigation (CID) Command for appropriate action.

(3) A confidential source reported in March 1976 in three reports that such devices as radios, tape recorders, and "pocket" digital calculators were being brought into a TRASANA Exclusion Area by personnel having access to the area. These devices reportedly could affect the computers used in the area, some of which have classified data in storage. The Activity Security Officer has been briefed on these alleged practices and ICIP project personnel have been tasked to provide follow-up reports on action taken by the supported command. The information contained in the reports has been provided to the Counterintelligence Services and SAVE Team elements at USAINTA as a matter of interest.

e. Operational Status:

(1) The two confidential sources provide coverage of TRASANA and the US Army Electronics Command, Office of Missile Electronics Warfare (OMEW), WSMR. One individual assigned to the US Army Missile Test and Evaluation Directorate is under assessment as a potential source.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

589

~~CONFIDENTIAL~~

Classified by [redacted]
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 4
DECLASSIFY ON [redacted]

~~CONFIDENTIAL~~

(2) The Quarterly Progress Briefing, postponed at the request of MG O. L. Tobiason, CDR, WSMR, will be presented during the next quarter.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2085 of 3957

~~CONFIDENTIAL~~

9. (U) LENTIL MONKEY: (OACSI Revalidation - 4 Feb 75)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA

b. Confidential Source Utilization: Eight

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) The female instructor in the Czechoslovakian Language Department reported in the last quarter as preparing to resign her position and return to Czechoslovakia now is reportedly having serious health problems. It is unknown if her health will cause a change in her original plans, and the FBI to date has not indicated whether or not that agency has a continued interest in the instructor or her spouse.

(2) A Polish Language Department instructor plans to visit his mother and a brother in Warsaw in mid-1976, a confidential source has learned. The instructor has submitted no formal request to DLI for the trip yet. The instructor's activities are monitored as a matter of intelligence interest because of his and his brother's travels. His brother, a medical doctor has visited in the US and Canada frequently over the last 20 years and was once detained by US Customs at the Canadian border for attempting to smuggle Communist propaganda into the US. During a 1974 visit to the US, the instructor's brother visited DLI, attended Polish Language Department functions, talked with and photographed the students. USAINTA is monitoring the instructor's activities.

(3) A Czech language instructor is continuing his efforts to obtain the release of his children from Czechoslovakia. A confidential source surfaced the most recent information that the Czech Government has informed the instructor he could get his children out of the country if he pays the Czech Government $66,000. ($6,000 for the cost of his time in a Czech prison and $60,000 as an educational tax on his and his wife's education.) Source did not have further information on this particular aspect, but reported that in mid-February 1976 the instructor gave many of the DLI Czech students a list of newly published books in the Czech language. The books are distributed by a Canadian firm, "Sixty Eight Publishers," Box 695 Station A, Toronto, Ontario M5W 1G2 Canada. The instructor told his classes that the Czech military had officially changed their method of counting for example, using "21" instead of "1 and 20." Insignificant in itself, this last item indicates that the instructor is maintaining ties with Czechoslovakian officials. USAINTA is monitoring the instructor's activities.

REGRADED UNCLASSIFIED
ON · SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

591

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 06

(4) Information developed from official sources during the period disclosed that an instructor of the Russian Language Department (RLD) apparently is suffering from mental problems. The instructor has written letters to a California senator, a nationally syndicated columnist, and the FBI, alleging that he is under surveillance of Soviet and US intelligence constantly and that his life is in danger. The Commander, USAINTA, provided a summary report on the instructor to the ACSI. The instructor later sent a telegram to the President of the United States. Both the FBI and the Secret Service have made inquiries into the matter. On 23 March 1976, the Commandant, DLI, took administrative action directing the instructor to undergo psychiatric evaluation. The instructor refused initially and was administratively suspended from teaching. At the end of the quarter, the instructor agreed to the examination and final disposition of the matter is pending.

e. Operational Status:

(1) As a result of the RLD incident described in d(4), above, the DLI Commandant has directed that the Civilian Personnel Office and Security Office screen records of faculty members for indications of mental problems. Once identified, action will be taken to obtain treatment for the individuals concerned.

(2) Eight confidential sources were utilized during the quarter; three sources were terminated due to graduation. Four new confidential sources were recruited, including one Technical Language Assistant (TLA). Fifteen individuals are under assessment as possible sources, including one instructor and one TLA. In addition to the confidential sources, there are 16 conventional sources providing coverage of seven language departments and the DLI staff.

(3) On 29 March 1976, the PLO presented the Quarterly Briefing to COL Samuel L. Stapleton, Commandant, DLI. Also present at the briefing were COL Donald K. Bradbury, CDR, 525th MI Group; MAJ Trevor Bissey, CDR, San Francisco Field Office, 525th MI Group; CPT Brendon A. Xiques, SAIC, Ft Ord Resident Office, 525th MI Group; and Mr. James Green, Asst Security Officer, DLI.

REGRADED UNCLASSIFIED
ON
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2087 of 3957

~~CONFIDENTIAL~~
~~SECRET~~

ICIP REPORT

1 April 1975 to 31 March 1976

(C) CANARY EFFORT: (OACSI Revalidation - 4 Feb 75)

a. Location: Fort Ritchie, MD

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 April 75 - 31 March 76:

(1) Confidential and conventional sources employed in the operation surfaced information on adverse suitability pertaining to 86 employees at Fort Ritchie, all of whom had security clearances and access to one of the sensitive activities supported. The suitability information included the entire spectrum in this category - alcohol and drug abuse, moral improprieties and mental instability. In these instances investigative action was taken to refute or substantiate the allegations or the individuals were removed from access to classified information. About 50% of the cases reported involved some degree of drug abuse; these were referred to the Criminal Investigation Command (CID) for action.

(2) Two separate reports were received concerning suspected Soviet Intelligence presence and interest in the activities of the supported installation. Details of these reports were provided the FBI in May 1975. In one instance an individual resembling a known KGB agent paid an unusual amount of attention to shipment of sensitive cargo to Fort Ritchie; in the second instance an individual assigned to Fort Ritchie reported that a second person whom he had met claimed to be in contact with the Soviets in Hagerstown, MD. b1 Per FBI

b1 Per FBI

(3) An ICIP source reported a possible compromise occurred when the Telecommunications Directorate, Site R, was tasked to prepare a special test tape containing test messages which could be used for coding and to devise compatibility between two computer systems. The test tape, though it consisted only of innocuous, unclassified messages, also contained fragments of sensitive, highly classified messages which had been picked up from residual magnetism on the reels of the equipment when the messages were recorded. This latter condition was not discovered until processing to make the systems compatible took place, after the tape had lain unsecured, in open storage, for about six weeks. A command investigation of the incident followed and a determination was made that apparently a compromise had not occurred, but as a result of the incident, changed security procedures were put into effect for the handling and storage of computer tapes, reels, and discs.

Regraded SECRET
ON 20MAR98
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

Classified by Cdr USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 4
DECLASSIFY ON 31 Dec 2006

CONFIDENTIAL

(4) Two possible SAEDA approaches to soldiers stationed at Fort Ritchie in January 1976 are currently under investigation by USAINTA and the FBI. Reports of a Fort Ritchie NCO Club bartender professing to be employed by the "CIA" and "military intelligence" are currently being investigated by USAINTA.

(5) In March 1976, an Army NCO assigned sensitive duties at Fort Ritchie volunteered that he had contacted by letter an agency of the East German Government. The NCO desired to make the matter of the contact part of official records in the event he should be later contacted by any agency or person from East Germany. Though the NCO's action was part of his research of his family history and ostensibly is an overt, sincere effort on his part, the East German Intelligence Services (EGIS) often take such opportunities to make intelligence approaches, especially if the US soldier-target has special clearances and access to sensitive information. The NCO is under instructions to report any responses to his letter.

d. Operational Status:

(1) CANARY EFFORT was first approved for implementation by OACSI, DA, on 11 June 1965.

(2) Operation CANARY EFFORT to be terminated effective 31 March 76. Supported commanders were briefed on the termination action during the quarter ending 31 Mar 76. All confidential sources used in the ICIP have been terminated.

(3) b1

(4) The Operation yielded 69 information reports and 116 other reports which were chiefly verbal reports provided to the supported commanders.

e. Comments: The ICIP at Fort Ritchie clearly has been a productive operation at a critically sensitive installation. Information obtained as a result of the ICIP and acted upon by the commanders concerned has served to strengthen the security of the installation. The 902d MI Gruop will continue to provide counterintelligence support to the installation under an overt comprehensive counterintelligence support program.

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(U) CANINE PLATE: (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD), Romulus, NY

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76: There was no significant information obtained during the period and there were no indications of any overt threat to the installation.

d. Operational Status: CANINE PLATE was first approved by OACSI, DA, for implementation on 18 Sep 73. Five conventional sources are contacted on a recurring basis by the Project Liaison Officer (PLO). One official sources is in a position to assist in spotting potemtial new sources. During the last year, the PLO expended a total of 400 manhours in the program. No funds were expended. No information of counterintelligence significance was surfaced in this period. Only conventional sources have been utilized in this operation.

e. Comments: The installation's mission remains the same, a supply depot for missile and artillery weapons systems with a nuclear capability. The Depot is considered a critically sensitive installation and a potential target for HOIS. However, there was no information reported to indicate the presence of any overt threat to the installation.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by CDR, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2000

595

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(b)(1) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal, AL

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76:

(1) An inserted covert confidential source was employed in this operation to attempt to learn the existing situation in the Optical Guidance Technology Office (OGTO), Advanced Sensors Directorate, USAMICOM, when reports received in 1974 alleged that lax security practices had led to loss and possible compromise of classified information and that several employees were engaging in sex orgies in offices during the day. In Sep 74, the CG, USAMICOM, conducted a Command Investigation as a result of these reports under the provisions of Army Regulation 15-6. As a result of that investigation, the CG, USAMICOM, requested that an ICIP operation be conducted in OGTO. The Source, once in place, had to rely chiefly upon elicitation to obtain his information because of his covert status, but during the period, did succeed in surfacing adverse suitability information on a civilian physicist with access to sensitive, SECRET information which indicated that he was probably the catalyst for the sexually-oriented activities of the OGTO employees. The employee, apparently obsessed with sex, had numerous extra-marital relations during the last five years. The Commander, USAMICOM, was provided a summary of information on the employee for appropriate command action. The employee transferred to another office in USAMICOM, which apparently broke up the clique and Source could uncover no new evidence of continuing activities among the remaining employees.

(2) In addition to the above, the Source provided substantial information on security weaknesses in the supported command to include poor housekeeping practices, lack of control of reproduction facilities, lack of proper control of area access, lax security attitudes, and possible compromise of security badges through continued losses by individuals. Source provided such security weakness and hazard details to the Project Case Officer who relayed it to overt MI project personnel at Redstone. The Project Liaison Officer provided these reports to the USAMICOM Commanding General and appropriate security personnel who have taken actions to remedy the security weaknesses.

Classified by: ADC USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
596 EXEMPTION CATEGORY 2
DECLASSIFY ON: 31 DEC 06

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

CONFIDENTIAL

d. (U) Operational Status:

(1) (U) CANTER RIDE was first approved by OACSI, DA, for implementation on 4 Mar 75.

(2) (S) b1

(3) (U) The operation yielded one Summary of Information and several oral reports on security weaknesses.

(4) (U) As the result of an 18 Feb 76 briefing presented to the USAMICOM Commanding General, the MI Group conducting the Operation, the project personnel, and the supported commander concurred in findings that the Operation had accomplished its original objective and should therefore be terminated. The CG, USAMICOM, declared that the operation was a success. The insert Source used in the operation has been withdrawn and reassigned. The CDR, USAINTA, and the ACSI verbally approved the termination of CANTER RIDE on 20 and 23 Feb 76, respectively with an effective date of 31 Mar 76.

e. (U) Comments: Counterintelligence support continues to be provided by elements of the MI Group stationed at USAMICOM.

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(c) CANVAS TAX: (OACSI Revalidation - 4 Feb 75)

a. Location: Sierra Army Depot (SIAD), US Army Materiel Development and Readiness Command (DARCOM) Herlong, CA

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During the Period 1 April 1975 to 31 March 1976:

(1) Reports alleged the use of illegal drugs by military personnel at SIAD. However, no details were available.

(2) Information was reported that an exclusion area personal identification badge was missing and that an inquiry failed to find or determine how the badge was lost. As a result of the missing badge incident, new identification badges were issued.

(3) An enlisted man assigned to SIAD was charged with malicious damage of a generator at SIAD and his security clearance was revoked by the Commander, SIAD.

d. Operational Status:

(1) During the reporting period 616 manhours were expended and 14 Agent Reports were submitted.

(2) TDY funds totalling $29.35 were expended; b1

b1

(3) At the end of the reporting period two confidential sources were being used.

e. Comments:

(1) This ICIP was administratively implemented in April 1974.

598

~~CONFIDENTIAL~~

Classified by C1C, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

~~CONFIDENTIAL~~

(2) The mission of the Sierra Army Depot (SIAD) is the operation of the Depot for the receipt, storage, issue, maintenance, and disposal of missile and artillery weapons with a nuclear capability. Included in the items handled by SIAD are ammunition, special weapons materials, propellants, explosive components of guided missiles, supplies, petroleum and chemical supplies, fire control test and measuring equipment, and other special weapons with a nuclear capability. SIAD also maintains a capability for systems modification in support of the joint AEC/DOD test firing programs.

(3) Sierra Army Depot is the major storage area for special weapons in the western part of the US. The special weapons that formerly were located at the Safeguard anti-Ballistic Missile Site and Savanna Army Depot are now at SIAD, which elevates it to one of the most important special weapons repositories in the US. The Depot is located in a remote area and its contents make it not only of interest to hostile intelligence, but also a target of terrorist groups who are involved in nuclear theft and blackmail.

(4) The Department of Army Sensitive Installation and Unit List, January 1976, lists SIAD as "Critically Sensitive (CS)."

(5) A large portion of the work force is in exclusion areas so access to them on a daily basis is severely restricted for project personnel. Coverage of these areas by confidential sources thus becomes necessary for effective CI coverage. A 20 Sep 75 report of the Nuclear Defense Agency entitled "Adversary View and Support - Nuclear Weapon Site Security; Adversary Capabilities," in assessing terrorist groups tactics employed to acquire a nuclear device and options available, cites the method most likely to succeed as one in which a member of the regular work force has been approached, recruited and is on the terrorist groups payroll. The detection of this type of activity among members of a work force in an exclusion area is greatly enhanced by employing a confidential source program. At the close of the reporting period, two confidential sources were being utilized in the operation to cover the Priority I Exclusion Area. A third individual is under assessment as a potential confidential source.

(6) Hostile intelligence services have high priority collection objectives pertaining to such activities as those conducted at SIAD.

(7) The SIAD, as outlined briefly in subpara (5) and (6), above, appears highly vulnerable to a double threat, that posed by the increasingly active terrorist groups who operate on a global scale and the ever present threat of HOIS penetration. The ICIP is necessary as an additional means to provide "early warnings" to assist the Commander in formulating necessary plans and taking proper action to protect the sensitive and highly-destructive special weapons stored at this location.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(8) At the most recent Quarterly Briefing on 13 Feb 76, the SIAD Commander indicated that he was pleased with the type of support being provided and requested continuation of the ICIP.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

600

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(U) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC.

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During the Period 1 April 1975 to 31 March 1976:

(1) An ICIP source reported that a PTC civilian employee was transferred from the coding and decoding section because he had coded an obscene message that was to be sent to an overseas user. Additionally, the ICIP source provided information concerning possible security violations involving the employee. Because of the employee's questionable suitability characteristics and conduct he was assigned to a job in PTC requiring minimum contact with classified information. Supervisors will continue to monitor his conduct and activities.

(2) An Army NCO assigned to PTC attempted to commit suicide by slashing his wrists. As a result of the information gained concerning the suicide attempt a Limited Investigation was initiated. The NCO was assigned to the Logistics Branch, PTC, pending results of the investigation. The investigation revealed that the NCO has a large number of outstanding debts, has lied on loan applications, and had ordered a 1976 automobile which cost in excess of five thousand dollars. Interviews concerning the NCO revealed alleged drug usage and homosexuality. The Limited Investigation was completed and referred to PTC for adjudication. The decision was made not to revoke the NCO's security clearance since he left the service on 9 April 1976 and will not be allowed to re-enlist.

(3) Adverse suitability information was reported on two additional NCOs assigned to PTC. Based on medical reports and rebellious attitudes one NCO was released from the Army by board action. The second NCO after a night of heavy drinking began hitting his wife when she tried to arouse him after he had "passed out." The wife filed assault charges with the Military Police but withdrew them later. The PTC commander counselled the NCO on his drinking and marital problems and assigned him duties where he has no access to classified information.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by ODR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 06

601

~~CONFIDENTIAL~~

CONFIDENTIAL

(4) During the course of an investigative of an enlisted WAC member of PTC who was absent-without-leave (KAWOL Investigation), it was discovered that the CID was also investigating her for theft and trafficking in drugs. The MI representative and CID agents coordinated their mutual investigations. PTC has suspended the WAC's access to classified material pending completion of the investigation.

d. Operational Status:

(1) CENSUS TIME was first approved by OACSI, DA, for implementation on 5 Feb 74.

(2) During the period of 1 April 1975 to 31 March 1976, 726 manhours were expended, no TDY or ICF funds were used. The operation produced seven information reports. One confidential source was used during the period but was terminated during the latter part of the period.

e. Comments: The PTC operations include an extremely high volume of ultra sensitive classified traffic processed at the highest level, and includes the cryptographic support rendered to the JCS, the NMCC, departments and executive agencies of the government, allied embassies, and the United Nations Building in New York. The PTC remains a potential target for HOIS; however, there is no information reported to indicate the presence of any identified threat to the installation.

Regraded UNCLASSIFIED on
3 Dec 07
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

CONFIDENTIAL

Page 2097 of 3957

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(C) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories, (HDL)), Adelphia, MD

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 - 31 Mar 76:

(1) Information was received that a First Secretary at the USSR Embassy, Washington, DC had visited HDL on two occasions. On one occasion he attended a meeting of the Institute of Electrical and Electronics Engineers, INC., a professional society for engineers which was held in the auditorium of HDL. The subject matter presented during the meeting was unclassified. At a second meeting of the society the Soviet Embassy official was denied entry. A report of the incidents were provided to the FBI and the Commander, HDL, made a determination that the society could no longer hold meetings at HDL in order to preclude any potential security threat.

(2) On two occasions an unidentified light aircraft flew over the test site, Woodbridge Research Facility (WRF), HDL, where a series of tests on foreign equipment under the Range Emory program was in progress. In both instances the aircraft circled over the Range Emory test cite for about 5-7 minutes. The overflights are being investigated in coordination with the FBI.

(3) An employee, HDL, made allegations of immoral activities by members of the HDL Security Office and a group at the Van Ness Avenue Facility, HDL. The employee claimed that she was being followed by members of the HDL Security Office. After investigating the employee's story, the Commander, HDL, believed that she was suffering from psychiatric problems and would have her visit a psychiatrist for a complete evaluation.

(4) Suitability information concerning an employee of the Woodbridge Research Facility (WRF) a branch of HDL located in Woodbridge, VA, involved a problem of alcohol abuse. After counseling, the employee participated in a rehabilitation program.

Classified by: ODR USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON: 31 DEC 06

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~ 603

CONFIDENTIAL

(5) From 7 October to 6 November 75, a courtesy penetration test of HDL's Adelphi Facility was conducted. The penetrations were successful and revealed several security weaknesses which were corrected by the supported command. As a result of the test a number of security guards were transferred and guard procedures were changed. In addition a new magnetic coded badge was approved for purchase in FY 77. As a follow-up implementation of "Lessons Learned" in the penetration test the ICIP Project Liaison Officer (PLO) and the HDL Security Officer prepared and delivered a series of lectures and classes to the HDL guard force on the penetration test. Additionally, the PLO delivered lectures on the penetration test to the faculty and students of the Counterintelligence Dept, US Army Intelligence Center and School, Fort Huachuca, AZ.

d. Operational Status:

(1) During the reporting period 880 manhours were expended, 18 information reports were submitted and 41 memorandums were prepared and provided to the supported commander.

(2) No TDY or b1 were expended.

e. Comments

(1) ICIP CENTAVO KID was approved by OACSI, DA, 18 Oct 73 and the supported commander was briefed on the implementation of the operation on 12 November 1973.

(2) The mission of the HDL includes critical sensitive research and development activities in support of the US Army. Some of the more sensitive activities include research into the hardening of communications equipment against nuclear weapons radiation; tests of nuclear warhead and missile systems to determine their ability to withstand nuclear weapons radiation; develop fuses for use with nuclear warheads and conducts development and testing of radiation hardened systems for Minutemen and Poseidon Missiles.

(3) The installation remains a potential target for hostile intelligence services.

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(C) GONDOLA STAR: (OACSI Revalidation - 16 Jan 76)

a. Location: Aberdeen Proving Ground (APG) and Edgewood Arsenal (EA), Aberdeen, MD

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76:

(1) Confidential and conventional sources employed in the operation surfaced information on adverse suitability pertaining to 13 employees at Aberdeen Proving Ground/Edgewood Arsenal. The suitability information included alcohol and drug abuse, moral improprieties, fraudulent claim on a TDY voucher and mental instability. Action was taken to substantiate or refute the reported allegations.

(2) Sources reported four instances of alien enlistees who were assigned to the sensitive installations. The Installation Intelligence Officer (IIO) was aware of the status of the four, that they did not have security clearances and had no access to classified information.

(3) Sources reported three instances of foreign travel during the period. One of these DOD affiliated employees who traveled to the USSR after attending a scientific conference in Finland is being contacted by US Intelligence. In another instance, a DOD civilian employee visited Poland and Czechoslovakia for about one month in June-July 1975. The employee and his spouse allegedly visited relatives in both countries. The employee has been debriefed by USAINTA. Source reported that the employee plans to travel to these countries again in 1976. In another instance, husband and wife DOD employees took a Smithsonian Institution-sponsored tour to Moscow and Leningrad. The husband has been debriefed by USAINTA and the wife will be debriefed at her convenience. Source reported that the couple planned to take another trip to Russia in 1976.

(4) Sources reported several instances of foreign contact by military and DOD civilian personnel in the supported activity. In one instance a citizen of the Federal Republic of Germany was assigned on an exchange program to work until Sep 76. A report of a civilian DOD employee at Edgewood Arsenal with some unexplained periods of time in his background prompted a request for a Limited Investigation from the supported command.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY
DECLASSIFY ON 31 Dec 2024

Page 2100 of 3957

(5) Sources reported two instances of Swedish citizens visiting the installations. It was determined that the one visit had been fully coordinated with the proper officials. In the second instance, it was determined that the visit had not been properly coordinated but that steps had been taken to insure the visitors would not be given access to classified information until guidance was provided by higher headquarters.

(6) Sources reported numerous instances of security weaknesses or poor security practices. These included unattended offices in which security containers were left open, a CONFIDENTIAL document left unsecured over a three day weekend, poorly controlled access to a classified scientific conference, movement of an office into a building in which no technical survey had been conducted prior to the move, typewriter ribbons and carbon papers not being disposed of as classified waste, and high-ranking civilian employee bringing his eight year old son into a controlled access area where a classified test was being conducted and remaining overnight.

d. Operational Status:

(1) GONDOLA STAR was first approved by OACSI, DA for implementation on 21 May 1965. On 18 Feb 75, the ACSI directed the termination of 12 ICIPS, including GONDOLA STAR, by 31 Mar 75. After reviewing correspondence initiated by the Commander, Aberdeen Proving Ground, which recommended that the ICIP GONDOLA STAR be continued, the ACSI reinstated the operation for a period of six months on 11 Jul 75, subject to a review after the six months elapsed. On 16 Jan 76, the ACSI approved continuation of the ICIP as an ongoing operation. The following statistics are for the period 11 Jul 75 to 31 Mar 76:

(a) During the reporting period 2,223 manhours were expended and 84 written information reports and 16 oral reports were submitted. b1 b1 no TDY funds were expended.

(b) At the end of the reporting period eight confidential sources were being used in the operation.

e. Comments: The ICIP has been a productive operation at a critically sensitive installation. Information obtained as a result of the ICIP and acted upon by the commanders concerned has served to strengthen the security of the installation. The 902d MI Group is conducting a comprehensive review of this operation for possible replacement of the operation by an overt counterintelligence support program.

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(C) LENS HOLDER: (OACSI Revalidation - 4 Feb 75)

a. Location: White Sands Missile Range (WSMR), NM

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76:

(1) Several reports from confidential sources during the period indicated that employees in the TRADOC Systems Analysis Activity (TRASANA) and the Army Missile Test and Evaluation Directorate (ARMTED) were following poor security practices in daily activities and not adhering to security regulations for safeguarding sensitive classified information. These security hazards included leaving security containers open and unattended for periods during the day, failing to complete security forms affixed to classified material containers, leaving classified material in work boxes after duty hours, and laxity on the part of security guards during night shifts. Security Officers of both TRASANA and ARMTED after being provided reports on these weaknesses briefed all their employees on requirements of WSMR Regulation 380-5 (Security Regulation) and reoriented all guard personnel on their security obligations.

(2) A confidential source reported that a US Army Officer assigned to the Office of Missile Electronics Warfare (OMEW) was misappropriating computer parts and electronic equipment which he was taking home to build his own computer. A summary of available information was provided the US Army Criminal Investigation Division Command for investigation by that agency. The same confidential source reported on 4 Feb 76 that two enlisted soldiers in sensitive positions in TRASANA were engaged in drug trafficking, but in separate operations. Local on-post investigation by the White Sands Missile Range Provost Marshal resulted in apprehension of one of the individuals. Information on the second soldier, allegedly involved in large-scale drug transactions and with criminal contacts, was reported to the Sixth Region, US Army Criminal Investigation Division Command for appropriate investigation.

(3) A confidential source reported that unknown persons had attempted on 11 Jan 76 to penetrate TRASANA, which is an Exclusion Area. On 12 Jan 76, the source reported an unidentified individual claiming to be a colonel had been permitted to enter the TRASANA Compound without the required identification. Investigations by the TRASANA security personnel disclosed that there was no substance to the 11 January report and the

Classified by ADC USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 96

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

person in the 12 January incident was identified and found to be a legitimate entrant into the facility. The incident did serve to illustrate the security awareness of the source and the personnel involved.

(4) A confidential source reported in March 1976 in three reports that devices, such as radios, tape recorders, and "pocket" digital calculators were being brought into a TRASANA Exclusion Area by personnel having access to the area. Many of the computers used in the area have classified information storage and the above-named devices allegedly can affect the computers' operations. The appropriate Security Officer has been appraised of these practices. ICIP project personnel have been tasked to provide follow-up reports on actions taken by the supported command. The information has also been provided as a matter of interest to the Counterintelligence Services and SAVE Team elements at USAINTA.

d. Operational Status:

(1) LENS HOLDER was first approved by the ACSI, DA, for implementation on 16 Sep 74.

(2) Two confidential sources provide coverage of the two principle supported activities, TRASANA and OMEW. An additional individual in the ARMTED is being assessed as a potential source.

(3) During the reporting period, 1,053 manhours were expended. b1 b1 there were no TDY outlays. The operation produced 36 written information reports and 24 memorandums and oral reports.

e. Comments:

(1) The mission of the White Sands Missile Range has remained unchanged since the inauguration of the ICIP and the previous OACSI revalidation on 4 Feb 75. The mission of WSMR is to evaluate the Safeguard Missile System missile vulnerability studies, missile control systems, and perform pre-production tests and analyses of missile systems. The mission of WSMR makes it a prime target of hostile intelligence. Activities at WSMR which have Priority I requirements for support are TRASANA, OMEW, ARMTED, the National Range Operations Directorate, and the US Army Safeguard Systems Evaluation Agency. These elements develop electronic countermeasures techniques to nullify vulnerabilities discovered in missile systems, conduct pre-production tests of rocket and guided missile systems, operate a nuclear effects facility and operate National Range Facilities for tests conducted at WSMR.

Page 2103 of 3957

~~CONFIDENTIAL~~

(2) The operation to date has proven to have value as an adjunct to the installation security program. The isolation of the installation, dispersion of many of its facilities, and the extent and nature of its computer facilities and missile testing ranges present a lucrative target for hostile intelligence service (HOIS) penetration. USMR's proximity to the US-Mexican border renders it vulnerable to HOIS operations based in a foreign country. Admittedly, the operation to date has not surfaced hard evidence of HOIS presence or penetration, but the scope of the threat must be recognized. Details of activities conducted at the site are of current interest to HOIS. The two-pronged capability of the ICIP, that is, extensive use of overt sources of all types, plus the covert effort exemplified by the confidential sources, appears to be necessary coverage at this time with the best potential for detection and discovery of HOIS activities.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(C) LENTIL MONKEY: (OACSI Revalidation - 4 Feb 75)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr.75 to 31 Mar 76:

(1) A source in the Chinese-Mandarin Language Department furnished information concerning a temporary instructor of that department who closely questioned her students about their knowledge of their future duties and assignments. She frequently expressed her displeasure in the task of teaching Chinese to students which would enable them to "conduct spying activities" directed at the People's Republic of China (PRC). The instructor also displayed a rebellious and uncooperative attitude toward necessary DLI administrative requirements. Born in Canton, China, she was a British citizen and no evidence of a pre-employment investigation could be found. DLI refused to renew her contract when it expired in Sep 75 and she departed DLI in that month.

(2) A Confidential Source reported information on an instructor of the German Language Department who travelled to East Germany in mid-1975 without notification or permission from DLI authorities. Upon completion of the travel, the instructor was admonished officially and informed that any future violation of the DLI regulations on foreign travel would result in temporary suspension.

(3) A visitor to the Russian Language Department in May 75 requested copies of training material used in the Russian Dept, claiming that he wanted it to use for language training in his reserve unit. The visitor was given two unclassified training exercises. Subsequent investigation identified the visitor and established that he was a former graduate of Russian at DLI, and additionally, that he was a bona fide member of a California-based Army Reserve unit. The incident, although not of a major significance as proven by the later investigation, did serve to underscore a need for better visitor control at DLI. The Director, DLI, placed special emphasis on this and the need for all personnel to be alert for unauthorized visitors and proper procedures for handling them. New visitor requirements and restrictions were published and distributed throughout DLI.

Classified by CDR USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 06

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~ 610

~~CONFIDENTIAL~~
~~SECRET~~

(4) An instructor in the Hungarian Language Department travelled to Hungary in Sep 75 with a stated purpose of visiting relatives. A review of the instructor's file revealed extensive foreign travel in Europe since 1971 and frequent contact with relatives and other persons in Hungary. File checks and inquiries of other agencies failed to reveal any substantial derogatory information concerning the instructor, but the potential hostage situation is evident in the continuing contacts. Monitoring of the instructor's activities continues.

(5) An ICIP source reported that an instructor in the Russian Language Department allegedly is a former member of the Soviet Army's equivalent to the US Army Security Agency who while in the Soviet Army received special training in English. This instructor left the USSR in Apr 74 and was hired at DLI in Oct 74. A coworker of the instructor left the Soviet Union in Apr 75 and was also hired as an instructor at DLI in Jul 75. Both of the instructors taught together at the Leningrad Herzen Pedagogical Institute in Leningrad in the late 1960s and early 1970s. The sequence of these events illustrate how quickly these individuals are able to secure employment after leaving the USSR, employment in which they are placed in extremely close contact with US intelligence personnel. Monitoring of the activities of these individuals continues.

(6) Two instructors in the Bulgarian Language Department who are man and wife were accused by fellow faculty members at DLI of being communists because of the unexplained details of their emigration to the West and the manner in which they left Bulgaria. The allegations led to charges and countercharges; full details of the incident were provided the FBI. The wife remains at DLI as an instructor, but as of the close of the reporting period on 31 Mar 76, the husband was employed elsewhere and no longer DOD-affiliated.

(7) A DLI employee of the Hebrew Project at DLI also created considerable internal dissension and bickering within the Hebrew Department when he maintained close contact with the Israeli Consulate in San Francisco. This caused associates to become suspicious of his motives and high level contacts. The employee, an alien with an impressive background, including possible intelligence activities, later applied for employment with the National Security Agency (NSA), which has been provided all information available to USAINTA.

(8) A confidential source reported that a Czechoslovakian Language Department (CLD) instructor was planning to withdraw her retirement fund money and return to Czechoslovakia with her two sons, allegedly to live there.

b1 Per FBI

~~SECRET~~ 611

Regraded ~~SECRET~~
ON 20 MAR 1998
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

~~CONFIDENTIAL~~

Page 2106 of 3957

SECRET

b1 Per FBI

At the close of the reporting period possible health problems appeared as a deterrent to the wife's original plans, but definite decisions in this regard are unknown.

b1 Per FBI

(9) A second CLD instructor has disclosed to several sources over the last two years his continuing efforts to obtain the release of his children from Czechoslovakia. The Czech Government recently informed the instructor that he could obtain the release of his children if he pays the Czech Government $66,000 as reimbursement for the cost of the time the instructor spent in a Czech prison and an education tax on the education acquired in Czechoslovakia by the instructor and his wife. The instructor disclosed that the Czech military had changed its method of counting. The reports indicate that the instructor is maintaining close, continuing ties with Czech Government officials and that a hostage situation with his children exists. Monitoring of his activities continues.

(10) Monitoring also continues on activities of a Polish Language Department (PLD) instructor who plans to visit his mother and a brother in Warsaw in mid-1976. The instructor has not applied formally to DLI for approval for the leave and the trip. The instructor frequently has travelled in the past to Europe. His brother, a medical doctor also travels extensively, and has been in the US and Canada often during the last 20 years. During a 1974 visit to the US, the instructor's brother visited DLI, attended PLD functions at DLI, talked with the US Army students at length and photographed many of the students in attendance. US Customs once detained the instructor's brother at the Canadian border for attempting to smuggle Communist propaganda into the US; US Customs confiscated the propaganda.

(11) An instructor in the Russian Language Department apparently is suffering from mental problems. The instructor has written to a California US Senator, a nationally syndicated columnist, and the FBI, alleging that he is constantly under surveillance by the Soviet KGB and US intelligence and further, that his life is in danger. The instructor also has sent a telegram to the President of the United States. Both the FBI and the Secret Service have made inquiries into the matter and conducted local investigations of the instructor. On 23 Mar 76, the DLI Commandant directed the instructor to undergo psychiatric evaluation. Initially, the instructor refused and was suspended from his duties administratively. At the end of the reporting period the instructor agreed to the examination. The results and final disposition are pending.

Regraded SECRET
ON 30 MAR 1998
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

SECRET

d. Operational Status:

(1) LENTIL MONKEY was first approved by ACSI, DA, for implementation on 11 September 1967.

(2) During the reporting period, 4,603 manhours were expended. b1 there were no TDY outlays.

(3) Production consisted of 360 written information reports and 220 Memorandums and oral reports.

(4) Eight confidential sources were active in the ICIP at the close of the period and additional coverage of language departments and administrative sections of DLI was obtained by 16 conventional sources.

e. Comments:

(1) The mission of DLI is to train DOD intelligence and communications security specialists in every major foreign language. Military attaches, employees of the CIA and FBI, as well as other federal agencies, are also trained at DLI, making it an extremely enticing target for hostile intelligence service operatives. The majority of the faculty of DLI have foreign backgrounds, some have only recently arrived from Communist Bloc countries and rapidly achieved employment in an installation where most of the students are in intelligence or destined for intelligence assignments upon graduation. Many of these instructors are in hostage situations by virtue of close, living relatives in the ComBloc countries with whom they maintain written contact and closer, if less frequent, personal contact. In maintaining contact with these ComBloc countries for any reason whatsoever, intelligence agencies of those countries in all likelihood have identified the instructors' place of employment and may have contacted them under one guise or another.

(2) In addition to extensive and frequent contacts with the governments of HoIS, many instructors who probably are completely imbued with the American way of life and are now US citizens or who intend to become citizens, nevertheless are vulnerable targets. The instructors acquire personal acquaintances among many intelligence personnel and, in the course of teaching and associating with the military in year-long classes, learn of the students' future assignments and do in some instances correspond with DLI alumnae after graduation. This unique characteristic of conditions at DLI serves to make the Institute an even more attractive target for HoIS approaches.

(3) As shown by statistics in paragraph d(2), and d(3), above, ICIP LENTIL MONKEY is the most productive of all the presently active ICIPS with a total of 360 written reports. Though 4,603 manhours were expended in the project, the actual cash outlay of b1 for the

~~CONFIDENTIAL~~

year, the lowest cost figure for any of the active ICIPS. Viewed from the cost-yield ratio alone, this operation is an extremely successful, economical effort.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

614

~~CONFIDENTIAL~~

INCL 3

615

~~CONFIDENTIAL~~

Period: 1 Apr 1975 to 31 Mar 1976

INTERNAL COUNTERINTELLIGENCE PROGRAM

ICIP	INSTALLATION	FIRST INITIATED (I) REVALIDATED (R)	SOURCES AS OF 31 MAR 76 CONF	SOURCES AS OF 31 MAR 76 CONVEN	INFO REPORTS AR, SR SOI	INFO REPORTS OTHER MEMO/ORAL	MAN HOURS	FUNDS TDY	b1
CANARY EFFORT 1/	USA Comm Cmd Ft Ritchie, MD	I-JUN 65 R-FEB 75	3	9	69	116	3,255	81	b1
CANINE PLATE 2/	Seneca Army Depot, AMC, Romulus, NY	I-NOV 73 R-FEB 75		5			400		
CANTER RIDE 1/	US Army Msle Cmd Redstone Arsenal, AL	I-MAR 75	1		1		697	1,315	b1
CANVAS TAX	Sierra Army Depot, AMC, Herlong, CA	I-APR 74 R-FEB 75	2	2	14	24	616	29	
CENSUS TIME 2/	Pentagon Telecom Ctr USACC-CONUS, Wash DC	I-FEB 74 R-FEB 75		2	7	6	726		
CENTAVO KID 2/	Harry Diamond Labs AMC, Wash DC	I-NOV 73 R-FEB 75		7	18	41	880		
GONDOLA STAR	Aberdeen Proving Gd Aberdeen, MD	I-MAY 65 R-JAN 76	8	10	84	16	2,223		b1
ENS HOLDER	White Sands Msle Rge, NM, TECOM, AMC	I-SEP 74 R-FEB 75	2		36	24	1,053		b1
LENTIL MONKEY	DLI, Pres of M, CA TRADOC	I-SEP 67 R-FEB 75	8	16	360	220	4,603		b1
	TOTAL		24	51	589	447	14,453	1,425	b1

1/ Terminated 31 Mar 76
2/ Terminated (Jun 76) after period covered by this report

~~CONFIDENTIAL~~

Classified by CDR, USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

Page 2111 of 3957

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

DAMI-DOH

MEMORANDUM THRU: ~~VICE CHIEF OF STAFF, UNITED STATES ARMY~~

NOTED USA 12 APR 1976
Date.....

FOR: ~~UNDER SECRETARY OF THE ARMY~~

COL John A. Todd, Exec., SAUS

SUBJECT: Internal Counterintelligence Program (ICIP) (U)--
INFORMATION MEMORANDUM

1. (U) During the past quarter, six of the currently active Internal Counterintelligence Program (ICIP) operations provided information on incidents involving personnel suitability and conditions reflecting poor security practices or weaknesses. Reports of these relatively minor conditions were furnished the commanders of the supported commands who took immediate corrective action.

2. (U) The total number of active ICIP operations remains at nine. Summaries of activity in these operations during the last quarter are inclosed.

9 Incl
as (C)

HAROLD R. AARON
Major General, GS
ACofs for Intelligence

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

* OCT-DEC 75

Noted by the Under Secretary of the Army with comment: "On next quarter's review, please provide an analysis (of each ICIP for the past year) to include statistics."

6/7

JOHN A. TODD
Colonel, GS

Classified by ACSI DA

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

DEPARTMENT OF THE ARMY
HEADQUARTERS
U.S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

MAY 11 1976

MIIA-SO-SA

SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOH/COL HAENDLE)
WASH DC 20310

1. (U) (C) During the 3d Quarter, FY 1976, two of the on-going ICIP operations were terminated effective 31 March 1976, CANTER RIDE at Redstone Arsenal, AL, and CANARY EFFORT at Fort Ritchie, MD. The Commander, USAINTA, and the ACSI verbally approved termination actions on 20 and 23 February 1976, and separate correspondence requesting formal termination was submitted to ACSI, DA, on 8 April 1976. The total number of active ICIP operations at the close of the 3d Quarter was seven. Summaries for each of these seven operations, plus the two which were terminated, are attached as TAB A, which is the quarterly report for the period ending 31 Mar 76.

2. (U) (C) The former Project Liaison Officers (PLO) of the two terminated ICIPS, CANARY EFFORT and CANTER RIDE, are continuing to provide counter-intelligence support to the sensitive elements at Redstone Arsenal and Fort Ritchie. These activities now receive comprehensive assistance through an overt, all-source, multi-discipline effort named the Direct Support Comprehensive Counterintelligence Program (DSCCP). A review of ICIP Operations CANINE PLATE, CENTAVO KID, and CENSUS TIME is currently being conducted to determine which of these operations should be converted to the DSCCP concept.

3. (U) (C) Through a comment on the DAMI-DOH Information Memorandum to the Under Secretary of the Army, subject: ICIP Program, dated 1 April 1976, the Under Secretary indicated that an analysis of each ICIP operation for the past year was to be provided with the next quarterly review. In compliance with those instructions, an analysis of each ICIP operation was made for the period 1 April 1975 to 31 March 1976. As a result of these analyses, five ICIPS (TAB B) are recommended for termination; four ICIPS (TAB C) are recommended for retention. At TAB D are statistics

[redacted] CDR USAINTA

[redacted] 2

[redacted] 31 DEC 06

618

[redacted]

MIIA-SO-SA
SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operations (U)

for each of the ICIP operations which are referred to in individual reviews. These statistics provide a recapitulation of pertinent costs, manhours, and production for the nine ICIP operations covered in this analysis.

5. (U) Recommend approval of termination and retention actions in TABS B and C.

WILLIAM I. JENNINGS
Special Assistant (OPS)

4 Incl
as

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

Page 2114 of 3957

MIIA-SO-SA

SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOH/COL HAENDLE)
WASH DC 20310

1. (U) During the 3d Quarter, FY 1976, two of the on-going ICIP operations were terminated effective 31 March 1976, CANTER RIDE at Redstone Arsenal, AL, and CANARY EFFORT at Fort Ritchie, MD. The Commander, USAINTA, and the ACSI verbally approved termination actions on 20 and 23 February 1976, and separate correspondence requesting formal termination was submitted to ACSI, DA, on 8 April 1976. The total number of active ICIP operations at the close of the 3d Quarter was seven. Summaries for each of these seven operations, plus the two which were terminated, are attached as TAB A, which is the quarterly report for the period ending 31 Mar 76.

2. (U) The former Project Liaison Officers (PLO) of the two terminated ICIPS, CANARY EFFORT and CANTER RIDE, are continuing to provide counter-intelligence support to the sensitive elements at Redstone Arsenal and Fort Ritchie. These activities now receive comprehensive assistance through an overt, all-source, multi-discipline effort named the Direct Support Comprehensive Counterintelligence Program (DSCCP). A review of ICIP Operations CANINE PLATE, CENTAVO KID, and CENSUS TIME is currently being conducted to determine which of these operations should be converted to the DSCCP concept.

3. (U) Through a comment on the DAMI-DOH Information Memorandum to the Under Secretary of the Army, subject: ICIP Program, dated 1 April 1976, the Under Secretary indicated that an analysis of each ICIP operation for the past year was to be provided with the next quarterly review. In compliance with those instructions, an analysis of each ICIP operation was made for the period 1 April 1975 to 31 March 1976. As a result of these analyses, five ICIPS (TAB B) are recommended for termination; four ICIPS (TAB C) are recommended for retention. At TAB D are statistics

CDR USAINTA

2

31 DEC 06

620

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

MILA-SO-SA
SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operations (U)

for each of the ICIP operations which are referred to in individual reviews. These statistics provide a recapitulation of pertinent costs, manhours, and production for the nine ICIP operations covered in this analysis.

5. (U) Recommend approval of termination and retention actions in TABS B and C.

4 Incl
as

WILLIAM I. JENNINGS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

621

Page 2116 of 3957

(U)

1. ~~(S)~~ CANARY EFFORT: (OACSI Revalidation - 4 Feb 75)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) On 15 January 1976, the PLO, as a result of a liaison visit with the Baltimore Division of the Federal Bureau of Investigation obtained data on the presence of Sino-Soviet Bloc personnel travelling within the environs of the target areas and information on those Sino-Soviet bloc personnel residing temporarily in the environs of the target area.

(2) On 28 January 1976 a member of the 572d Military Police Co, Ft Ritchie, was approached by an unidentified individual at Hagerstown Junior College, Hagerstown, MD, who claimed to be employed at Site R. The individual described Site R in general terms, but made no attempt to elicit information from the soldier. Investigative efforts failed to identify the individual. All available information was provided the Hagerstown Resident Office of the FBI. A USAINTA investigation of the incident is continuing.

(3) On 28 January 1976, an unidentified individual approached a soldier assigned to the US Army Communications Command East Coast Telecommunications Center (USACCECTC) and requested a tour of that facility. The individual appeared interested in the antenna configuration of Satellite Communications/Direct Communication Links (SATCOM/DSL). The request for the tour was refused; the soldier reported the incident. All available information was provided the Hagerstown Resident Office of the FBI. USAINTA investigation of the incident is continuing.

(4) During the reporting period information was developed on a Non-Appropriated Fund (NAF) employee who is a bartender employed at the Ft Ritchie NCO Club. The bartender allegedly claimed to patrons that she was in the employ of both "Military Intelligence" and the "CIA." An investigation is being conducted by USAINTA.

(5) On 18 March 1976, a US Army NCO assigned sensitive duties in the Alternate National Military Command Center (ANMCC) volunteered information concerning his entering into correspondence with an agency of the East German Government. The NCO, who has been researching his family history for the last six years, was attempting to obtain a record of the military service of his great-great grandfather in the period circa 1810. In the course of an inquiry to the Federal Republic of

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603,DoD 5200.1-R

623
622 Classified by ...USAINTA...
FROM ...
SCHEDULE OF ...
DECLASSIFY ON: DEC ...

Germany (FRG) Ambassador in Washington and the FRG Government, he was advised to contact the German Historical Central Archives in East Germany. The NCO volunteered the information so it could be made a matter of official record in the event he should be contacted in any fashion by East Germany in the future. The Chief, ANMCC, was provided information on the above. The NCO was given a SAEDA briefing under the provisions of AR 381-12 with special emphasis on reporting procedures. The NCO will provide Army Intelligence with copies of any correspondence he receives in this regard. At present the opportunity for further exploitation appears minimal.

e. Operational Status:

(1) In February 1976, the 902d MI Group selected Operation CANARY EFFORT to be terminated and replaced by a Direct Support Comprehensive Counterintelligence Program (DSCCP) which is being developed by the 902d MI Group. Supported commanders were briefed on the termination in conjunction with the scheduled quarterly briefings as described below. All confidential sources used in this ICIP have been terminated. The CDR, USAINTA, and the ACSI indicated verbal approval of the termination on 20 and 23 February 1976, respectively. The effective termination date for CANARY EFFORT is 31 March 1976.

(2) During the quarter, the PLO presented 21 SAEDA/Threat/Security Awareness briefings to personnel assigned to supported activities at Fort Detrick and Fort Ritchie.

(3) The PLO presented the Quarterly Progress Briefing to LTC Dale S. Cockle, CDR, USACC ECTC, on 30 March 1976.

(4) The PLO, on 1 April 1976, presented the Quarterly Progress Briefing to COL John S. Eberle, CDR, US Army Communications Command (USACC) Site R.

(5) On 5 April 1976, the PLO gave the Quarterly Progress Briefing to the supported command, HQ, 7th Signal Command and Ft Ritchie, with the following officials present: COL Harold G. deMoya, CDR, Ft Ritchie; COL John J. Plosay, Jr., Deputy CDR, Ft Ritchie and Mr. Joseph J. Carroll, Acting Assistant Chief of Staff, Intelligence and Security, 7th Signal Command and Ft Ritchie.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

2. (U) CANINE PLATE (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD), Romulus, NY

b. Confidential Source Utilization: None

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status:

Five conventional sources are contacted on a recurring basis by the Project Liaison Officer (PLO) in this operation; one of these plans retirement in July 1976. One newly contacted official source is in a position to assist in spotting potential new sources. No threat information was surfaced during this quarter. On 5 March 1976 the PLO provided the Quarterly Briefing to LTC Earl Hain, Acting Depot Commander. LTC Hain was designated by COL Alden Cox, CDR, SAD, to receive the briefing during the absence of COL Cox

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

624

3. (U) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal, AL

b. Confidential Source Utilization: One

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status:

On 18 February 1976, COL Hassel Parker, CDR, 902d MI Group, with the Project Liaison Officer (PLO) in attendance, provided a special briefing on this operation to MG Turnmeyer, CDR, USAMICOM. COL Lange, USAMICOM Chief of Staff, was also present during the briefing. As a result of the briefing, it was agreed by the participants that since the operation had accomplished its objective it should be terminated and the insert source should be extracted to reduce the risk of compromise. MG Turnmeyer expressed his deep appreciation for the information provided by the operation and concurred with the suggested termination. The source used in this operation has been reassigned and will be debriefed subsequent to his 8 April 1976 reporting date. The CDR, USAINTA, and the ACSI, DA indicated verbal approval of the termination on 20 February and 23 February 1976, respectively. The effective termination date for CANTER RIDE is 31 March 1976.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CDR USAINTA

625

4. (C) CANVAS TAX: (OACSI Revalidation - 4 Feb 75)

a. Location: Sierra Army Depot (SIAD), Herlong, CA

b. Confidential Source Utilization: Two

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained: None

e. Operational Status:

(1) The two confidential sources are providing coverage of the Priority I activities of SIAD which are Exclusion Areas I and II. Two conventional sources and one casual source cover the Priority II activities which are the staff and security organizations of the Depot. One individual assigned to the Special Weapons Section, Exclusion Area II is under assessment as a potential source.

(2) The Quarterly Progress Report for the 2d Quarter, FY 76, which had been postponed at the request of the CDR, SIAD, was presented by the PLO on 13 Feb 76 to the following SIAD officials: COL Robert Hawlk, CDR, SIAD; LTC Robert Render, Deputy CDR; MAJ Robert Folster, Security Officer; CPT Wayne Heringer, Intelligence Officer and Mr. Anthony Tornabene, Assistant Intelligence Officer. The following personnel from the 525th MI Group also attended the briefing: COL Donald Bradbury, CDR; LTC Arthur McQueen, Operations Officer, and MAJ Trevor Bissey, CDR, San Francisco Field Office.

(3) ICIP Sources have been tasked to report any significant counterintelligence EEI or indicators of hostile intelligence activity impacting on Operation Rocking Force (U), a special weapons project presently in progress at SIAD.

(4) The Quarterly Progress Briefing for the 3d Quarter, FY 76, will be presented by the PLO on or about 30 April 1976 to the SIAD officials listed in paragraph 5e(2), above.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by ...CDR USAINSCOM...
...FICATION
...
DECLASSIFY ON: 31 DEC 84

626

CONFIDENTIAL

[redacted]

5. (C) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC

b. Confidential Source Utilization: None

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) The Limited Investigation reported in the last quarter on the PTC NCO who had attempted suicide and allegedly had involved himself in financial troubles, drugs, and homosexuality was completed and referred to PTC for adjudication. The decision was made not to revoke the NCO's security clearance since he left the service on 9 April 1976 and will not be allowed to re-enlist.

(2) During the course of an investigation of an enlisted WAC member of PTC with a SECRET security clearance who was Absent-Without-Leave, it was discovered that CID, Ft Meyer was also investigating her for theft and trafficking in drugs. The Project Liaison Officer (PLO) and CID agents coordinated their mutual investigations. Drug charges are pending the results of laboratory tests of substances purchased from the WAC by CID informants. PTC has suspended the WAC's access to classified material pending completion of the investigation.

(3) The PLO arranged with appropriate 902d MI Group elements to present formal SAEDA briefings to all PTC personnel, including the PTC elements in the Hoffman and Forrestal Buildings. This project is scheduled for completion in the next quarter.

e. Operational Status:

(1) The Hoffman Telecommunications Center has been brought under coverage of this ICIP, as requested by COL Donald E. Clark, PTC Commander, in the previous quarter.

(2) On 24 March 1976, the PLO presented the Quarterly Progess Briefing to COL Clark, CDR, PTC. CW2 Leonard Gross, Alternate PLO, was also present at the briefing.

[redacted]

Regraded UNCLASSIFIED on
3 Dec 07
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

Page 2122 of 3957

6. (C) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories (HDL), Adelphi, MD

b. Confidential Source Utilization: None

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) As a follow-up implementation of "Lessons Learned" in the courtesy penetration test conducted at HDL's Adelphi Facility in the previous quarter, the Project Liaison Officer (PLO) and the HDL Security Officer prepared and delivered a series of lectures and classes to the HDL Guard Force on the penetration test. The Guard Force is operating under new instructions designed to thwart attempted penetrations. A new HDL Badge and Pass System, utilizing a magnetic coded badge and a computer control device, will be started in mid-1976.

(2) The PLO delivered lectures on the penetration test conducted at HDL to the faculty and students of the Counterintelligence Dept, US Army Intelligence Corps School, Fort Huachuca, AZ, on 20 and 21 January 1976.

(3) The PLO, assisted by other 902d MI Group personnel conducted several technical inspections at HDL. The PLO provided advice and assistance at several design meetings concerning new buildings at HDL.

(4) Other security advice was provided by the PLO to the Woodbridge Research Facility (WRF), Woodbridge, VA, and the Gaithersburg Test Site (GTS), Gaithersburg, MD. The PLO assisted in devising Operational Security techniques at these sites, the only HDL facilities at which outdoor testing takes place. HDL requested to be placed on distribution for the SATRAN II system but had not received any output from the system as of the close of the reporting period.

e. Operational Status:

On 16 March 1976, the PLO presented the Quarterly Briefing to MAJ Kenneth F. Keller, Executive Officer, HDL, and Mr. James F. Yeick, Security Officer, HDL.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by CDR USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 3
DECLASSIFY ON: 31 DEC 76

623

[redacted]

8. (U) LENS HOLDER: (OACSI Revalidation - 4 Feb 75)

a. Location: White Sands Missile Range (WSMR), NM

b. Confidential Source Utilization: Two

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) A confidential source reported that unknown persons had attempted on 11 January 1976 to penetrate the TRADOC Systems Analysis Activity (TRASANA). On 12 January 1976, it was reported that an unidentified individual claiming to be a colonel had been permitted to enter the TRASANA Compound. These incidents were reported immediately to the Security Officer, TRASANA. An investigation by TRASANA security personnel disclosed that there was no substance to the 11 January report and the person in the second incident of 12 January was identified and found to be a legitimate entrant into the facility. The incidents did serve to illustrate the security awareness of the source and the personnel involved.

(2) A source surfaced information on 4 February 1976 that two enlisted soldiers at TRASANA were engaged in drug trafficking, but in separate individual operations. Local on-post investigation resulted in apprehension of one of the individuals. All available information on the second individual was reported to the Sixth Region, US Army Criminal Investigation Division Command for appropriate action.

(3) A confidential source reported in March 1976 in three reports that such devices as radios, tape recorders, and "pocket" digital calculators were being brought into a TRASANA Exclusion Area by personnel having access to the area. These devices reportedly could affect the computers used in the area, some of which have classified data in storage. The Activity Security Officer has been briefed on these alleged practices and ICIP project personnel have been tasked to provide follow-up reports on action taken by the supported command. The information contained in the reports has been provided to the Counterintelligence Services and SAVE Team elements at USAINTA as a matter of interest.

e. Operational Status:

(1) The two confidential sources provide coverage of TRASANA and the US Army Electronics Command, Office of Missile Electronics Warfare (OMEW), WSMR. One individual assigned to the US Army Missile Test and Evaluation Directorate is under assessment as a potential source.

(2) The Quarterly Progress Briefing, postponed at the request of MG O. L. Tobiason, CDR, WSMR, will be presented during the next quarter.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

629

[redacted]

Classified by ...CDR...
EXEMPT FROM ...CATION
SCHEDULE OF ... 11652
EXEMPTION ...
DECLASSIFY ON: ...DEC ...

[redacted]

(24)

GONDOLA STAR: (OACSI Revalidation - 11 Jul 75)

a. Location: Aberdeen Proving Ground (APG), and Edgewood Arsenal, Aberdeen, MD

b. Confidential Source Utilization: Eight

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

A confidential source identified an individual in the Biomedical Laboratory, Edgewood Arsenal, as an alien enlistee. Project personnel briefed the appropriate security personnel and a background investigation, to include a polygraph examination, was initiated. The investigation had not been concluded at the close of the quarter.

e. Operational Status:

(1) On 23 March 1976, the PLO presented the Quarterly Progress Report to COL Alvin D. Ungerleider, CDR, APG, on those activities pertaining to the Aberdeen area. Mr. Harry A. Mencke, Installation Intelligence Officer, APG, was present also.

(2) On 25 March 1976, the PLO presented the Quarterly Progress Report on Edgewood Arsenal activities to COL Kenneth L. Stahl, CDR, Edgewood Arsenal, with CPT Vincent J. Falconio, Chief, Security Office, Edgewood Arsenal, also present.

[redacted] DECLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

630

[redacted]

8. (U) LENS HOLDER: (OACSI Revalidation - 4 Feb 75)

a. Location: White Sands Missile Range (WSMR), NM

b. Confidential Source Utilization: Two

c. Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) A confidential source reported that unknown persons had attempted on 11 January 1976 to penetrate the TRADOC Systems Analysis Activity (TRASANA). On 12 January 1976, it was reported that an unidentified individual claiming to be a colonel had been permitted to enter the TRASANA Compound. These incidents were reported immediately to the Security Officer, TRASANA. An investigation by TRASANA security personnel disclosed that there was no substance to the 11 January report and the person in the second incident of 12 January was identified and found to be a legitimate entrant into the facility. The incidents did serve to illustrate the security awareness of the source and the personnel involved.

(2) A source surfaced information on 4 February 1976 that two enlisted soldiers at TRASANA were engaged in drug trafficking, but in separate individual operations. Local on-post investigation resulted in apprehension of one of the individuals. All available information on the second individual was reported to the Sixth Region, US Army Criminal Investigation Division Command for appropriate action.

(3) A confidential source reported in March 1976 in three reports that such devices as radios, tape recorders, and "pocket" digital calculators were being brought into a TRASANA Exclusion Area by personnel having access to the area. These devices reportedly could affect the computers used in the area, some of which have classified data in storage. The Activity Security Officer has been briefed on these alleged practices and ICIP project personnel have been tasked to provide follow-up reports on action taken by the supported command. The information contained in the reports has been provided to the Counterintelligence Services and SAVE Team elements at USAINTA as a matter of interest.

e. Operational Status:

(1) The two confidential sources provide coverage of TRASANA and the US Army Electronics Command, Office of Missile Electronics Warfare (OMEW), WSMR. One individual assigned to the US Army Missile Test and Evaluation Directorate is under assessment as a potential source.

(2) The Quarterly Progress Briefing, postponed at the request of MG O. L. Tobiason, CDR, WSMR, will be presented during the next quarter.

631

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~ ~~SECRET~~

9 (S) (U) LENTIL MONKEY: (OACSI Revalidation - 4 Feb 75)

a. (U) Location: Defense Language Institute (DLI), Presidio of Monterey, CA

b. (U) Confidential Source Utilization: Eight

c. (U) Information Obtained or Reported on Non-Affiliated Civilians: None

d. Useful Information Obtained:

(1) (S) The female instructor in the Czechoslovakian Language Department reported in the last quarter as preparing to resign her position and return to Czechoslovakia now is reportedly having serious health problems.

Referred

(2) (U) A Polish Language Department instructor plans to visit his mother and a brother in Warsaw in mid-1976, a confidential source has learned. The instructor has submitted no formal request to DLI for the trip yet. The instructor's activities are monitored as a matter of intelligence interest because of his and his brother's travels. His brother, a medical doctor has visited in the US and Canada frequently over the last 20 years and was once detained by US Customs at the Canadian border for attempting to smuggle Communist propaganda into the US. During a 1974 visit to the US, the instructor's brother visited DLI, attended Polish Language Department functions, talked with and photograhed the students. USAINTA is monitoring the instructor's activities.

(3) (U) A Czech language instructor is continuing his efforts to obtain the release of his children from Czechoslovakia. A confidential source surfaced the most recent information that the Czech Government has informed the instructor he could get his children out of the country if he pays the Czech Government $66,000. ($6,000 for the cost of his time in a Czech prison and $60,000 as an educational tax on his and his wife's education.) Source did not have further information on this particular aspect, but reported that in mid-February 1976 the instructor gave many of the DLI Czech students a list of newly published books in the Czech language. The books are distributed by a Canadian firm, "Sixty Eight Publishers," Box 695 Station A, Toronto, Ontario M5W 1G2 Canada. The instructor told his classes that the Czech military had officially changed their method of counting for example, using "21" instead of "1 and 20." Insignificant in itself, this last item indicates that the instructor is maintaining ties with Czechoslovakian officials. USAINTA is monitoring the instructor's activities.

Regraded SECRET
ON 20 MAR 1998
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

~~SECRET~~

632

~~CONFIDENTIAL~~

(4) Information developed from official sources during the period disclosed that an instructor of the Russian Language Department (RLD) apparently is suffering from mental problems. The instructor has written letters to a California senator, a nationally syndicated columnist, and the FBI, alleging that he is under surveillance of Soviet and US intelligence constantly and that his life is in danger. The Commander, USAINTA, provided a summary report on the instructor to the ACSI. The instructor later sent a telegram to the President of the United States. Both the FBI and the Secret Service have made inquiries into the matter. On 23 March 1976, the Commandant, DLI, took administrative action directing the instructor to undergo psychiatric evaluation. The instructor refused initially and was administratively suspended from teaching. At the end of the quarter, the instructor agreed to the examination and final disposition of the matter is pending.

e. Operational Status:

(1) As a result of the RLD incident described in d(4), above, the DLI Commandant has directed that the Civilian Personnel Office and Security Office screen records of faculty members for indications of mental problems. Once identified, action will be taken to obtain treatment for the individuals concerned.

(2) Eight confidential sources were utilized during the quarter; three sources were terminated due to graduation. Four new confidential sources were recruited, including one Technical Language Assistant (TLA). Fifteen individuals are under assessment as possible sources, including one instructor and one TLA. In addition to the confidential sources, there are 16 conventional sources providing coverage of seven language departments and the DLI staff.

(3) On 29 March 1976, the PLO presented the Quarterly Briefing to COL Samuel L. Stapleton, Commandant, DLI. Also present at the briefing were COL Donald K. Bradbury, CDR, 525th MI Group; MAJ Trevor Bissey, CDR, San Francisco Field Office, 525th MI Group; CPT Brendon A. Niques, SAIC, Ft Ord Resident Office, 525th MI Group; and Mr. James Green, Asst Security Officer, DLI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

633

[redacted]

ICIP REPORT

1 April 1975 to 31 March 1976

(U) CANARY EFFORT: (OACSI Revalidation - 4 Feb 75)

a. Location: Fort Ritchie, MD

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 - 31 Mar 76:

(1) Confidential and conventional sources employed in the operation surfaced information on adverse suitability pertaining to 86 employees at Fort Ritchie, all of whom had security clearances and access to one of the sensitive activities supported. The suitability information included the entire spectrum in this category - alcohol and drug abuse, moral improprieties and mental instability. In these instances investigative action was taken to refute or substantiate the allegations or the individuals were removed from access to classified information. About 50% of the cases reported involved some degree of drug abuse; these were referred to the Criminal Investigation Division for action.

(2) Two separate reports were received concerning suspected Soviet Intelligence presence and interest in the activities of the supported installation. Details of these reports were provided the FBI in May 1975 In one instance an individual resembling a known KGB agent paid an unusual amount of attention to shipment of sensitive cargo to Fort Ritchie; in the second instance an individual assigned to Fort Ritchie reported that a second person whom he had met claimed to be in contact with the Soviets in Hagerstown, MD. As of 31 Mar 76, the FBI investigations of the reports were inconclusive.

(3) An ICIP source reported a possible compromise occurred when the Telecommunications Directorate, Site R, was tasked to prepare a special test tape containing test messages which could be used for coding and to devise compatibility between two computer systems. The test tape, though it consisted only of innocuous, unclassified messages, also contained fragments of sensitive, highly classified messages which had been picked up from residual magnetism on the reels of the equipment when the messages were recorded. This latter condition was not discovered until processing to make the systems compatible took place, after the tape had lain unsecured, in open storage, for about six weeks. A command investigation of the incident followed and a determination was made that apparently a compromise had not occurred, but as a result of the incident, changed security procedures were put into effect for the handling and storage of computer tapes, reels, and discs.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

634

[redacted]

Classified by CDR USAINSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY
DECLASSIFY ON Ind. Ctr.

~~CONFIDENTIAL~~

(4) (U) Two possible SAEDA approaches to soldiers stationed at Fort Ritchie in January 1976 are currently under investigation by USAINTA and the FBI. Reports of a Fort Ritchie NCO Club bartender professing to be employed by the "CIA" and "military intelligence" are currently being investigated by USAINTA.

(5) (U) In March 1976, an Army NCO assigned sensitive duties at Fort Ritchie volunteered that he had contacted by letter an agency of the East German Government. The NCO desired to make the matter of the contact part of official records in the event he should be later contacted by any agency or person from East Germany. Though the NCO's action was part of his research of his family history and ostensibly is an overt, sincere effort on his part, the East German Intelligence Services (EGIS) often take such opportunities to make intelligence approaches, especially if the US soldier-target has special clearances and access to sensitive information. The NCO is under instructions to report any responses to his letter.

d (U) Operational Status:

(1) (U) CANARY EFFORT was first approved for implementation by OACSI, DA, on 11 June 1965.

(2) (U) In Feb 76, the 902d MI Group selected Operation CANARY EFFORT to be terminated and replaced by an overt, direct support counterintelligence program. Supported commanders were briefed on the termination action during the quarter ending 31 Mar 76. All confidential sources used in the ICIP have been terminated. The CDR, USAINTA, and the ACSI verbally approved the termination on 20 and 23 Feb 76, respectively.

(3) (C) During the reporting period, b1 b1 $80.00 in TDY and travel, and 3,255 manhours were expended.

(4) (U) The Operation yielded 69 information reports and 116 other reports which were chiefly verbal reports provided to the supported commanders.

e (U) Comments: The ICIP at Fort Ritchie clearly has been a productive operation at a critically sensitive installation. Information obtained as a result of the ICIP and acted upon by the commanders concerned has served to strengthen the security of the installation. The 902d MI Group believes that effective counterintelligence support to the installation can be continued under an overt comprehensive counterintelligence support program, which replaced the present ICIP effective 31 Mar 76.

f (U) Recommendation: None.

~~CONFIDENTIAL~~

Page 2130 of 3957

ICIP REPORT

1 April 1975 to 31 March 1976

(C) CANINE PLATE: (OACSI Revalidation - 4 Feb 75)

a. (U) Location: Seneca Army Depot (SAD), Romulus, NY

b. (U) Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. (U) Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76: There was no significant information obtained during the period and there were no indications of any overt threat to the installation.

d. (C) Operational Status: CANINE PLATE was first approved by OACSI, DA, for implementation on 18 Sep 73. During the reporting period 400 manhours were expended in the ICIP. However, there were no reports submitted, no funds expended, neither TDY nor [b1] There were no confidential sources utilized, only conventional sources.

e. (U) Comments: The installation's mission remains the same, a supply depot for missile and artillery weapons systems with a nuclear capability. The Depot is considered a critical and sensitive installation; therefore, remains as a potential target for HOIS. However, there was no information reported to indicate the presence of any overt threat to the installation. The MI Group has been conducting a thorough review of the ICIP to determine the advisability of terminating the operation.

f. (U) Recommendation: That the ICIP CANINE PLATE be terminated but that increased overt liaison with additional security support be provided the installation commander.

Classified by ODCSUSATA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 3
DECLASSIFY ON: 31 DEC 86

636

[redacted]

ICIP REPORT

1 April 1975 to 31 March 1976

(C) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal, AL

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76:

(1) An inserted covert confidential source was employed in this operation to attempt to learn the existing situation in the Optical Guidance Technology Office (OGTO), Advanced Sensors Directorate, USAMICOM, when reports received in 1974 alleged that lax security practices had led to loss and possible compromise of classified information and that several employees were engaging in sex orgies in offices during the day. In Sep 74, the CG, USAMICOM, conducted a Command Investigation as a result of these reports under the provisions of Army Regulation 15-6. As a result of that investigation, the CG, USAMICOM, requested that an ICIP operation be conducted in OGTO. The Source, once in place, had to rely chiefly upon elicitation to obtain his information because of his covert status, but during the period, did succeed in surfacing adverse suitability information on a civilian physicist with access to sensitive, SECRET information which indicated that he was probably the catalyst for the sexually-oriented activities of the OGTO employees. The employee, apparently obsessed with sex, had numerous extra-marital relations during the last five years. The Commander, USAMICOM, was provided a summary of information on the employee for appropriate command action. The employee transferred to another office in USAMICOM, which apparently broke up the clique and Source could uncover no new evidence of continuing activities among the remaining employees.

(2) In addition to the above, the Source provided substantial information on security weaknesses in the supported command to include poor housekeeping practices, lack of control of reproduction facilities, lack of proper control of area access, lax security attitudes, and possible compromise of security badges through continued losses by individuals. Source provided such security weakness and hazard details to the Project Case Officer who relayed it to overt MI project personnel at Redstone. The Project Liaison Officer provided these reports to the USAMICOM Commanding General and appropriate security personnel who have taken actions to remedy the security weaknesses.

REGRADED UNCLASSIFIED
ON Sep 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

637

d. Operational Status:

(1) CANTER RIDE was first approved by OACSI, DA, for implementation on 4 Mar 75.

(2) During the period, $1,315 in TDY and travel expenses were incurred [redacted] b1 A total of 697 manhours were expended in the operation.

(3) The operation yielded one Summary of Information and several oral reports on security weaknesses.

(4) As the result of an 18 Feb 76 briefing presented to the USAMICOM Commanding General, the MI Group conducting the Operation, the project personnel, and the supported commander concurred in findings that the Operation had accomplished its original objective and should therefore be terminated. The CG, USAMICOM, declared that the operation was a success. The insert Source used in the operation has been withdrawn and reassigned. The CDR, USAINTA, and the ACSI verbally approved the termination of CANTER RIDE on 20 and 23 Feb 76, respectively.

e. Comments: Counterintelligence support continues to be provided by elements of the MI Group stationed at USAMICOM.

f. Recommendation: None.

635

[redacted]

~~CONFIDENTIAL~~

ICIP REPORT

1 April 1975 to 31 March 1976

(C) CANVAS TAX: (OACSI Revalidation - 4 Feb 75)

a. Location: Sierra Army Depot (SIAD), US Army Materiel Command, Herlong, CA

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During the Period 1 April 1975 to 31 March 1976:

(1) Reports alleged the use of illegal drugs by military personnel at SIAD. However, no details were available.

(2) Information was reported that an exclusion area personal identification badge was missing and that an inquiry failed to find or determine how the badge was lost. As a result of the missing badge incident, new identification badges were issued.

(3) An enlisted man assigned to SIAD was charged with malicious damage of a generator at SIAD and his security clearance was revoked by the Commander, SIAD.

d. Operational Status:

(1) During the reporting period 616 manhours were expended and 14 Agent Reports were submitted.

(2) TDY funds totalling $29.35 were expended; there were no b1 expenses.

(3) At the end of the reporting period two confidential sources were being used.

e. Comments:

(1) This ICIP was administratively implemented in April 1974.

(2) The mission of the Sierra Army Depot (SIAD) is the operation of the Depot for the receipt, storage, issue, maintenance, and disposal of missile and artillery weapons with a nuclear capability. Included in the items handled by SIAD are ammunition, special weapons materials, propellants, explosive components of guided missiles, supplies, petroleum and chemical supplies, fire control test and measuring equipment, and other special weapons with a nuclear capability. SIAD also maintains a capability for systems modification in support of the joint AEC/DOD test firing programs.

639

Classified by ...CDR USAINTA.....
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF E.O. 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON ...31 DEC 76...

~~CONFIDENTIAL~~

(3) Sierra Army Depot is the major storage area for special weapons in the western part of the US. The special weapons that formerly were located at the Safeguard anti-Ballistic Missile Site and Savanna Army Depot are now at SIAD, which elevates it to one of the most important special weapons repositories in the US. The Depot is located in a remote area and its contents make it not only of interest to hostile intelligence, but also a target of terrorist groups who are involved in nuclear theft and blackmail.

(4) The Department of Army Sensitive Installation and Unit List, January 1976, lists SIAD as "Critically Sensitive (CS)."

(5) A large portion of the work force is in exclusion areas so access to them on a daily basis is severely restricted for project personnel. Coverage of these areas by confidential sources thus becomes necessary for effective CI coverage. A 20 Sep 75 report of the Nuclear Defense Agency entitled "Adversary View and Support - Nuclear Weapon Site Security; Adversary Capabilities," in assessing terrorist groups tactics employed to acquire a nuclear device and options available, cites the method most likely to succeed as one in which a member of the regular work force has been approached, recruited and is on the terrorist groups payroll. The detection of this type of activity among members of a work force in an exclusion area is greatly enhanced by employing a confidential source program. At the close of the reporting period, two confidential sources were being utilized in the operation to cover the Priority I Exclusion Area. A third individual is under assessment as a potential confidential source.

(6) Hostile intelligence services have high priority collection objectives pertaining to such activities as those conducted at SIAD.

(7) The SIAD, as outlined briefly in subpara (5) and (6), above, appears highly vulnerable to a double threat, that posed by the increasingly active terrorist groups who operate on a global scale and the ever present threat of HoIS penetration. The ICIP is necessary as an additional means to provide "early warnings" to assist the Commander in formulating necessary plans and taking proper action to protect the sensitive and highly-destructive special weapons stored at this location.

(8) At the most recent Quarterly Briefing on 13 Feb 76, the SIAD Commander indicated that he was pleased with the type of support being provided and requested continuation of the ICIP.

f. Recommendation: In view of the above, recommend that ICIP CANVAS TAX be continued.

640

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

ICIP REPORT

1 April 1975 to 31 March 1976

(U) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC.

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During the Period 1 April 1975 to 31 March 1976:

(1) An ICIP source reported that a PTC civilian employee was transferred from the coding and decoding section because he had coded an obscene message that was to be sent to an overseas user. Additionally, the ICIP source provided information concerning possible security violations involving the employee. Because of the employee's questionable suitability characteristics and conduct he was assigned to a job in PTC requiring minimum contact with classified information. Supervisors will continue to monitor his conduct and activities.

(2) An Army NCO assigned to PTC attempted to commit suicide by slashing his wrists. As a result of the information gained concerning the suicide attempt a Limited Investigation was initiated. The NCO was assigned to the Logistics Branch, PTC, pending results of the investigation. The investigation revealed that the NCO has a large number of outstanding debts, has lied on loan applications, and had ordered a 1976 automobile which cost in excess of five thousand dollars. Interviews concerning the NCO revealed alleged drug usage and homosexuality. The Limited Investigation was completed and referred to PTC for adjudication. The decision was made not to revoke the NCO's security clearance since he left the service on 9 April 1976 and will not be allowed to re-enlist.

(3) Adverse suitability information was reported on two additional NCOs assigned to PTC. Based on medical reports and rebellious attitudes one NCO was released from the Army by board action. The second NCO after a night of heavy drinking began hitting his wife when she tried to arouse him after he had "passed out." The wife filed assault charges with the Military Police but withdrew them later. The PTC commander counselled the NCO on his drinking and marital problems and assigned him duties where he has no access to classified information.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by [redacted]
[redacted]
[redacted]
[redacted]

641

CONFIDENTIAL

(4) During the course of an investigation of an enlisted WAC member of PTC who was away-without-leave (KAWOL Investigation), it was discovered that the CID was also investigating her for theft and trafficking in drugs. The MI representative and CID agents coordinated their mutual investigations. PTC has suspended the WAC's access to classified material pending completion of the investigation.

d. Operational Status:

(1) CENSUS TIME was first approved by OACSI, DA, for implementation on 5 Feb 74.

(2) During the period of 1 April 1975 to 31 March 1976, 726 manhours were expended, no TDY nor b1 funds were used. The operation produced seven information reports. One confidential source was used during the period but was terminated during the latter part of the period.

e. Comments: The PTC operations include an extremely high volume of multimedia ultra sensitive compartmented classified traffic processed at the highest level of the military establishment command group being served, and includes the cryptographic operation, maintenance and logistical mission and support rendered to the JCS, the NMCC, departments and executive agencies of the government allied embassies, and the United Nations Building in New York. The installation remains as a potential target for HOIS; however, there was no information reported to indicate the presence of any overt threat to the installation. The MI Group has been conducting a thorough review of the ICIP to determine the advisability of terminating the operation and implementing an overt direct support comprehensive counterintelligence program. In view of the above the continuation of an ICIP is not warranted at this time.

f. Recommendation: That the ICIP CENSUS TIME be terminated and an increased overt liaison with additional direct security support be provided the installation commander.

b42

CONFIDENTIAL

ICIP REPORT

1 April 1975 to 31 March 1976

(C) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories, (HDL), Adelphia, MD

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 - 31 Mar 76:

(1) Information was received that a First Secretary at the USSR Embassy, Washington, DC had visited HDL on two occasions. On one occasion he attended a meeting of the Institute of Electrical and Electronics Engineers, INC., a professional society for engineers which was held in the auditorium of HDL. The subject matter presented during the meeting was unclassified. At a second meeting of the society the Soviet Embassy official was denied entry. A report of the incidents were provided to the FBI and the Commander, HDL, made a determination that the society could no longer hold meetings at HDL in order to preclude any potential security threat.

(2) On two occasions an unidentified light aircraft flew over the test site, Woodbridge Research Facility (WRF), HDL, where a series of tests on foreign equipment under the Range Emory program was in progress. In both instances the aircraft circled over the Range Emory test site for about 5-7 minutes. The overflights are being investigated in coordination with the FBI.

(3) An employee, HDL, made allegations of immoral activities by members of the HDL Security Office and a group at the Van Ness Avenue Facility, HDL. The employee claimed that she was being followed by members of the HDL Security Office. After investigating the employee's story, the Commander, HDL, believed that she was suffering from psychiatric problems and would have her visit a psychiatrist for a complete evaluation.

(4) Suitability information concerning an employee of the Woodbridge Research Facility (WRF) a branch of HDL located in Woodbridge, VA, involved a problem of alcohol abuse. After counseling, the employee participated in a rehabilitation program.

643

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

(5) A courtesy penetration test of HDL's Adelphi Facility was conducted and revealed several security weaknesses which were corrected by the supported command. As a result of the test a number of security guards were transferred and guard procedures were changed. In addition a new magnetic coded badge was approved for purchase in FY 77. As a follow-up implementation of "Lessons Learned" in the penetration test the ICIP Project Liaison Officer (PLO) and the HDL Security Officer prepared and delivered a series of lectures and classes to the HDL guard force on the penetration test. Additionally, the PLO delivered lectures on the penetration test to the faculty and students of the Counterintelligence Dept, US Army Intelligence Corps School, Fort Huachuca, AZ.

d. Operational Status

(1) During the reporting period 880 manhours were expended, 18 information reports were submitted and 41 memorandums were prepared and provided to the supported commander.

(2) No TDY or b1 funds were expended.

e. Comments

(1) ICIP CENTAVO KID was approved by OACSI, DA, 18 Oct 73 and the supported commander was briefed on the implementation of the operation on 12 November 1973.

(2) The mission of the HDL includes critical sensitive research and development activities in support of the US Army. Some of the more sensitive activities include research into the hardening of communications equipment against nuclear weapons radiation; tests of nuclear warhead and missile systems to determine their ability to withstand nuclear weapons radiation; develop fuses for use with nuclear warheads and conducts development and testing of radiation hardened systems for Minutemen and Poseidon Missiles.

(3) The installation remains a potential target for HOIS and the hostile intelligence service have an interest in the research and development activities of the type conducted at HDL. However, the amount of significant information surfaced by the ICIP does not warrant the expenditure of manhours at this time to continue the ICIP.

(4) The MI Group is reviewing the ICIP with a view of terminating the program and instead implementing an overt direct support counterintelligence program.

f. Recommendation: That the ICIP CENTAVO KID be terminated and an overt direct support counterintelligence program be implemented.

644

CONFIDENTIAL

ICIP REPORT

1 April 1975 to 31 March 1976

(U) GONDOLA STAR: (OACSI Revalidation - 16 Jan 76)

a. Location: Aberdeen Proving Ground (APG) and Edgewood Arsenal (EA), Aberdeen, MD

b. Information Obtained Off-Post and/or Reported ob Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76:

(1) Confidential and conventional sources employed in the operation surfaced information on adverse suitability pertaining to 13 employees at Aberdeen Proving Ground/Edgewood Arsenal. The suitability information included alcohol and drug abuse, moral improprieties, fraudulent claim on a TDY voucher and mental instability. Action was taken to substantiate or refute the reported allegations.

(2) Sources reported four instances of alien enlistees who were assigned to the sensitive installations. The Installation Intelligence Officer (IIO) was aware of the status of the four, that they did not have security clearances and had no access to classified information.

(3) Sources reported three instances of foreign travel during the period. One of these individuals who traveled to the USSR after attending a scientific conference in Finland is being exploited as a DOMEX lead. In another instance, a civilian employee visited Poland and Czechoslovakia for about one month in June-July 1975. The employee and his spouse allegedly visited relatives in both countries. The employee has been debriefed by USAINTA. Source reported that the employee plans to travel to these countries again in 1976. In another instance, husband and wife DOD employees took a Smithsonian Institution-sponsored tour to Moscow and Leningrad. The husband has been debriefed by USAINTA and the wife will be debriefed at her convenience. Source reported that the couple planned to take another trip to Russia in 1976.

(4) Sources reported several instances of foreign contact by military and DOD civilian personnel in the supported activity. In one instance a citizen of the Federal Republic of Germany was assigned on an exchange program to work until Sep 76. A report of a civilian DOD at Edgewood Arsenal with some unexplained periods of time in his background prompted a request for a Limited Investigation from the supported command.

Classified by COL USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY
DECLASSIFY ON DEC 11

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

645

(5) Sources reported two instances of Swedish citizens visiting the installations. It was determined that the one visit had been fully coordinated with the proper officials. In the second instance, it was determined that the visit had not been properly coordinated but that steps had been taken to insure the visitors would not be given access to classified information until guidance was provided by higher headquarters.

(6) Sources reported numerous instances of security weaknesses or poor security practices. These included unattended offices in which security containers were left open, a CONFIDENTIAL document left unsecured over a three day weekend, poorly controlled access to a classified scientific conference, movement of an office into a building in which no technical survey had been conducted prior to the move, typewriter ribbons and carbon papers not being disposed of as classified waste, and a high-ranking civilian employee bringing his eight year old son into a controlled access area where a classified test was being conducted and remaining overnight.

d. Operational Status:

(1) GONDOLA STAR was first approved by OACSI, DA for implementation on 21 May 1965. On 18 Feb 75, the ACSI directed the termination of 12 ICIPS, including GONDOLA STAR, by 31 Mar 75. After reviewing correspondence initiated by the Commander, Aberdeen Proving Ground, which recommended that the ICIP GONDOLA STAR be continued, the ACSI reinstated the operation for a period of six months on 11 Jul 75, subject to a review after the six months elapsed. On 16 Jan 76, the ACSI approved continuation of the ICIP as an ongoing operation. The following statistics are for the period 11 Jul 75 to 31 Mar 76:

(2) During the reporting period 2,223 manhours were expended and 84 written information reports and 16 oral reports were submitted. The operation cost $700 in ICF, no TDY funds were expended.

(3) At the end of the reporting period eight confidential sources were being used in the operation.

e. Comments: The ICIP has been a productive operation at a critically sensitive installation. Information obtained as a result of the ICIP and acted upon by the commanders concerned has served to strengthen the security of the installation. The 902d MI Group is conducting a comprehensive review of this operation for possible replacement of the operation by an overt counterintelligence support program.

f. Recommendation: Recommend that ICIP GONDOLA STAR be continued pending completion of the 902d MI Group review.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

646

ICIP REPORT

1 April 1975 to 31 March 1976

(U) LENS HOLDER: (OACSI Revalidation - 4 Feb 75)

a. Location: White Sands Missile Range (WSMR), NM

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76:

(1) Several reports from confidential sources during the period indicated that employees in the TRADOC Systems Analysis Activity (TRASANA) and the Army Missile Test and Evaluation Directorate (ARMTED) were following poor security practices in daily activities and not adhering to security regulations for safeguarding sensitive classified information. These security hazards included leaving security containers open and unattended for periods during the day, failing to complete security forms affixed to classified material containers, leaving classified material in work boxes after duty hours, and laxity on the part of security guards during night shifts. Security Officers of both TRASANA and ARMTED after being provided reports on these weaknesses briefed all their employees on requirements of WSMR Regulation 330-5 (Security Regulation) and reoriented all guard personnel on their security obligations.

(2) A confidential source reported that a US Army Officer assigned to the Office of Missile Electronics Warfare (OMEW) was misappropriating computer parts and electronic equipment which he was taking home to build his own computer. A summary of available information was provided the US Army Criminal Investigation Division Command for investigation by that agency. The same confidential source reported on 4 Feb 76 that two enlisted soldiers in sensitive positions in TRASANA were engaged in drug trafficking, but in separate operations. Local on-post investigation by the White Sands Missile Range Provost Marshal resulted in apprehension of one of the individuals. Information on the second soldier, allegedly involved in large-scale drug transactions and with criminal contacts, was reported to the Sixth Region, US Army Criminal Investigation Division Command for appropriate investigation.

(3) A confidential source reported that unknown persons had attempted on 11 Jan 76 to penetrate TRASANA, which is an Exclusion Area. On 12 Jan 76, the source reported an unidentified individual claiming to be a colonel had been permitted to enter the TRASANA Compound without the required identification. Investigations by the TRASANA security personnel disclosed that there was no substance to the 11 January report and the

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

647

CONFIDENTIAL

person in the 12 January incident was identified and found to be a legitimate entrant into the facility. The incident did serve to illustrate the security awareness of the source and the personnel involved.

(4) A confidential source reported in March 1976 in three reports that devices, such as radios, tape recorders, and "pocket" digital calculators were being brought into a TRASANA Exclusion Area by personnel having access to the area. Many of the computers used in the area have classified information storage and the above-named devices allegedly can affect the computers' operations. The appropriate Security Officer has been appraised of these practices. ICIP project personnel have been tasked to provide follow-up reports on actions taken by the supported command. The information has also been provided as a matter of interest to the Counterintelligence Services and SAVE Team elements at USAINTA.

d. Operational Status:

(1) LENS HOLDER was first approved by the ACSI, DA, for implementation on 16 Sep 74.

(2) Two confidential sources provide coverage of the two principle supported activities, TRASANA and OMEW. An additional individual in the ARMTED is being assessed as a potential source.

(3) During the reporting period, 1,053 manhours were expended. The operation cost b1 there were no TDY outlays. The operation produced 36 written information reports and 24 memorandums and oral reports.

e. Comments:

(1) The mission of the White Sands Missile Range has remained unchanged since the inauguration of the ICIP and the previous OACSI revalidation on 4 Feb 75. The mission of WSMR is to evaluate the Safeguard Missile System missile vulnerability studies, missile control systems, and perform pre-production tests and analyses of missile systems. The mission of WSMR makes it a prime target of hostile intelligence. Activities at WSMR which have Priority I requirements for support are TRASANA, OMEW, ARMTED, the National Range Operations Directorate, and the US Army Safeguard Systems Evaluation Agency. These elements develop electronic countermeasures techniques to nullify vulnerabilities discovered in missile systems, conduct pre-production tests of rocket and guided missile systems, operate a nuclear effects facility and operate National Range Facilities for tests conducted at WSMR.

CONFIDENTIAL

Page 2143 of 3957

(2) The operation to date has proven to have value as an adjunct to the installation security program. The isolation of the installation, disperson of many of its facilities, and the extent and nature of its computer facilities and missile testing ranges present a lucrative target for hostile intelligence service (HoIS) penetration. USMR's proximity to the US-Mexican border renders it vulnerable to HoIS operations based in a foreign country. Admittedly, the operation to date has not surfaced hard evidence of HoIS presence or penetration, but the scope of the threat must be recognized. Details of activities conducted at the site are of current interest to HoIS. The two-pronged capability of the ICIP, that is, extensive use of overt sources of all types, plus the covert effort exemplified by the confidential sources, appears to be a necessary coverage at this time with the best potential for detection and discovery of HoIS activities.

f. Recommendation: Based on the above, recommend that ICIP LENS HOLDER be continued.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

649

ICIP REPORT

1 April 1975 to 31 March 1976

(C) LENTIL MONKEY: (OACSI Revalidation - 4 Feb 75)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76:

(1) A source in the Chinese-Mandarin Language Department furnished information concerning a temporary instructor of that department who closely questioned her students about their knowledge of their future duties and assignments. She frequently expressed her displeasure in the task of teaching Chinese to students which would enable them to "conduct spying activities" directed at the People's Republic of China (PRC). The instructor also displayed a rebellious and uncooperative attitude toward necessary DLI administrative requirements. Born in Canton, China, she was a British citizen and no evidence of a pre-employment investigation could be found. DLI refused to renew her contract when it expired in Sep 75 and she departed DLI in that month.

(2) A Confidential Source reported information on an instructor of the German Language Department who travelled to East Germany in mid-1975 without notification or permission from DLI authorities. Upon completion of the travel, the instructor was admonished officially and informed that any future violation of the DLI regulations on foreign travel would result in temporary suspension.

(3) A visitor to the Russian Language Department in May 75 requested copies of training material used in the Russian Dept, claiming that he wanted it to use for language training in his reserve unit. The visitor was given two unclassified training exercises. Subsequent investigation identified the visitor and established that he was a former graduate of Russian at DLI, and additionally, that he was a bona fide member of a California-based Army Reserve unit. The incident, although not of a major significance as proven by the later investigation, did serve to underscore a need for better visitor control at DLI. The Director, DLI, placed special emphasis on this and the need for all personnel to be alert for unauthorized visitors and proper procedures for handling them. New visitor requirements and restrictions were published and distributed throughout DLI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by ...

650

~~SECRET~~

(4) An instructor in the Hungarian Language Department travelled to Hungary in Sep 75 with a stated purpose of visiting relatives. A review of the instructor's file revealed extensive foreign travel in Europe since 1971 and frequent contact with relatives and other persons in Hungary. File checks and inquiries of other agencies failed to reveal any substantial derogatory information concerning the instructor, but the potential hostage situation is evident in the continuing contacts. Monitoring of the instructor's activities continues.

(5) An ICIP source reported that an instructor in the Russian Language Department allegedly is a former member of the Soviet Army's equivalent to the US Army Security Agency who while in the Soviet Army received special training in English. This instructor left the USSR in Apr 74 and was hired at DLI in Oct 74. A coworker of the instructor left the Soviet Union in Apr 75 and was also hired as an instructor at DLI in Jul 75. Both of the instructors taught together at the Leningrad Herzen Pedagogical Institute in Leningrad in the late 1960s and early 1970s. The sequence of these events illustrate how quickly these individuals are able to secure employment after leaving the USSR, employment in which they are placed in extremely close contact with US intelligence personnel. Monitoring of the activities of these individuals continues.

(6) Two instructors in the Bulgarian Language Department who are man and wife were accused by fellow faculty members at DLI of being communists because of the unexplained details of their emigration to the West and the manner in which they left Bulgaria. The allegations led to charges and countercharges; full details of the incident were provided the FBI. The wife remains at DLI as an instructor, but as of the close of the reporting period on 31 Mar 76, the husband was employed elsewhere and no longer DOD-affiliated.

(7) A DLI employee of the Hebrew Project at DLI also created considerable internal dissension and bickering within the Hebrew Department when he maintained close contact with the Israeli Consulate in San Francisco. This caused associates to become suspicious of his motives and high level contacts. The employee, an alien with an impressive background, including possible intelligence activities, later applied for employment with the National Security Agency (NSA), which has been provided all information available to USAINTA.

(8) A confidential source reported that a Czechoslovakian Language Department (CLD) instructor was planning to withdraw her retirement fund money and return to Czechoslovakia with her two sons, allegedly to live there.

b1 Per FBI

~~SECRET~~

651

Regraded SECRET
ON 20 MAR 1998
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

~~SECRET~~

b1 Referred

At the close of the reporting period possible health problems appeared as a deterrent to the wife's original plans, but definite decisions in this regard are unknown.

b1 Per FBI

(9) A second CLD instructor has disclosed to several sources over the last two years his continuing efforts to obtain the release of his children from Czechoslovakia. The Czech Government recently informed the instructor that he could obtain the release of his children if he pays the Czech Government $66,000 as reimbursement for the cost of the time the instructor spent in a Czech prison and an education tax on the education acquired in Czechoslovakia by the instructor and his wife. The instructor disclosed that the Czech military had changed its method of counting. The reports indicate that the instructor is maintaining close, continuing ties with Czech Government officials and that a hostage situation with his children exists. Monitoring of his activities continues.

(10) Monitoring also continues on activities of a Polish Language Department (PLD) instructor who plans to visit his mother and a brother in Warsaw in mid-1976. The instructor has not applied formally to DLI for approval for the leave and the trip. The instructor frequently has travelled in the past to Europe. His brother, a medical doctor also travels extensively, and has been in the US and Canada often during the last 20 years. During a 1974 visit to the US, the instructor's brother visited DLI, attended PLD functions at DLI, talked with the US Army students at length and photographed many of the students in attendance. US Customs once detained the instructor's brother at the Canadian border for attempting to smuggle Communist propaganda into the US; US Customs confiscated the propaganda.

(11) An instructor in the Russian Language Department apparently is suffering from mental problems. The instructor has written to a California US Senator, a nationally syndicated columnist, and the FBI, alleging that he is constantly under surveillance by the Soviet KGB and US intelligence and further, that his life is in danger. The instructor also has sent a telegram to the President of the United States. Both the FBI and the Secret Service have made inquiries into the matter and conducted local investigations of the instructor. On 23 Mar 76, the DLI Commandant directed the instructor to undergo psychiatric evaluation. Initially, the instructor refused and was suspended from his duties administratively. At the end of the reporting period the instructor agreed to the examination. The results and final disposition are pending.

Regraded ~~SECRET~~
ON 20 MAR 1998
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

652

~~SECRET~~

d. Operational Status:

(1) LENTIL MONKEY was first approved by ACSI, DA, for implementation on 11 September 1967.

(2) During the reporting period, 4,603 manhours were expended. b1 there were no TDY outlays.

(3) Production consisted of 360 written information reports and 220 Memorandums and oral reports.

(4) Eight confidential sources were active in the ICIP at the close of the period and additional coverage of language departments and administrative sections of DLI was obtained by 16 conventional sources.

e. Comments:

(1) The mission of DLI is to train DOD intelligence and communications security specialists in every major foreign language. Military attaches, employees of the CIA and FBI, as well as other federal agencies, are also trained at DLI, making it an extremely enticing target for hostile intelligence service operatives. The majority of the faculty of DLI have foreign backgrounds, some have only recently arrived from Communist Bloc countries and rapidly achieved employment in an installation where most of the students are in intelligence or destined for intelligence assignments upon graduation. Many of these instructors are in hostage situations by virtue of close, living relatives in the ComBloc countries with whom they maintain written contact and closer, if less frequent, personal contact. In maintaining contact with these ComBloc countries for any reason whatsoever, intelligence agencies of those countries in all likelihood have identified the instructors' place of employment and may have contacted them under one guise or another.

(2) In addition to extensive and frequent contacts with the governments of HoIS, many instructors who probably are completely imbued with the American way of life and are now US citizens or who intend to become citizens, nevertheless are vulnerable targets. The instructors acquire personal acquaintances among many intelligence personnel and, in the course of teaching and associating with the military in year-long classes, learn of the students' future assignments and do in some instances correspond with DLI alumnae after graduation. This unique characteristic of conditions at DLI serves to make the Institute an even more attractive target for HoIS approaches.

(3) As shown by statistics in paragraph d(2), and d(3), above, ICIP LENTIL MONKEY is the most productive of all the presently active ICIPS with a total of 360 written reports. Though 4,603 manhours were expended in the project, the actual cash outlay of ICF was $372 for the

year, the lowest cost figure for any of the active ICIPS. Viewed from the cost-yield ratio alone, this operation is an extremely successful, economical effort.

f. Recommendation: In view of the above recommend that ICIP LENTIL MONKEY be retained.

RELEASED UNCLASSIFIED
ON SEP -5 1997 FOI/PO
BY CDR USAINSCOM
AUTH PARA 1-603 DoD 5200.1-R

654

~~CONFIDENTIAL~~

Period: 1 Apr 1975 to 31 Mar 1976

INTERNAL COUNTERINTELLIGENCE PROGRAM

ICIP	INSTALLATION	FIRST INITIATED REVALID	SOURCES AS OF 31 MAR 76 CONF	SOURCES AS OF 31 MAR 76 CONVEN	INFO REPORTS AR, SR SOI	INFO REPORTS OTHER MEMO/ORAL	MAN HOURS	FUNDS TDY	FUNDS b1
CANARY EFFORT	USA Comm Cmd Ft Ritchie, MD	JUN 65 FEB 75	3	9	69	116	3,255	81	b1
CANINE PLATE	Seneca Army Depot, AMC, Romulus, NY	NOV 73 FEB75		5			400		
CANTER RIDE	US Army Msle Cmd Redstone Arsenal, AL	MAR 75	1		1		697	1,315	b1
CANVAS TAX	Sierra Army Depot, AMC, Herlong, CA	APR 74 FEB 75	2	2	14	24	616	29	
CENSUS TIME	Pentagon Telecom Ctr USACC - CONUS, Wash DC	FEB 74 FEB 75		2	7	6	726		
CENTAVO KID	Harry Diamond Labs AMC, Wash DC	NOV 73 FEB 75		7	18	41	880		
GONDOLA STAR	Aberdeen Proving Gd Aberdeen, MD	MAY 65 JAN 76	8	10	84	16	2,223		b1
LENS HOLDER	White Sands Msle Rge, NM, TECOM, AMC	SEP 74 FEB 75	2		36	24	1,053		b1
LENTIL MONKEY	DLI, Pres of M, CA TRADOC	SEP 67 FEB 75	8	16	360	220	4,603		b1
955	TOTAL		24	51	589	447	14,453	1,425	b1

~~CONFIDENTIAL~~

Page 2150 of 3957

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY COR USAINSCOM FOIPO
AUTH PARA 1-603 DoD 5200.1R

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 2 June 1976

ACTION REQUIRED:

To obtain formal ACSI approval for termination of three ICIP operations.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) Background:

-- Contained in USAINTA's 3d Quarter, FY 1976, ICIP Operations Report, 11 May 76, was recommendation to terminate three operations: CANINE PLATE (U) at Seneca Army Depot; CENSUS TIME (U) at Pentagon Telecommunications Center and CENTAVO KID (U) at Harry Diamond Laboratories.

-- USAINTA recommendation based on 902d MI Group review of ICIP's to determine advisability to terminate these ICIP's and replace them by an overt direct support comprehensive CI program.

2. (U) Discussion:

-- After a thorough review of the ICIP report on these operations, it is determined that they can be terminated with no adverse affect on the installations served. Installations concurred.

-- Increased overt liaison with additional security support will be provided the installations by the 902d MI Group. 902d MI Gp Pamphlet No. 381-3, dated 22 Apr 76, outlines the Direct Support Comprehensive Counterintelligence Program (DSCCP) (TAB C) outlines overt liaison procedures without employing confidential sources.

-- ICIP Reports on CANINE PLATE (U), CENSUS TIME (U) and CENTAVO KID (U) are attached at TAB B.

-- With the termination of these ICIP's, there remains four active CONUS ICIP operations.

-- Ltr to USAINTA at TAB A, furnishes formal termination of these ICIP's and instructs USAINTA to conduct review of the remaining four ICIP's to determine need for continuance, and to forward results and recommendations to this office NLT 21 June 1976.

(Continue on plain bond)

IMPLICATIONS	CINPO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		
			DIR		
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

ACTION OFFICER (Name, grade, phone and signature)
Mildred Brannan
M. Brannan/GS-13/53501
656

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

UPGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

DAMI-DOH
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

3. (U) Recommendation: That ltr TAB A be approved by the ACSI and signed.

REGRADED UNCLASSIFIED
ON SEP 5, 1997
BY USAINSCOM FOIPA
Auth Para 4-102 DOD 5200.1R

657

~~CONFIDENTIAL~~

Page 2152 of 3957

~~CONFIDENTIAL~~

DAMI-DOH

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Commander
US Army Intelligence Agency
ATTN: MIIA-SO
Fort Meade, Maryland 20755

1. (U) Reference, 3d Quarter, FY 1976, ICIP Operations Report, wherein you recommended termination of three ICIP operations.

2. (U) ICIP operations, CANINE PLATE (U), CENSUS TIME (U), and CENTAVO KID (U) are formally terminated as recommended.

3. (U) Request that a full review of the remaining four active CONUS ICIP operations be conducted to determine the need for their continuance or discontinuance, and the results, with your recommendations, be forwarded to this office NLT 25 June 76.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

ACSI, DA

658

31 Dec 2006

~~CONFIDENTIAL~~

[redacted]

ICIP REPORT

1 April 1975 to 31 March 1976

(c) CANINE PLATE: (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD), Romulus, NY.

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76: There was no significant information obtained during the period and there were no indications of any overt threat to the installation.

d. Operational Status: CANINE PLATE was first approved by OACSI, DA, for implementation on 18 Sep 73. During the reporting period 400 manhours were expended in the ICIP. However, there were no reports submitted, no funds expended, neither TDY nor b1 There were no confidential sources utilized, only conventional sources.

e. Comments: The installation's mission remains the same, a supply depot for missile and artillery weapons systems with a nuclear capability. The Depot is considered a critical and sensitive installation; therefore, remains as a potential target for HOIS. However, there was no information reported to indicate the presence of any overt threat to the installation. The MI Group has been conducting a thorough review of the ICIP to determine the advisability of terminating the operation.

f. Recommendation: That the ICIP CANINE PLATE be terminated but that increased overt liaison with additional security support be provided the installation commander.

[redacted]

659

ICIP REPORT

1 April 1975 to 31 March 1976

(C) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC.

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During the Period 1 April 1975 to 31 March 1976:

(1) An ICIP source reported that a PTC civilian employee was transferred from the coding and decoding section because he had coded an obscene message that was to be sent to an overseas user. Additionally, the ICIP source provided information concerning possible security violations involving the employee. Because of the employee's questionable suitability characteristics and conduct he was assigned to a job in PTC requiring minimum contact with classified information. Supervisors will continue to monitor his conduct and activities.

(2) An Army NCO assigned to PTC attempted to commit suicide by slashing his wrists. As a result of the information gained concerning the suicide attempt a Limited Investigation was initiated. The NCO was assigned to the Logistics Branch, PTC, pending results of the investigation. The investigation revealed that the NCO has a large number of outstanding debts, has lied on loan applications, and had ordered a 1976 automobile which cost in excess of five thousand dollars. Interviews concerning the NCO revealed alleged drug usage and homosexuality. The Limited Investigation was completed and referred to PTC for adjudication. The decision was made not to revoke the NCO's security clearance since he left the service on 9 April 1976 and will not be allowed to re-enlist.

(3) Adverse suitability information was reported on two additional NCOs assigned to PTC. Based on medical reports and rebellious attitudes one NCO was released from the Army by board action. The second NCO after a night of heavy drinking began hitting his wife when she tried to arouse him after he had "passed out." The wife filed assault charges with the Military Police but withdrew them later. The PTC commander counselled the NCO on his drinking and marital problems and assigned him duties where he has no access to classified information.

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

Classified by ODR USAINSTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 06

6601

(4) During the course of an investigation of an enlisted WAC member of PTC who was away-without-leave (KAWOL Investigation), it was discovered that the CID was also investigating her for theft and trafficking in drugs. The MI representative and CID agents coordinated their mutual investigations. PTC has suspended the WAC's access to classified material pending completion of the investigation.

d. Operational Status:

(1) CENSUS TIME was first approved by OACSI, DA, for implementation on 5 Feb 74.

(2) During the period of 1 April 1975 to 31 March 1976, 726 manhours were expended, no TDY nor b1 were used. The operation produced seven information reports. One confidential source was used during the period but was terminated during the latter part of the period.

e. Comments: The PTC operations include an extremely high volume of multimedia ultra sensitive compartmented classified traffic processed at the highest level of the military establishment command group being served, and includes the cryptographic operation, maintenance and logistical mission and support rendered to the JCS, the NMCC, departments and executive agencies of the government allied embassies, and the United Nations Building in New York. The installation remains as a potential target for HOIS; however, there was no information reported to indicate the presence of any overt threat to the installation. The MI Group has been conducting a thorough review of the ICIP to determine the advisability of terminating the operation and implementing an overt direct support comprehensive counterintelligence program. In view of the above the continuation of an ICIP is not warranted at this time.

f. Recommendation: That the ICIP CENSUS TIME be terminated and an increased overt liaison with additional direct security support be provided the installation commander.

Page 2156 of 3957

ICIP REPORT

1 April 1975 to 31 March 1976

(C) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories, (HDL), Adelphia, MD

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 - 31 Mar 76:

(1) Information was received that a First Secretary at the USSR Embassy, Washington, DC had visited HDL on two occasions. On one occasion he attended a meeting of the Institute of Electrical and Electronics Engineers, INC., a professional society for engineers which was held in the auditorium of HDL. The subject matter presented during the meeting was unclassified. At a second meeting of the society the Soviet Embassy official was denied entry. A report of the incidents were provided to the FBI and the Commander, HDL, made a determination that the society could no longer hold meetings at HDL in order to preclude any potential security threat.

(2) On two occasions an unidentified light aircraft flew over the test site, Woodbridge Research Facility (WRF), HDL, where a series of tests on foreign equipment under the Range Emory program was in progress. In both instances the aircraft circled over the Range Emory test cite for about 5-7 minutes. The overflights are being investigated in coordination with the FBI.

(3) An employee, HDL, made allegations of immoral activities by members of the HDL Security Office and a group at the Van Ness Avenue Facility, HDL. The employee claimed that she was being followed by members of the HDL Security Office. After investigating the employee's story, the Commander, HDL, believed that she was suffering from psychiatric problems and would have her visit a psychiatrist for a complete evaluation.

(4) Suitability information concerning an employee of the Woodbridge Research Facility (WRF) a branch of HDL located in Woodbridge, VA, involved a problem of alcohol abuse. After counseling, the employee participated in a rehabilitation program.

DECLASSIFIED UNCLASSIFIED
SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1

(5) A courtesy penetration test of HDL's Adelphi Facility was conducted and revealed several security weaknesses which were corrected by the supported command. As a result of the test a number of security guards were transferred and guard procedures were changed. In addition a new magnetic coded badge was approved for purchase in FY 77. As a follow-up implementation of "Lessons Learned" in the penetration test the ICIP Project Liaison Officer (PLO) and the HDL Security Officer prepared and delivered a series of lectures and classes to the HDL guard force on the penetration test. Additionally, the PLO delivered lectures on the penetration test to the faculty and students of the Counterintelligence Dept, US Army Intelligence Corps School, Fort Huachuca, AZ.

d. Operational Status

(1) During the reporting period 880 manhours were expended, 18 information reports were submitted and 41 memorandums were prepared and provided to the supported commander.

(2) No TDY or b1 were expended.

e. Comments

(1) ICIP CENTAVO KID was approved by OACSI, DA, 18 Oct 73 and the supported commander was briefed on the implementation of the operation on 12 November 1973.

(2) The mission of the HDL includes critical sensitive research and development activities in support of the US Army. Some of the more sensitive activities include research into the hardening of communications equipment against nuclear weapons radiation; tests of nuclear warhead and missile systems to determine their ability to withstand nuclear weapons radiation; develop fuses for use with nuclear warheads and conducts development and testing of radiation hardened systems for Minutemen and Poseidon Missiles.

(3) The installation remains a potential target for HOIS and the hostile intelligence service have an interest in the research and development activities of the type conducted at HDL. However, the amount of significant information surfaced by the ICIP does not warrant the expenditure of manhours at this time to continue the ICIP.

(4) The MI Group is reviewing the ICIP with a view of terminating the program and instead implementing an overt direct support counterintelligence program.

f. Recommendation: That the ICIP CENTAVO KID be terminated and an overt direct support counterintelligence program be implemented.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 2 June 1976

ACTION REQUIRED

To obtain formal ACSI approval for termination of three ICIP operations.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) Background:

-- Contained in USAINTA's 3d Quarter, FY 1976, ICIP Operations Report, 11 May 76, was recommendation to terminate three operations: CANINE PLATE (U) at Seneca Army Depot; CENSUS TIME (U) at Pentagon Telecommunications Center and CENTAVO KID (U) at Harry Diamond Laboratories.

-- USAINTA recommendation based on 902d MI Group review of ICIP's to determine advisability to terminate these ICIP's and replace them by an overt direct support comprehensive CI program.

2. (U) Discussion:

-- After a thorough review of the ICIP report on these operations, it is determined that they can be terminated with no adverse affect on the installations served. Installations concurred.

-- Increased overt liaison with additional security support will be provided the installations by the 902d MI Group. 902d MI Gp Pamphlet No. 381-3, dated 22 Apr 76, outlines the Direct Support Comprehensive Counterintelligence Program (DSCCP) (TAB C) outlines overt liaison procedures without employing confidential sources.

-- ICIP Reports on CANINE PLATE (U), CENSUS TIME (U) and CENTAVO KID (U) are attached at TAB B.

-- With the termination of these ICIP's, there remains four active CONUS ICIP operations.

-- Ltr to USAINTA at TAB A, furnishes formal termination of these ICIP's and instructs USAINTA to conduct review of the remaining four ICIP's to determine need for continuance, and to forward results and recommendations to this office NLT 21 June 1976.

(Continue on plain bond)

IMPLICATIONS CINFO YES ☐ NO ☐ PRIM PROGS YES ☐ NO ☐ BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		4
			DIR		4 June 76.
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

ACTION OFFICER (Name, grade, phone and signature)
M. Brannan/GS-13/53501
664

ACSI FORM 21, 13 Sep 71

~~CONFIDENTIAL~~

REGRADED WHEN SEPARATED FROM CLASSIFIED ENCLOSURE

CONFIDENTIAL

DAMI-DOH
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

3. (U) Recommendation: That ltr TAB A be approved by the ACSI and signed.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

665

CONFIDENTIAL

Page 2160 of 3957

~~CONFIDENTIAL~~

3 JUL 1976

DAMI-DOH

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Commander
US Army Intelligence Agency
ATTN: MIIA-SO
Fort Meade, Maryland 20755

1. (U) Reference, 3d Quarter, FY 1976, ICIP Operations Report, wherein you recommended termination of three ICIP operations.

2. (U) ICIP operations, CANINE PLATE (U), CENSUS TIKE (U), and CENTAVO KID (U) are formally terminated as recommended.

3. (U) Request that a full review of the remaining four active CONUS ICIP operations be conducted to determine the need for their continuance or discontinuance, and the results, with your recommendations, be forwarded to this office NLT 28 June 76.

(sgd) Harold R. Aaron

HAROLD R. AARON
Major General, GS
Acting for the Director

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

ACSI, DA

666

31 Dec 2006

~~CONFIDENTIAL~~

CONFIDENTIAL

ICIP REPORT

1 April 1975 to 31 March 1976

(C) CANINE PLATE: (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD), Romulus, NY.

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 to 31 Mar 76: There was no significant information obtained during the period and there were no indications of any overt threat to the installation.

d. Operational Status: CANINE PLATE was first approved by OACSI, DA, for implementation on 18 Sep 73. During the reporting period 400 manhours were expended in the ICIP. However, there were no reports submitted, no funds expended, neither TDY nor b1 There were no confidential sources utilized, only conventional sources.

e. Comments: The installation's mission remains the same, a supply depot for missile and artillery weapons systems with a nuclear capability. The Depot is considered a critical and sensitive installation; therefore, remains as a potential target for HOIS. However, there was no information reported to indicate the presence of any overt threat to the installation. The MI Group has been conducting a thorough review of the ICIP to determine the advisability of terminating the operation.

f. Recommendation: That the ICIP CANINE PLATE be terminated but that increased overt liaison with additional security support be provided the installation commander.

Classified by: OCS 4.3(a)(3)
EXEMPTION
DECLASSIFY ON:

667

ICIP REPORT

1 April 1975 to 31 March 1976

(S) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC.

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During the Period 1 April 1975 to 31 March 1976:

(1) An ICIP source reported that a PTC civilian employee was transferred from the coding and decoding section because he had coded an obscene message that was to be sent to an overseas user. Additionally, the ICIP source provided information concerning possible security violations involving the employee. Because of the employee's questionable suitability characteristics and conduct he was assigned to a job in PTC requiring minimum contact with classified information. Supervisors will continue to monitor his conduct and activities.

(2) An Army NCO assigned to PTC attempted to commit suicide by slashing his wrists. As a result of the information gained concerning the suicide attempt a Limited Investigation was initiated. The NCO was assigned to the Logistics Branch, PTC, pending results of the investigation. The investigation revealed that the NCO has a large number of outstanding debts, has lied on loan applications, and had ordered a 1976 automobile which cost in excess of five thousand dollars. Interviews concerning the NCO revealed alleged drug usage and homosexuality. The Limited Investigation was completed and referred to PTC for adjudication. The decision was made not to revoke the NCO's security clearance since he left the service on 9 April 1976 and will not be allowed to re-enlist.

(3) Adverse suitability information was reported on two additional NCOs assigned to PTC. Based on medical reports and rebellious attitudes one NCO was released from the Army by board action. The second NCO after a night of heavy drinking began hitting his wife when she tried to arouse him after he had "passed out." The wife filed assault charges with the Military Police but withdrew them later. The PTC commander counselled the NCO on his drinking and marital problems and assigned him duties where he has no access to classified information.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by Auth USAINTA
DECLASSIFICATION
DECL ON: DEC 06

668

CONFIDENTIAL

(4) During the course of an investigation of an enlisted WAC member of PTC who was away-without-leave (AWOL Investigation), it was discovered that the CID was also investigating her for theft and trafficking in drugs. The MI representative and CID agents coordinated their mutual investigations. PTC has suspended the WAC's access to classified material pending completion of the investigation.

d. Operational Status:

(1) CENSUS TIME was first approved by OACSI, DA, for implementation on 5 Feb 74.

(2) During the period of 1 April 1975 to 31 March 1976, 726 manhours were expended, no TDY nor b1 were used. The operation produced seven information reports. One confidential source was used during the period but was terminated during the latter part of the period.

e. Comments: The PTC operations include an extremely high volume of multimedia ultra sensitive compartmented classified traffic processed at the highest level of the military establishment command group being served, and includes the cryptographic operation, maintenance and logistical mission and support rendered to the JCS, the NMCC, departments and executive agencies of the government allied embassies, and the United Nations Building in New York. The installation remains as a potential target for HOIS; however, there was no information reported to indicate the presence of any overt threat to the installation. The MI Group has been conducting a thorough review of the ICIP to determine the advisability of terminating the operation and implementing an overt direct support comprehensive counterintelligence program. In view of the above the continuation of an ICIP is not warranted at this time.

f. Recommendation: That the ICIP CENSUS TIME be terminated and an increased overt liaison with additional direct security support be provided the installation commander.

CONFIDENTIAL

Page 2164 of 3957

[redacted]

ICIP REPORT

1 April 1975 to 31 March 1976

(2) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories, (HDL), Adelphia, MD

b. Information Obtained Off-Post and/or Reported on Non-Affiliated Civilians: None

c. Significant Information Obtained During Period 1 Apr 75 - 31 Mar 76:

(1) Information was received that a First Secretary at the USSR Embassy, Washington, DC had visited HDL on two occasions. On one occasion he attended a meeting of the Institute of Electrical and Electronics Engineers, INC., a professional society for engineers which was held in the auditorium of HDL. The subject matter presented during the meeting was unclassified. At a second meeting of the society the Soviet Embassy official was denied entry. A report of the incidents were provided to the FBI and the Commander, HDL, made a determination that the society could no longer hold meetings at HDL in order to preclude any potential security threat.

(2) On two occasions an unidentified light aircraft flew over the test site, Woodbridge Research Facility (WRF), HDL, where a series of tests on foreign equipment under the Range Emory program was in progress. In both instances the aircraft circled over the Range Emory test cite for about 5-7 minutes. The overflights are being investigated in coordination with the FBI.

(3) An employee, HDL, made allegations of immoral activities by members of the HDL Security Office and a group at the Van Ness Avenue Facility, HDL. The employee claimed that she was being followed by members of the HDL Security Office. After investigating the employee's story, the Commander, HDL, believed that she was suffering from psychiatric problems and would have her visit a psychiatrist for a complete evaluation.

(4) Suitability information concerning an employee of the Woodbridge Research Facility (WRF) a branch of HDL located in Woodbridge, VA, involved a problem of alcohol abuse. After counseling, the employee participated in a rehabilitation program.

[redacted]

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

670

(5) A courtesy penetration test of HDL's Adelphi Facility was conducted and revealed several security weaknesses which were corrected by the supported command. As a result of the test a number of security guards were transferred and guard procedures were changed. In addition a new magnetic coded badge was approved for purchase in FY 77. As a follow-up implementation of "Lessons Learned" in the penetration test the ICIP Project Liaison Officer (PLO) and the HDL Security Officer prepared and delivered a series of lectures and classes to the HDL guard force on the penetration test. Additionally, the PLO delivered lectures on the penetration test to the faculty and students of the Counterintelligence Dept, US Army Intelligence Corps School, Fort Huachuca, AZ.

d. Operational Status

(1) During the reporting period 880 manhours were expended, 13 information reports were submitted and 41 memorandums were prepared and provided to the supported commander.

(2) No TDY or b1 were expended.

e. Comments

(1) ICIP CENTAVO KID was approved by OACSI, DA, 18 Oct 73 and the supported commander was briefed on the implementation of the operation on 12 November 1973.

(2) The mission of the HDL includes critical sensitive research and development activities in support of the US Army. Some of the more sensitive activities include research into the hardening of communications equipment against nuclear weapons radiation; tests of nuclear warhead and missile systems to determine their ability to withstand nuclear weapons radiation; develop fuses for use with nuclear warheads and conducts development and testing of radiation hardened systems for Minutemen and Poseidon Missiles.

(3) The installation remains a potential target for HOIS and the hostile intelligence service have an interest in the research and development activities of the type conducted at HDL. However, the amount of significant information surfaced by the ICIP does not warrant the expenditure of manhours at this time to continue the ICIP.

(4) The MI Group is reviewing the ICIP with a view of terminating the program and instead implementing an overt direct support counterintelligence program.

f. Recommendation: That the ICIP CENTAVO KID be terminated and an overt direct support counterintelligence program be implemented.

671

CONFIDENTIAL

Want to
review right to
see if
with -
while.

I
assume you
will include this
on daily spot to
DIA
and

~~SENSITIVE~~

HAND CARRY

~~SENSITIVE~~

Page 2167 of 3957

THIS MUST REMAIN T O P D O C U M E N T

DOSSIER NO. ZF011946W
Vol 6 of 7 Vols

As of 18 Sep 85 (Date) all material included in this file conforms with DA policies currently in effect.

Delmar Smith (Signature) 18 Sep 85 (Date Signed)

Delmar Smith (Printed Name) GS5 (Grade)

Reviewed for Retention
Criteria UP AR 381-10
Reviewer [illegible] Date 4 Jan 92

THIS MUST REMAIN T O P D O C U M E N T

IA (HQ) Form 2214
(1 Sep 78)

Replaces MIIA Fm 315, 1 Jun 75, which may be used until supplies are exhausted.

673

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO WITH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 21 May 76

ACTION REQUIRED: To obtain approval/disapproval to USAREUR ICIP OPLAN on USASA Field Station Berlin (USASAFSB) (C)

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (C) Background:

-- Since 1970, Project FILMAN has provided support to USASA Field Station Berlin (USASAFSB). FILMAN was designed to use sources from the local work force and personnel located in establishments frequented by the work force. Problems encountered from peripheral nature of sources and their difficulty in becoming accepted into USASA circles. See TAB B.

-- Cdr, 766th MID proposed an Aggressive Defensive Source Acquisition Program (ADSAP) support arrangement for USASAFSB which would provide more direct source access and control of source coverage.

-- In August 1975, Cdr USASAFSB and DCSSEC, HQ USASA concurred in proposal. In September 1975, ACSI, DA and DCSI, USAREUR briefed and supported concept. In October 1975, Cdr, USASA concurred in cancellation of FILMAN and initiation of ADSAP. (See TAB C) Subsequently, concept discarded in favor of subject ICIP.

-- By ltr 28 April 1976, DCSI, USAREUR forwarded subject ICIP for ACSI approval.

2. (U) Discussion:

-- Purpose of subject ICIP is to collect significant CI information through use of overt liaison contacts, casual sources and confidential recruited sources assigned to USASAFSB. Sources will be specifically targeted against Hostile Intelligence Services (HOIS) activities directed toward USASA and against security vulnerabilities of USASA personnel.

-- On 14 May 1976, DCSSEC, HQ USASA, reviewed subject ICIP and concurred in OPLAN. The DCSSEC recommended deletion of coordination with Cdr, USASA Europe (Para 2b(4)(c), "in view of realignment of functions and need for compartmentation, coordination reflected in para 4e(2) is sufficient." (TAB A)

(Continue on plain bond)

IMPLICATIONS CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			DR		
			DIV		24 May 76
			DIR		
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*
Miss Brannan/53501

634
5702-76

ACSI, DA

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

DAMI-DOH
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

-- 3d Indorsement, TAB A, the ACSI, DA informs DCSI, USAREUR that subject ICIP approved.

3. (U) Recommendation: That 3d Indorsement (TAB A) be approved and signed.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

675

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

19 SEP 1975

19 SEP 1975

AEUMI-BCK

SUBJECT: Project Filman (U)

Commander
USASAFSB
ATTN: S-2
APO 09742

1. (U) The purpose of this proposed action is to provide increased and improved counterintelligence support to the US Army Security Agency Field Station, Berlin (USASAFSB).

2. (U) In 1970, a CI operations plan was submitted by Berlin Field Station, 66th MI Group, to correspond with the activation of the USASAFSB site known as "Teufelsberg". The operations plan was ~~designed to provide counterintelligence support to the project through the utilization of sources, either among the local work force or through personnel located in establishments frequented by the work force. Because the local work force was too transient in nature to effectively insert a source before they completed work on site, source recruitment efforts were concentrated on individuals who associated with ASA personnel at local entertainment establishments and at social functions.~~ Initially through coordination with the S-2, USASAFSB, a list of establishments frequented by USASAFSB personnel was prepared and attempts were made to introduce sources into some of the establishments. We presently have ~~six sources under the Filman project who have provided limited information.~~ However, to date these sources have provided routine ~~information of low level CI significance, primarily of interest to US Army Berlin Brigade and not to USASAFSB. In approximately 1973, USASA withdrew financial support of Filman and fiscal responsibility reverted to the 66th MI Group. The primary difficulty with the Filman project has been the peripheral nature of the sources and their difficulty in becoming accepted into ASA circles, since ASA personnel appear to associate in fairly close knit ASA circles. In short, peripheral sources have provided only peripheral leads.~~

CLASSIFIED BY: Cdr, 66th MI Group
EXEMPT FROM GDS OF EO 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON: Notification by Originator

REGRADED UNCLASSIFIED
ON SEP 1987
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

676

INCL # 1

~~CONFIDENTIAL~~

DECLASSIFIED AUTHORITY

~~CONFIDENTIAL~~

19 SEP 1975

AEUMI-BCE
SUBJECT: Project Filman (U)

3. (U) I ~~propose~~ that the ~~Filman project be cancelled~~, that permission be granted to recruit ASA personnel within USASAFSB, and ~~that the Aggressive Defensive Source Acquisition Program (ADSAP) be used as the vehicle to provide defensive counterespionage support to USASAFSB.~~ A brief description of ADSAP and general ADSAP EEI is attached as Inclosure. This would enhance CI coverage of USASAFSB by providing more flexibility within the framework of one source program, access to the target areas and target personalities, a wider range of operations for sources, and more streamlined administrative procedures for the management of sources. Current Filman sources will be converted to the ADSAP program. Sources will be preferably recruited within the target activity to provide information on personalities and activities. Additional sources will be recruited on the periphery or outside of the target sites in order to enhance overall CI coverage. Once it has been determined where a possible shortfall of information occurs, a concerted effort will be made to obtain sources who can provide that information. Indiscriminant selection and recruitment of sources will be avoided and emphasis will be placed on a prospective source's ability to fulfill the requirements levied on him. 766th MID will provide the S-2, USASAFSB with the desired qualifications for personnel to be utilized in the program and he will be requested to screen present personnel assigned to his unit to determine those best qualified for recruitment. ADSAP will not supplant the S-2, USASAFSB program of internal informants, but will augment his present activities. A target analysis will be prepared by this Detachment in coordination with the S-2, USASAFSB. ~~Information solely of a suitability nature, will be reported directly to the S-2, USASAFSB.~~ All other information will be reported in accordance with reporting requirements, as outlined in LOI 6-TD, 66th MI Group.

4. (U) Preliminary discussions, conducted in August 1975, with the Commander, USASAFSB, the Deputy Chief of Staff, Security, USASA Headquarters, Arlington Hall, Virginia, and the Commander, 66th MI Group, indicated a favorable response to the above proposal.

5. (U) This Detachment requests your comments, recommendations, and approval of the above proposal.

1 Incl
as

ALLYN C. HOULTRY
LTC, MI
Commanding

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

2

677

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

AGGRESSIVE DEFENSIVE SOURCE ACQUISITION PROGRAM (ADSAP)

ADSAP concerns itself with two categories of human sources as defined by 66th MI Group LOI Number 6-TD. These two source categories are Conventional and Confidential. The ADSAP is a CI threat information collection program and sources recruited under this program should not be recruited for coverage of a specific CE target. Sources are recruited within and on the periphery of sensitive installations and activities by combining both active and passive measures to counter the information collection capability of hostile intelligence services (HoIS) operating against US Forces. The passive measures are designed to protect defense information from unauthorized disclosure or compromise, while the aggressive measures are designed to obtain information which will lead to the detection and neutralization of HoIS efforts directed against US Forces.

General ADSAP EEI:

a. Detection of suspicious activities, undue inquisitiveness or obvious lack of good security practices on the part of or involving US Forces personnel.

b. Identification of US Forces personnel who closely and continually associate with foreign nationals having connections with Soviet Bloc countries.

c. Identification of US forces personnel who make unauthorized or frequent authorized travel to Soviet Bloc countries.

d. Identification of US Forces personnel who have continued contact with local national personnel.

e. Detection of disaffected personnel.

f. Identification of US Forces personnel whose activities and/or character weaknesses either individually or in a combination constitute a clear and significant threat to US Forces in that they have rendered the US Forces connected personnel susceptible to exploitation by HoIS. Susceptibility to HoIS exploitation because of adverse suitability factors should be coupled with at least one of the foregoing indicators of possible HoIS interest. Specific suitability factors which could render US Forces personnel vulnerable to HoIS exploitation would be excessive indebtedness or recurring financial difficulties; unexplained affluence; conduct such as criminal, immoral or homosexual acts which could render

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

678

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

the individual susceptible to pressure; current and past mental and emotional instability; unusual work habits that do not conform to the daily pattern of fellow employees, sudden unexplained changes in working or social habits; sexual misconduct; infidelity; marital problems; trading on the interzonal routes or otherwise utilizing linguistic capabilities with Soviet or other bloc personnel in unauthorized situations.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

IAER-I

7 OCT 1975

SUBJECT: Aggressive Defensive Source Acquisition Program (ADSAP) (U)

Commander
US Army Security Agency
ATTN: DCSSEC
Arlington Hall Station
Arlington, Virginia 22212

1. (C) Attached is a copy of a letter received on 19 September 1975 from Commander, 766th Military Intelligence Detachment, 66th MI Group, entitled "Project FILMAN". The letter is self explanatory but can be summarized as follows: Counterintelligence support to USASAFS Berlin has been conducted since 1970 under the provisions of FILMAN. Although FILMAN was satisfactory in concept, it suffered from a lack of precise support definition, particularly in source acquisition and reporting.

2. (C) Cdr, 766th MID, proposes an ADSAP support arrangement which would provide more direct source access to USASA personnel and direct control of source coverage of actual or potential espionage approaches. Cdr, USASAFS Berlin concurs in the concept and desires to implement the program. COL Holden was briefed on the program during his visit to Berlin in August 1975 and concurred in the proposal. MG Aaron, DA ACSI, and MG Dillard, USAREUR DCSI, were also briefed in September 1975 and supported the concept.

3. (C) Request your concurrence in cancellation of Project FILMAN and adoption of the ADSAP by USASAFS Berlin/766th MID. Appropriate safeguards will be maintained with regard to withdrawal of USASA sources should hostile intelligence interest focus on a USASA soldier. Request a reply as soon as possible so we can begin negotiating a new Memorandum of Understanding with 66th MI Group.

FOR THE COMMANDER:

1 Incl
as

GERALD J. REIMAN
MAJ, MI
Asst Adjutant

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by C2K USASAFS B
SCHEDULE OF EXECUTIVE ORDER 11652
DECLASSIFY ON: NOTICE OF ORIGINATOR

680

INCL #2

DEPARTMENT OF THE ARMY
UNITED STATES ARMY SECURITY AGENCY
ARLINGTON HALL STATION
ARLINGTON, VIRGINIA 22212

IACG

20 OCT 1975

SUBJECT: Aggressive Defensive Source Acquisition Program (ADSAP) (U)

Commander
USASA Field Station, Berlin
APO New York 09742

1. (U) Reference IAEB-L Letter, dated 7 October 1975, Subject: Aggressive Defensive Source Acquisition Program (ADSAP) (U).

2. (S) I concur in cancellation of Project FILMAN and initiation of the Aggressive Defensive Source Acquisition Program by the 766th MID, 66th MI Group. A copy of the completed Memorandum of Understanding will be provided to this HQ, ATTN: DCSSEC.

for WILLIAM I. ROLYA
Brigadier General, USA
Commanding

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by DoD 5200.1-R
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Upon Expiration

INCL # 3

681

~~CONFIDENTIAL~~

ROUTING AND TRANSMITTAL SLIP

1 TO: Mr Kelly	INITIALS	CIRCULATE	ACTION
	DATE	COORDINATION	
2	INITIALS	FILE	
	DATE	INFORMATION	
3	INITIALS	NOTE AND RETURN	
	DATE	PER CONVERSATION	
4	INITIALS	SEE ME	
	DATE	SIGNATURE	

Mr. Kelly has green copy for file

for-

REMARKS

Believe you (or I) should orally brief HCSI, get his approval, and then you sign for him.

I ADEROSA signed for the DCSI

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM	DATE	PHONE
John L. Peter III Colonel, GS 682	21 MAY 1976	76079

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41CFR) 100-11.206

5041-101-01

* GPO : 1975-588-906

REGRADED UNCLASSIFIED ON SEP 1997 BY CDR USAINSCOM FOIPO AUTH PARA 1-603 DoD 5200.1-R

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 21 May 1976

ACTION REQUIRED

To obtain approval/disapproval to terminate ODCSI, USAREUR ICIP CARELESS TOKEN (U).

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1 (U) Background:

-- ICIP CARELESS TOKEN approved by ACSI on 25 Feb 76.

-- ICIP designed to detect and counter vulnerability to espionage by USASA personnel assigned to Det N, USASA Field Station, Augsburg, (USASAFSA) FRG.

2 (U) Discussion:

-- On 5 April 76, CDR 511th MI Bn recommended that ICIP be terminated. On 9 Apr 76, ODCSI, USAREUR, and on 14 May 76 DCSSEC HQUSASA concurred in recommendation to terminate.

-- Rationale for termination:

o Drawdown of USASA Det. Only seven USASA personnel now assigned to station.

o Drawdown precludes further expenditure of CI assets and efforts required by CARELESS TOKEN.

o NCOIC Det N appears completely competent to accomplish duties and control subordinates.

o Regular contact between PLO and NCOIC, and occasional casual contact between PLO and USASA Det N personnel on an opportunity basis can accomplish goals of this ICIP. Pertinent info derived from such contacts would be reported promptly to S2, USASAFS Augsburg.

-- 3d Ind (Red TAB A) informs ODCSI, USAREUR that ACSI, DA approves termination of CARELESS TOKEN.

(Continue on plain bond)

IMPLICATIONS — CINFO YES ☐ NO ☐ | FRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BB		
			DIV		
			DIR		21 26 May
			EX		
			ACSI		
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

ACTION OFFICER (Name, grade, phone and signature)
M. BRANNAN/GS-13/53501

683

ACSI FORM 28, 13 Sep 71

CONFIDENTIAL

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

DAMI-DOH
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

3. (U) Recommendation: That 3d Ind (Red TAB A) be approved by the ACSI and signed by the DO for the ACSI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

684

~~CONFIDENTIAL~~

Page 2179 of 3957

DAMI-DOH (9 Apr 76) 3d Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U) 21 MAY 1976

HQDA, Office of the Assistant Chief of Staff for Intelligence, The Pentagon, Washington, DC 20310

TO: Commander-in-Chief, US Army Europe and Seventh Army, ATTN: AEAGB-CI(SO), APO New York 09403

Your recommendation to terminate CARELESS TOKEN is approved.

FOR THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE:

(sgd) Merrill T. Kelly

1 Incl
nc

MERRILL T. KELLY
Acting Director of Intelligence Operations

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

685

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAISC DOI/PO
AUTH PARA 2-200.1-R

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY, EUROPE and SEVENTH ARMY
APO 09403

9 APR 1976

AEAGB-CI(SO)

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

HQDA (DAMI-DOH)
WASH DC 20310

1. (U) References:

a. Operations Plan, 66th MI Group, 5 May 1975, subject as above, with 5th Indorsement, DAMI-DOH, OACSI, DA, 25 February 1976 (C).

b. Letter, AEAGB-CI(SO), USAREUR, 10 February 1976, subject as above (C).

2. (U) Attached is the Quarterly Status Report pertaining to the ICIP CARELESS TOKEN for the period ending 1 April 1976.

3. (~~C~~) This office concurs in the recommendation by the 511th MI Battalion that this ICIP be terminated. The diminishing sensitivity of the target activity, and reduction in target personnel would appear not to justify the futher expenditure of counterintelligence assets and efforts required by this ICIP. Consequently this office is directing initiation of formal coordination with US Army Security Agency (USASA), Field Station Augsburg for the purpose of terminating CARELESS TOKEN.

4. (U) Request HQ, USASA be advised of USAREUR plans to terminate this ICIP. Comments in this regard by your office and HQ USASA would be appreciated.

5. (U) ODCSI, USAREUR, Action Officer is Mr David R. Smith, AEAGB-CI(SO), HM 7354 (AUTOSEVOCOM 6742).

FOR THE DEPUTY CHIEF OF STAFF, INTELLIGENCE:

W. J. IADEROSA
Colonel, GS
Chief, Counterintelligence Division

1 Incl
as

CLASSIFIED BY ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY (2)
DECLASSIFY ON (APPROVAL OF ACSI, DA)

686

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DAMI-DOH (9 Apr 76) 1st Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

DA, OACofS for Intelligence, ATTN: DAMI-DOH, Washington, DC 20310 1 3 MAY 19

TO: Commander, US Army Security Agency, ATTN: DCSSEC, Arlington Hall Station, Arlington, VA 22212

1. (C) This office concurs in the DCSI, USAREUR recommendation that the ICIP, CARELESS TOKEN, be terminated.

2. (U) Request your comments or concurrence.

FOR THE DIRECTOR OF INTELLIGENCE OPERATIONS:

J.V. Handle, Col, GS

JOHN L. HEISS
Colonel, GS
Chief, HUMINT Division

1 Incl
nc (C)

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Warning Notice. Sensitive Intelligence Sources and Methods Involved

2

687

~~CONFIDENTIAL~~

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON approval of ACSI

~~CONFIDENTIAL~~

IASEC-S (9 Apr 76) 2nd Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Headquarters, US Army Security Agency, ATTN: DCSSEC, Arlington Hall Station, Arlington, Virginia 22212

TO: HQDA, OACSfS for Intelligence, ATTN: DAMI-DOH, Washington, DC 20310

USASA concurs in recommendation to terminate CARELESS TOKEN.

1 Incl
nc (C)
(U)

WILLIAM B. HOLDEN
COL, GS
DCSSEC

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

UNCLASSIFIED WHEN SEPARATED
REGRADED
FROM CLASSIFIED INCLOSURES

688

~~CONFIDENTIAL~~

RE-GRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DOD 5200.1-R

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
511TH MILITARY INTELLIGENCE BATTALION
66TH MILITARY INTELLIGENCE GROUP
APO 09696

AEUMI-N-CE
B03130-328-76

5 April 1976

SUBJECT: CARELESS TOKEN (U)
(Quarterly Status Report)

Commander
66th Military Intelligence Group
ATTN: AEUMI-T-CI (EXCLUSIVE FOR ICIP CONTROL OFFICER)
APO 09108

1. (U) References:

a. OPLAN, 511th MI Battalion, AEUMI-N-CE, 1-75, 1 May 1975.

b. AEAGB-CI(SO), DTG 151640Z Jul 75, ICIP.

c. AEUMI-N-CE, B03130-061-76, 23 January 1976, CARELESS TOKEN (U).

d. AEAGB-CI(SO), DTG 091510Z Mar 76, CARELESS TOKEN (U).

2. (U) This Quarterly Status Report is submitted in accordance with the above references and covers the period 16 January - 1 April 1976. A one-time adjustment in reporting dates has been made to allow the reporting period to coincide with each calendar quarter.

3. General:

a. Company B, Forward Operations Battalion, terminated its operational mission at 2400 hours, 7 February 1976. During the period following, Company B personnel were engaged in transporting the classified operational files and equipment from the site to Augsburg. All Company B assigned or attached personnel have departed the target area. Destruction of all but two of the former Company B operations buildings is underway and is being performed by Facilities Engineers (FE) personnel from Regensburg and Grafenwoehr. Both of the two remaining buildings are to be removed under the Regensburg FE supervision under the same contract that will provide for landscaping the northern end of the compound, and removal of the rock at the northwestern end that presently blocks a portion of the antenna scanning area. The dismounted communications vans were not sold at the site as previously

CLASSIFICATION
EXEMPT 12, 180ct74
11652
EXEMPT
DECLASSIFY

689

AMERICAN REVOLUTION BICENTENNIAL 1776-1976

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

AEUMI-N-CE 5 April 1976

SUBJECT: CARELESS TOKEN (U)

reported would be the case, but instead have been removed to the Property Disposal Facility at Nuernberg for disposition.

b. Two members of Company B applied for European separations since November 1975, but it was not determined whether or not the applications had been approved, since both personnel had been transferred to Augsburg. SP5 b6 MOS: 98G2LRU, DPOB: b6 in b6 was scheduled for discharge on 20 May 1976. She had a US fee passport b6 issued 15 November 1973 in Boston, MA, and indicated her intent to remain in Europe for a 12 month period for travel purposes. SP5 b6 MOS: 98G2LRU, DPOB: b6 in b6 was scheduled for discharge on 9 January 1976, but extended his enlistment until 10 November 1976. He had a US fee passport b6 issued 6 July 1973 at New Orleans, LA, and indicated his intent to remain in Germany for 12 months to study. Both b6 and b6 were unmarried.

c. On 10 February 1976, CW2 b6 USASAFS Augsburg (USASAFSA) arrived on TDY at the target area accompanied by one or two other personnel from the same station. b6 is the Communications Security Custodian for USASAFSA and he supervised the removal of cryptographic communications equipment and escorted it back to USASAFSA. He stayed at the Kolmerhof Hotel in Rimbach, opposite the Company B administrative area. On 12 February 1976 he departed Rimbach and returned to Augsburg. On 12 February, the manager of the Kolmerhof Hotel contacted Company B to advise that an American guest had entered a room at the hotel on the night of 11-12 February. The guest was apparently extremely intoxicated, had become ill, and had vomited in large amounts all over the room, causing damage to carpets, furniture and bedding; evidence also indicated that the guest had urinated on the floor of the room. The manager presented a bill for DM 100 (approximately $40.00) and asked that it be passed on to the guest. The guest was determined to have been b6 and he readily admitted having caused the damage and subsequently paid the bill.

d. Additional information concerning the physical plant at the target was obtained as follows:

(1) Sewage service is provided by the firm Franz Lederer, St Sebastian Platz 1, Brueck (UQ0458). Water service is provided by the firm Hans Lober, Rauschstrasse, Nuernberg vorm Wald (UQ1069). The water is delivered by truck. The Comptroller Office, Seventh Army Training Center (SATC), Grafenwoehr advised that funds had been allotted to connect the target to the sewer and water systems of the adjacent French/Bundeswehr compound. The construction of those lines will be completed by July 1976 and will replace the septic and holding tanks now in use. Agency checks are being conducted on the above-mentioned firms.

690

[redacted]

~~CONFIDENTIAL~~

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

5 April 1976

(2) OBAG (the Upper Bavaria Power Company) has declared the main power cable serving the target, the French/Bundeswehr compound and the nearby Bundespost (German postal system) TV relay tower to be inadequate. OBAG intends to lay a new power cable parallel to the present one, and has asked each using agency to contribute to the costs, on a pro-rata basis. As the situation now stands, loss of outside power would automatically put the LfV generator into operation. That generator is capable of supplying full electric power to both the operational and living areas of the target for a maximum of 206 hours. After that time, the generator must be shut down for refueling, oil and maintenance.

(3) The SATC Military Community Fire Marshal recently inspected the target and indicated that some water must be made available for emergency fire use. The Neukirchen-Heilig Blut (UQ5258) Volunteer Fire Department indicated it had a 40-minute reaction time. The projected hookup to the French/Bundeswehr compound water system should make sufficient water available.

e. Due to the staggered schedules of target personnel, they had decided against hiring a cook and will prepare their own meals as a community effort. Inquiries at the local Labor Office revealed an estimated monthly salary for a cook would amount to about DM 1300 and this had a major impact on their decision.

4. (U) Operational Matters:

a. Information provided in the previous Quarterly Status Report is corrected/clarified as follows: There will be no SI area at the target. The highest access/classification will be Secret/Crypto. A request for a technical inspection had been submitted through ASA channels several months previously, which was not known by target personnel. The entire area, including the common room, will be subjected to a technical inspection prior to 21 May 1976.

b. Reference paragraph 4c of reference c: b6 closed the Hoherbogen Restaurant in late February 1976 and moved to the Augsburg area. Since his departure, the restaurant has remained closed. The entire file concerning b6 will be prepared for transfer to Special Operations Detachment, 66th Military Intelligence Group for monitoring of b6 activities in the Augsburg area.

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

691

~~CONFIDENTIAL~~

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

5 April 1976

c. b6, owner of "Tina's Bar" in Furth-im-Wald (UQ4364), also intended to move to Augsburg. b6 reportedly was a girl friend of several of the Company B senior enlisted personnel. b6 claimed to have enough money to purchase or lease any type of establishment in the Augsburg area that she chose. Agency checks will be conducted concerning b6 and the information will be passed to Special Operations Detachment if she moves to Augsburg.

d. Target members have the following privately-owned vehicles:

License Number	Type	Owner
KS-8739	1975 Chev van	b6
JA-9692	1964 VW sedan	
KH-8553	1970 Opel	
JT-8306	1967 Mercedes	

Additionally, SP5 Pack owns two motorcycles, neither of which is registered at the present time. He intends to register one of them and to store the other for shipment to CONUS when he is discharged in August 1976. SP4 b6 is buying a car from one of the civilian contractors in Augsburg and will pick it up soon.

e. Target members have had contact with three Americans in the area, at least two of whom are former Company B members. Barbara LNU was discharged in early 1976, is living in Koetzting (UQ4349) and is engaged to a German citizen. A check of recent Company B rosters identified SP4 b6 b6 MOS: 98G2LRU and SP4 b6, MOS: 98G2LCX as two possible individuals involved. SP4 b6 of the target unit has been in contact with the American owner of "Fulsome's Club" in Koetzting. A third American, possibly formerly stationed at the site, but not yet identified, allegedly works in Cham (UQ3054).

(U) (c) Source Activity:

a. B58,786 has departed the target area for reassignment.

b. PLO liaison contacts have revealed the following information concerning target personalities:

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2187 of 3957

~~CONFIDENTIAL~~

AEUMI-N-CE 5 April 1976
SUBJECT: CARELESS TOKEN (U)

(1) SFC b6 is a dedicated NCO who appears to know his job. He attended nearly three months of specialized training in the LFV system and related activities and is very knowledgeable of the mechanics involved in operation of the system. His assessment of individual members of the team coincides with the observations of the PLO. b6 appears to enjoy a spirit of mutual cooperation with the PLO. b6 advised the PLO that he has had very little trouble with the six personnel under his supervision, but the personalities of the six are beginning to emerge and he wished he had more indications of leadership qualities (i.e., willingness to accept responsibilities) from them.

(2) SP5 b6 nominally assistant NCOIC, is a quiet follower. He does his job, keeps his room very neatly, but is very non-assertive.

(3) SP5 Pack is probably the most responsible of the team, has an excellent personality, gets along well with everyone, and appears satisfied with his job and his hobby of motorcycles. His easy-going responsibility is attributed to his background; he is married and has one child. Prior to entering the Army, he had a good job in civilian life, and he knows how to work and to get along with others.

(4) SP4 b6 is a divorcee whose former wife is assigned to an ASA unit in West Berlin. He is a good worker but likes to enjoy himself after work. He has earned the respect of other team members because of his ability to separate work from play.

(5) SP4 b6 is an unknown quantity, but he has not caused any problems and he works well with others.

(6) SP4 b6 is an extrovert who enjoys being the center of attention. He does not get along well with SP4 b6

(7) SP4 b6 is an introvert and the complete opposite of b6 b6 has an acid personality and only tolerates having others around him. He does not like his present assignment and has submitted two requests to be returned to Augsburg. He appears to be able to sit in a room full of people and no one will notice he is there. PLO assessment of b6 and b6 are that they are typical ASA "kids", intelligent, not particularly gregarious, and sarcastic as long as they can get away with it.

693

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP 5, 1997
BY USAINSCOM FOIPA
Auth Para 4-102 DOD 5200.1R

Page 2188 of 3957

AEUMI-N-CE 5 April 1976
SUBJECT: CARELESS TOKEN (U)

c. No problems of a security nature have arisen during the reporting period. There have been no indications of Hostile Intelligence targetting against target personnel during the reporting period. A vehicle from the Soviet Military Liaison Mission-Frankfurt was active in the target area on 6 March 1976. Four sightings were reported during a two hours period; three were non-PRA sightings and one was a shallow penetration of PRA #13 near Hoherbogen. One of the sightings was reported by Company B personnel.

6. (C) Comments:

a. In amplification of previous generalized comments concerning the continued viability of the operation at the target, it is recommended that this operation be terminated at its present location. Whether or not the operation should be moved to another location where more sensitive ASA operations are being conducted is beyond the purview of a recommendation by this Battalion. The recommendation to terminate the operation at its present location was discussed informally with the S2, USASAFSA on 18 March 1976 and was received with no serious objection. Rationale for the recommendation is as follows:

(1) With the departure of Company B personnel from the target area, a total of seven personnel remain. The operations now being performed are far less sensitive and involve activity that is essentially automatic. LFV team members are essentially mechanics. It is less likely that a hostile intelligence service will devote the same priority as they did previously to exploit target personnel. Any confidential source recruited to cover the target "from within" would result in one individual watching the other six. It is not believed that a confidential source relationship with SFC Helus would be desirable nor appropriate; an effective liaison relationship with the PLO should be able to achieve the same results. Recruitment of another member of the team and targetting him against team members would necessarily include that source reporting on b6 activities. With the close working relationship of all team members, this type of activity could well lead to a gradual breakdown in the team effort and adversely affect b6 leadership effectiveness, as it would provide for an unofficial complaint channel and allow team members to "gang up" on the NCOIC. rather than fill the goals of the operation as indicated in reference a. Any compromise at the target of such confidential source activities would probably lead to a complete breakdown in effective liaison between b6 and the PLO.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2189 of 3957

~~CONFIDENTIAL~~

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

5 April 1976

(2) SFC b6 appears to be completely competent to do his job and to control his subordinates. His apparent leadership and management techniques, his insights into the various personalities of team personnel and his indicated awareness of potential problem areas all indicate that the PLO should be able to accomplish the goals of the plan through regular liaison with b6 and occasional casual contact with other target personnel on an opportunity basis.

(3) The time and expense required to conduct confidential source operations to achieve the goals of the operation do not appear to be justified for the reasons stated above. It is believed the same results can be achieved through aggressive and effective liaison.

(4) Termination of the OPLAN (reference a) presupposes that nothing would change outwardly regarding the PLO's relationship to the target; he would still visit as often as before, he would conduct himself in the same manner and he would continue to submit detailed reports on the results of each liaison visit. Any information obtained as a result of liaison that indicated a threat to the target or its personnel, or character or personality weaknesses of target personnel would be reported to the S2, USASAFSA without delay and coordination would be effected for appropriate investigative action.

b. As an alternate proposal, if the recommendation in paragraph 6a is not favorably considered, recommend that the OPLAN remain in effect, but that it be changed to limit contact with target personnel to liaison, that further consideration to the recruitment of confidential sources be dropped, and that Quarterly Status Reports continue to be submitted.

FADLO M. MASSABNI
LTC, MI
Commanding

Tel: NBG Mil (2621)-7165/Foss

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

695

7

~~CONFIDENTIAL~~

DAMI-DOH (9 Apr 76) 1st Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

DA, OACofS for Intelligence, ATTN: DAMI-DOH, Washington, DC 20310

TO: Commander, US Army Security Agency, ATTN: DCSSEC, Arlington Hall Station, Arlington, VA 22212

1. (U) This office concurs in the DCSI, USAREUR recommendation that the ICIP, CARELESS TOKEN, be terminated.

2. (U) Request your comments or concurrence.

FOR THE DIRECTOR OF INTELLIGENCE OPERATIONS:

KARL V. HAENDLE
Colonel, GS, USA
JOHN L. HEISS III
Colonel, GS
Chief, HUMINT Division

1 Incl
nc (C)

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Return to Iris Keaman

2 ACSI, DA

696

Warning Notice, Sensitive Intelligence Sources and Methods Involved

2 approval of ACSI

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

AEAGB-CI(SO)

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

HQDA (DAMI-DOH)
WASH DC 20310

1. (U) References:

a. Operational Plan, 66th MI Group, 5 May 1975, subject as above, with 5th Indorsement, DAMI-DOH, OACSI, DA, 25 February 1976 (U).

b. Letter, AEAGB-CI(SO), USAREUR, 10 February 1976, subject as above (U).

2. (U) Attached is the Quarterly Status Report pertaining to the ICIP CARELESS TOKEN for the period ending 1 April 1976.

3. (U) This office concurs in the recommendation by the 511th MI Battalion that this ICIP be terminated. The diminishing sensitivity of the target activity, and reduction in target personnel would appear not to justify the futher expenditure of counterintelligence assets and efforts required by this ICIP. Consequently this office is directing initiation of formal coordination with US Army Security Agency (USASA), Field Station Augsburg for the purpose of terminating CARELESS TOKEN.

4. (U) Request HQ, USASA be advised of USAREUR plans to terminate this ICIP. Comments in this regard by your office and HQ USASA would be appreciated.

5. (U) ODCSI, USAREUR, Action Officer is Mr David R. Smith, AEAGB-CI(SO), HM 7354 (AUTOSEVOCOM 6742).

FOR THE DEPUTY CHIEF OF STAFF, INTELLIGENCE:

1 Incl
as

A. J. IADEROSA
Colonel, GS
Chief, Counterintelligence
Division

697

~~CONFIDENTIAL~~

CLASSIFIED BY ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY (2)
DECLASSIFY ON (APPROVAL OF ACSI DA)

DEPARTMENT OF THE ARMY
511TH MILITARY INTELLIGENCE BATTALION
66TH MILITARY INTELLIGENCE GROUP
APO 09696

AEUMI-N-CE
B03130-328-76

5 April 1976

SUBJECT: CARELESS TOKEN (U)
(Quarterly Status Report)

Commander
66th Military Intelligence Group
ATTN: AEUMI-T-CI (EXCLUSIVE FOR ICIP CONTROL OFFICER)
APO 09108

1. (U) References:

a. OPLAN, 511th MI Battalion, AEUMI-N-CE, 1-75, 1 May 1975.

b. AEAGB-CI(SO), DTG 151640Z Jul 75, ICIP.

c. AEUMI-N-CE, B03130-061-76, 23 January 1976, CARELESS TOKEN (U).

d. AEAGB-CI(SO), DTG 091510Z Mar 76, CARELESS TOKEN (U).

2. (U) This Quarterly Status Report is submitted in accordance with the above references and covers the period 16 January - 1 April 1976. A one-time adjustment in reporting dates has been made to allow the reporting period to coincide with each calendar quarter.

3. (C) General:

a. Company B, Forward Operations Battalion, terminated its operational mission at 2400 hours, 7 February 1976. During the period following, Company B personnel were engaged in transporting the classified operational files and equipment from the site to Augsburg. All Company B assigned or attached personnel have departed the target area. Destruction of all but two of the former Company B operations buildings is underway and is being performed by Facilities Engineers (FE) personnel from Regensburg and Grafenwoehr. Both of the two remaining buildings are to be removed under the Regensburg FE supervision under the same contract that will provide for landscaping the northern end of the compound, and removal of the rock at the northwestern end that presently blocks a portion of the antenna scanning area. The dismounted communications vans were not sold at the site as previously

698

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOIPO
Auth Para 1-603 DoD 5200.1R

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

5 April 1976

reported would be the case, but instead have been removed to the Property Disposal Facility at Nuernberg for disposition.

b. Two members of Company B applied for European separations since November 1975, but it was not determined whether or not the applications had been approved, since both personnel had been transferred to Augsburg. SP5 b6 MOS: 98G2LRU, DPOB: b6 in b6 was scheduled for discharge on 20 May 1976. She had a US fee passport b6 issued 15 November 1973 in Boston, MA, and indicated her intent to remain in Europe for a 12 month period for travel purposes. SP5 b6 MOS: 98G2LRU, DPOB: b6 in b6 was scheduled for discharge on 9 January 1976, but extended his enlistment until 10 November 1976. He had a US fee passport b6 issued 6 July 1973 at New Orleans, LA, and indicated his intent to remain in Germany for 12 months to study. Both b6 and b6 were unmarried.

c. On 10 February 1976, CW2 b6 USASAFS Augsburg (USASAFSA) arrived on TDY at the target area accompanied by one or two other personnel from the same station. b6 is the Communications Security Custodian for USASAFSA and he supervised the removal of cryptographic communications equipment and escorted it back to USASAFSA. He stayed at the Kolmerhof Hotel in Rimbach, opposite the Company B administrative area. On 12 February 1976 he departed Rimbach and returned to Augsburg. On 12 February, the manager of the Kolmerhof Hotel contacted Company B to advise that an American guest had entered a room at the hotel on the night of 11-12 February. The guest was apparently extremely intoxicated, had become ill, and had vomited in large amounts all over the room, causing damage to carpets, furniture and bedding; evidence also indicated that the guest had urinated on the floor of the room. The manager presented a bill for DM 100 (approximately $40.00) and asked that it be passed on to the guest. The guest was determined to have been b6 and he readily admitted having caused the damage and subsequently paid the bill.

d. Additional information concerning the physical plant at the target was obtained as follows:

(1) Sewage service is provided by the firm Franz Lederer, St Sebastian Platz 1, Brueck (UQ0458). Water service is provided by the firm Hans Lober, Rauschstrasse, Nuernberg vorm Wald (UQ1069). The water is delivered by truck. The Comptroller Office, Seventh Army Training Center (SATC), Grafenwoehr advised that funds had been allotted to connect the target to the sewer and water systems of the adjacent French/Bundeswehr compound. The construction of those lines will be completed by July 1976 and will replace the septic and holding tanks now in use. Agency checks are being conducted on the above-mentioned firms.

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

699

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

5 April 1976

(2) OBAG (the Upper Bavaria Power Company) has declared the main power cable serving the target, the French/Bundeswehr compound and the nearby Bundespost (German postal system) TV relay tower to be inadequate. OBAG intends to lay a new power cable parallel to the present one, and has asked each using agency to contribute to the costs, on a pro-rata basis. As the situation now stands, loss of outside power would automatically put the LfV generator into operation. That generator is capable of supplying full electric power to both the operational and living areas of the target for a maximum of 206 hours. After that time, the generator must be shut down for refueling, oil and maintenance.

(3) The SATC Military Community Fire Marshal recently inspected the target and indicated that some water must be made available for emergency fire use. The Neukirchen-Heilig Blut (UQ5258) Volunteer Fire Department indicated it had a 40-minute reaction time. The projected hookup to the French/Bundeswehr compound water system should make sufficient water available.

e. Due to the staggered schedules of target personnel, they had decided against hiring a cook and will prepare their own meals as a community effort. Inquiries at the local Labor Office revealed an estimated monthly salary for a cook would amount to about DM 1300 and this had a major impact on their decision.

4. (C) Operational Matters:

a. Information provided in the previous Quarterly Status Report is corrected/clarified as follows: There will be no SI area at the target. The highest access/classification will be Secret/Crypto. A request for a technical inspection had been submitted through ASA channels several months previously, which was not known by target personnel. The entire area, including the common room, will be subjected to a technical inspection prior to 21 May 1976.

b. Reference paragraph 4c of reference c: b6 closed the Hoherbogen Restaurant in late February 1976 and moved to the Augsburg area. Since his departure, the restaurant has remained closed. The entire file concerning b6 will be prepared for transfer to Special Operations Detachment, 66th Military Intelligence Group for monitoring of b6 activities in the Augsburg area.

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

700

AEUMI-N-CE 5 April 1976
SUBJECT: CARELESS TOKEN (U)

c. b6 owner of "Tina's Bar" in Furth-im-Wald (UQ4364), also intended to move to Augsburg. b6 reportedly was a girl friend of several of the Company B senior enlisted personnel. b6 claimed to have enough money to purchase or lease any type of establishment in the Augsburg area that she chose. Agency checks will be conducted concerning b6 and the information will be passed to Special Operations Detachment if she moves to Augsburg.

d. Target members have the following privately-owned vehicles:

License Number	Type	Owner
KS-8739	1975 Chev van	b6
JA-9692	1964 VW sedan	
KH-8553	1970 Opel	
JT-8306	1967 Mercedes	

Additionally, SP5 Pack owns two motorcycles, neither of which is registered at the present time. He intends to register one of them and to store the other for shipment to CONUS when he is discharged in August 1976. SP4 b6 is buying a car from one of the civilian contractors in Augsburg and will pick it up soon.

e. Target members have had contact with three Americans in the area, at least two of whom are former Company B members. Barbara LNU was discharged in early 1976, is living in Koetzting (UQ4349) and is engaged to a German citizen. A check of recent Company B rosters identified SP4 b6 b6 MOS: 98G2LRU and SP4 b6, MOS: 98G2LCX as two possible individuals involved. SP4 b6 of the target unit has been in contact with the American owner of "Fulsome's Club" in Koetzting. A third American, possibly formerly stationed at the site, but not yet identified, allegedly works in Cham (UQ3054).

5. (U) Source Activity:

a. B58,786 has departed the target area for reassignment.

b. PLO liaison contacts have revealed the following information concerning target personalities:

REGARDED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

701

Page 2196 of 3957

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

5 April 1976

(1) SFC b6 is a dedicated NCO who appears to know his job. He attended nearly three months of specialized training in the LFV system and related activities and is very knowledgeable of the mechanics involved in operation of the system. His assessment of individual members of the team coincides with the observations of the PLO. b6 appears to enjoy a spirit of mutual cooperation with the PLO. b6 advised the PLO that he has had very little trouble with the six personnel under his supervision, but the personalities of the six are beginning to emerge and he wished he had more indications of leadership qualities (i.e., willingness to accept responsibilities) from them.

(2) SP5 b6, nominally assistant NCOIC, is a quiet follower. He does his job, keeps his room very neatly, but is very non-assertive.

(3) SP5 Pack is probably the most responsible of the team, has an excellent personality, gets along well with everyone, and appears satisfied with his job and his hobby of motorcycles. His easy-going responsibility is attributed to his background; he is married and has one child. Prior to entering the Army, he had a good job in civilian life, and he knows how to work and to get along with others.

(4) SP4 b6 is a divorcee whose former wife is assigned to an ASA unit in West Berlin. He is a good worker but likes to enjoy himself after work. He has earned the respect of other team members because of his ability to separate work from play.

(5) SP4 b6 is an unknown quantity, but he has not caused any problems and he works well with others.

(6) SP4 b6 is an extrovert who enjoys being the center of attention. He does not get along well with SP4 b6

(7) SP4 b6 is an introvert and the complete opposite of b6 b6 has an acid personality and only tolerates having others around him. He does not like his present assignment and has submitted two requests to be returned to Augsburg. He appears to be able to sit in a room full of people and no one will notice he is there. PLO assessment of b6 and b6 are that they are typical ASA "kids", intelligent, not particularly gregarious, and sarcastic as long as they can get away with it.

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

702

Page 2197 of 3957

AEUMI-N-CE 5 April 1976
SUBJECT: CARELESS TOKEN (U)

c. No problems of a security nature have arisen during the reporting period. There have been no indications of Hostile Intelligence targetting against target personnel during the reporting period. A vehicle from the Soviet Military Liaison Mission-Frankfurt was active in the target area on 6 March 1976. Four sightings were reported during a two hours period; three were non-PRA sightings and one was a shallow penetration of PRA #13 near Hoherbogen. One of the sightings was reported by Company B personnel.

6. (C) Comments:

a. In amplification of previous generalized comments concerning the continued viability of the operation at the target, it is recommended that this operation be terminated at its present location. Whether or not the operation should be moved to another location where more sensitive ASA operations are being conducted is beyond the purview of a recommendation by this Battalion. The recommendation to terminate the operation at its present location was discussed informally with the S2, USASAFSA on 18 March 1976 and was received with no serious objection. Rationale for the recommendation is as follows:

(1) With the departure of Company B personnel from the target area, a total of seven personnel remain. The operations now being performed are far less sensitive and involve activity that is essentially automatic. LFV team members are essentially mechanics. It is less likely that a hostile intelligence service will devote the same priority as they did previously to exploit target personnel. Any confidential source recruited to cover the target "from within" would result in one individual watching the other six. It is not believed that a confidential source relationship with SFC Helus would be desirable nor appropriate; an effective liaison relationship with the PLO should be able to achieve the same results. Recruitment of another member of the team and targetting him against team members would necessarily include that source reporting on b6 activities. With the close working relationship of all team members, this type of activity could well lead to a gradual breakdown in the team effort and adversely affect b6 leadership effectiveness, as it would provide for an unofficial complaint channel and allow team members to "gang up" on the NCOIC. rather than fill the goals of the operation as indicated in reference a. Any compromise at the target of such confidential source activities would probably lead to a complete breakdown in effective liaison between b6 and the PLO.

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

703

AEUMI-N-CE 5 April 1976
SUBJECT: CARELESS TOKEN (U)

(2) SFC b6 appears to be completely competent to do his job and to control his subordinates. His apparent leadership and management techniques, his insights into the various personalities of team personnel and his indicated awareness of potential problem areas all indicate that the PLO should be able to accomplish the goals of the plan through regular liaison with b6 and occasional casual contact with other target personnel on an opportunity basis.

(3) The time and expense required to conduct confidential source operations to achieve the goals of the operation do not appear to be justified for the reasons stated above. It is believed the same results can be achieved through aggressive and effective liaison.

(4) Termination of the OPLAN (reference a) presupposes that nothing would change outwardly regarding the PLO's relationship to the target; he would still visit as often as before, he would conduct himself in the same manner and he would continue to submit detailed reports on the results of each liaison visit. Any information obtained as a result of liaison that indicated a threat to the target or its personnel, or character or personality weaknesses of target personnel would be reported to the S2, USASAFSA without delay and coordination would be effected for appropriate investigative action.

b. As an alternate proposal, if the recommendation in paragraph 6a is not favorably considered, recommend that the OPLAN remain in effect, but that it be changed to limit contact with target personnel to liaison, that further consideration to the recruitment of confidential sources be dropped, and that Quarterly Status Reports continue to be submitted.

FADLO M. MASSABNI
LTC, MI
Commanding

Tel: NBG Mil (2621)-7165/Foss

REGARDED UNCLASSIFIED
ON SEP 05 1993
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

704

~~CONFIDENTIAL~~

DAMI-DOH (28 Apr 76) 1st Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

DA, OACofS for Intelligence, ATTN: DAMI-DOH, Washington, DC 20310 1 [illegible] 1976

TO: Commander, US Army Security Agency, ATTN: DCSSEC, Arlington Hall Station, Arlington, VA 22212

1. (C) The attached Operations Plan for an Internal Counterintelligence Program (ICIP) in support of the US Army Security Agency Field Station Berlin is forwarded for review by the Commander, US Army Security Agency.

2. (U) Request correspondence be returned to this office after approval or comment by your commander.

FOR THE DIRECTOR OF INTELLIGENCE OPERATIONS:

KARL V. HAENDLE
Colonel, GS, USA
JOHN L. HEISS III
Colonel, GS
Chief, HUMINT Division

1 Incl
nc (C)

REGRADED UNCLASSIFIED
ON SEP 5
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Return to Miss Brannan

ACSI, DA

3

705

Classified by [illegible]
[illegible] 2 [illegible]
approval of ACSI

~~CONFIDENTIAL~~

26 APR 1976

AEAGB-CI(SO)

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

HQDA (DAMI-DOH)
WASH DC 20310

1. (U) References:

a. Message, DAMI-DOH, DA, 032115Z December 1975, subject as above (S).

b. Message, AEAGB-CI(SO), USAREUR, 061755Z January 1976, subject as above (S) (BOM).

c. Message, DAMI-DOH, DA, 092117Z April 1976, subject as above (C) (BOM).

2. (U) ~~(C)~~ The attached Operations Plan for an Internal Counterintelligence Program (ICIP), in support of the US Army Security Agency Field Station Berlin (USASAFSB) is furnished for ACSI review and approval. The ICIP is designed to supplant Project FILMAN, and external CI support program, and to provide the Cdr, USASAFSB a more complete CI program for identifying and neutralizing the hostile intelligence threat to his activities and personnel.

3. (U) ~~(C)~~ Cdr, USASA, Arlington Hall, concurred in the proposed cancellation of Project FILMAN and initiation of an Aggressive Defensive Source Acquisition Program (ADSAP) (see inclosure 3 to basic OPLAN). However, the ADSAP concept was subsequently discarded in favor of an ICIP. Consequently, recommend the attached OPLAN be coordinated with Cdr, USASA, Arlington Hall.

4. (U) Recommend approval.

CLASSIFIED BY ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON APPROVAL OF ACSI, DA

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~ 706

AEAGB-CI(SO)
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

5. (U) ODCSI, USAREUR, Action Officer is Mr David R. Smith, AEAGB-CI(SO), HM 7354 (AUTOSEVOCOM 6742).

1 Incl
as

OLIVER W. DILLARD
Major General, GS
Deputy Chief of Staff,
Intelligence

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

707

~~CONFIDENTIAL~~

OPERATIONS PLAN

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

DATE: 13 February 1976

REFERENCES: a. Letter, AEAGB-CI(SO), dated 27 December 1974, Subject: Internal Counterintelligence Program (ICIP) with 1st Ind, AEAGI-T-CE, 15 January 1975

OPLAN NO: 01-76(BCE)BLN

PROJECT NO: 924134

b. Group Regulation 381-10, Defensive Counterintelligence Sources, dated 4 February 1976.

c. FM 30-17A(C), Counterintelligence Special Operations, February 1973.

d. AR 381-12, Subversion and Espionage Directed Against the US Army and Deliberate Security Violations, 18 October 1974.

e. Letter, IACG, dated 20 October 1975, Subject: Aggressive Defensive Source Acquisition Program (ADSAP)(U).

---

1. (U) MISSION.

a. Requirement: To collect significant counterintelligence information through the utilization of overt liaison contacts (OLC). Casual Sources (CS) and Confidential Recruited Sources (CRS) assigned to the US Army Security Agency Field Station Berlin (USASAFSB), hereafter referred to as ASA. The Sources will be specifically targetted against Hostile Intelligence Services (HoIS) activities directed towards ASA and against the security vulnerabilities of ASA personnel.

b. Objective: To provide responsible commanders and supervisors in ASA with a concentrated program designed to detect, eliminate or neutralize

CLASSIFIED BY: ACSI, DA
EXEMPT FROM GDS OF EO 11652
EXEMPTION CATEGORY: 2
DECLASSIFY ON: Specific approval of ODCSI, DA

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOUPO AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Operations Plan,

(1) espionage, sabotage, subversion or deliberate security violations against ASA or ASA personnel;

(2) disloyalty, disaffection, and security weaknesses prevalent among personnel assigned to ASA;

(3) individuals in sensitive positions who, by character weaknesses or personal conduct, render themselves vulnerable to coercion or blackmail by HoIS, either while the individuals are in their present positions or when they are assigned later to another unit.

c. Base of Operations: Berlin Field Office, 766th MI Detachment, West Berlin.

2. (U) PERSONNEL.

a. Source Personnel: Not yet selected. Spotting has started with the assistance of S-2, ASA, but no vetting or recruitment of Sources will be made prior to the approval of this OPLAN. To give adequate coverage of ASA, a minimum of 12 CS/CRS's will be required within ASA. The Sources must meet the following criteria:

(1) Reasonable amount of intelligence and high degree of common sense.

(2) Above-average sense of loyalty to duty and country, and a strong dedication to duty assignment.

(3) Trustworthy, reliable and discreet.

(4) Ability to take directions.

(5) Clean record, to include no character deficiencies.

(6) DEROS not later than one year from recruitment.

b. US Army Intelligence Personnel:

(1) Project Liaison Officer (PLO): The PLO will be responsible for OLCs and the spotting, assessing and recruitment of Sources at ASA. The OIC, CE/SAR Team, will be the PLO.

(2) Project Control Officer (PCO): The PCO will be responsible for the management and control of Sources in this operation. The OIC, CE Programs, will be the PCO.

(3) Case Officers (CO): Only Special Agents (S/A) assigned to the Berlin Field Office will initially be tasked to act as CO's.

709

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PC
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

CONFIDENTIAL

Operations Plan,

(4) Other Supervision:

(a) Supervision for the conduct and operating control of this operation will be vested in the OIC, CE Section.

(b) Broad operational [illegible] control and policy guidance are vested in the Berlin Field Office Commander and Operations Officer.

(c) The Director of Operations, Headquarters, 66th MI Group, will be responsible for the operational control of this ICIP, will coordinate all ICIP activities with the ICIP Control Officer, ODCSI, USAREUR, and with the Commander, USASA Europe, and will levy requirements on other subordinate counterintelligence (CI) elements of the 66th MI Group as appropriate.

3. ~~(C)~~ COVER AND DOCUMENTATION:

a. b1

(1) b1

(2) b1

b. b1

c. b1

d. b1

4 (~~U~~) EXECUTION.

a. Background: The location and highly sensitive mission of ASA make it of logical interest to HoIS, particularly in this area to Soviet

CONFIDENTIAL

~~CONFIDENTIAL~~

Operations Plan,

Intelligence Services (SIS) and Intelligence Services of the German Democratic Republic, whose technical and personal access to ASA areas are facilitated by the geographical location of ASA which is completely surrounded by a Communist country. HoIS can use some uncontrolled means of transportation to enter and leave the vicinities of ASA installations, and can use any of several official East Bloc representations in the area as cover for their activities. Past investigations and CI special operations have confirmed HoIS interest in ASA and in HoIS' collection of data on ASA personnel, to include personalia, character traits and weaknesses, and possible motivating points. Headquarters, USASA, Arlington Hall, Virginia, has approved the use of ASA personnel in ICIP.

b. Concept:

(1) The cultivation and use of OLC's, and the spotting, assessing and recruitment of non-ASA personnel in the area will continue in effect and be expanded as necessary, without requiring prior approval under this OPLAN.

(2) Upon approval of this OPLAN, coordination will be effected with S-2, ASA, for purposes of obtaining Leads and for facilitating screening of ASA personnel records. In addition, the PLO will develop other means of spotting and assessing Leads as described in paragraph 3a(2) above. PLO will also be the initial point of contact for those ICIP assets who have been transferred from another area to this area.

c. Source Activities in the Target Area: Sources will perform their normal military duties while covertly and discreetly attempting to answer the following EEI, both from on-duty and off-duty contacts and experiences:

(1) Identification of ASA personnel who closely and continuously associate with foreign nationals having connections with Communist countries;

(2) Identification of ASA personnel who perform authorized or unauthorized travel to Communist countries;

(3) Detection of disaffected ASA personnel;

(4) Detection of ASA personnel whose activities and/or character weaknesses render them vulnerable to blackmail or HoIS exploitation;

(5) Detection of ASA personnel whose activities are indicative of potential defection or desertion;

(6) Detection of ASA personnel who have memberships in or associate with members of organizations, clubs, groups or other activities which pose actual or potential threats to the security of ASA.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 2206 of 3957

Operations Plan,

d. Security Considerations:

(1) Individuals who are approached for recruitment who decline to function as Sources will be asked to sign security statements which clearly state that it is unlawful to make any unauthorized disclosure concerning the recruitment approach or the activities under this OPLAN.

(2) Individuals who are approached for recruitment prior to their arrival at the ASA target area, and who decline to function as Sources, will be considered for assignment to some location other than the target area, if circumstances and military priorities permit.

(3) No actual or potential Source will be made aware of the source relationship with any other individual in this program.

(4) All CRS's will be met under covert conditions, away from the target area; under conditions that will provide maximum security against inadvertent disclosure of the source relationship.

(5) Separate and plausible cover stories for status and for action will be arranged with each CRS to provide a logical reason for regular meetings between CRS and CO.

(6) Each CRS will be provided sufficient training in security and meeting arrangements so as to minimize possibilities of compromise of the source relationship.

(7) In the event of compromise of a CRS and/or the nature of this operation, termination of the source will follow under such conditions as are warranted by the circumstances of the compromise. In the event of a compromise, denial of US Army Intelligence involvement will be achieved where plausible.

(8) Non-US Local Wage Rate Investigators employed by the 66th MI Group will not be made aware of the existence of this OPLAN or of the Source relationship with any CRS.

(9) Knowledgeability of this OPLAN, to include the identity of the target, will be kept to a strict minimum. Only those individuals with a strict "need to know" will be made cognizant.

(10) Upon the termination of a Source in this area, proper debriefing action will be taken in accordance with 66th MI Group Regulation 381-10 and consideration will be given to the transfer of Source to the appropriate CI element in the Source's new assignment area.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

Operations Plan,

e. Production:

(1) Operational information will be forwarded by Agent Report and/or other appropriate reporting means to Headquarters, 66th MI Group, ATTN: AEUMI-T-CI.

(2) Suitability information or security information having an immediate, significant impact on the command will be brought to the attention of the Commander, USASAFSS, through his S-2.

(3) Information pertaining to or identifying overt or covert sources will not normally be passed as individual items to ASA without the specific approval of DCSI USAREUR, through Headquarters, 66th MI Group.

(4) Once this OPLAN has been approved and placed into operation, progress reports will be submitted every 60 days.

(5) Periodic briefings to ASA can be accomplished through OLC's by the PLO.

5. ~~(C)~~ COMMUNICATIONS:

a. b1

b. b1

c. b1

6. ~~(C)~~ TRAINING: b1

CONFIDENTIAL

CONFIDENTIAL

Operations Plan,

b1

a. b1

b. b1

c. b1

d. b1

e. b1

f. b1

7. ~~(c)~~ FINANCE AND LOGISTICS:

a. Finance:

b1

(1) b1

(2) b1

(3) b1

(4) b1

(5) b1

b. Logistics: No special logistics or equipment requirements are foreseen at this time, which would require procurement of equipment not presently on hand. If such equipment requirements arise, appropriate requests will be submitted for approval and funding.

714

CONFIDENTIAL

~~CONFIDENTIAL~~

Operations Plans,

c. Estimates: See attached Financial Annex for an estimate of overall expenses to be incurred by PLO, CO's and Sources. through the remainder of FY 76. and FY 77.

8. (U) TERMINATION:

a. The duration of this PLAN will be for an indefinite period, or until such time that it is determined that the sensitivity of the target and/or the drawdown of assigned personnel at the target, no longer warrant continuation of the operation.

b. Termination of Sources will be in accordance with 66th MI Group Regulation 381-10, or other appropriate source directives.

9. (U) COORDINATION:

a. The purpose and objective of this OPLAN as outlined in Mission above has been coordinated with the Commander, USASAFSB.

b. Preliminary coordination of the action which this OPLAN is to accomplish was initiated as indicated in ANNEX B (coordination background).

c. EEI developed in and derived from this operation will be reviewed at all levels for acquisition and retention criteria contained in AR 380-13.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

715

~~CONFIDENTIAL~~

Page 2210 of 3957

CONFIDENTIAL

ANNEX A - FINANCES

1. (C) Fourth Quarter - FY-76:

a. b1

b. b1

c. b1

d. b1

e. b1

2. (C) FY-76-T (July to 1 October 76):

a. b1

b. b1

c. b1

d. b1

e. b1

3. (C) FY-77 (All four Quarters):

a. b1

b. b1

Classified by (ACSI, DA)
X from GDS of EO 11652
X Category (2)
Declassify on (Originator ACSI, DA)

716

CONFIDENTIAL

~~CONFIDENTIAL~~

ANNEX A - FINANCES

c. b1

d. b1

e. b1

717

~~CONFIDENTIAL~~

Page 2212 of 3957

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

5 USC 552 (b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 718-720

IAGPA-CSF Form 6-R
1 Sep 93

~~CONFIDENTIAL~~

ANNEX B - COORDINATION BACKGROUND

1. (U) (C) CI support provided by the 766th MI Detachment to the US Army Security Agency Field Station, Berlin (USASAFSB) is in accordance with the provisions reflected in OPLAN titled project Filman. The proposal to improve CI support provided to USASAFSB by cancelling project Filman and replacing it with an existing Aggressive Defensive Source Acquisition Program (ADSAP) was presented to USASAFSB in a letter dated 19 September 1975, copy of which is attached to this Annex as Inclosure 1.

2. (U) (C) USASAFSB forwarded to Headquarters, US Army Security Agency, Arlington Hall Station, the above referenced letter (Inclosure 1) with a recommendation that project Filman be replaced with the 766th MI Detachment's ADSAP. Copy of the USASAFSB letter is attached to this Annex as Inclosure 2.

3. (U) (C) In a letter dated 20 October 1975, the Commander of the US Army Security Agency concurred in the cancellation of project Filman and initiation of the 766th MI Detachment's ADSAP program. A copy of the letter is attached to this Annex as Inclosure 3.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by (ACSI, DA)
X from OADR of EO 11652
X Category (2)
Declassify on Cancel of ACSI

~~CONFIDENTIAL~~

Page 2214 of 3957

~~CONFIDENTIAL~~

19 SEP 75

19 SEP 1975

AEUMI-BCE

SUBJECT: Project Filman (U)

Commander
USASAFSB
ATTN: S-2
APO 09742

1. (U) The purpose of this proposed action is to provide increased and improved counterintelligence support to the US Army Security Agency Field Station, Berlin (USASAFSB).

2. (U) In 1970, a CI operations plan was submitted by Berlin Field Station, 66th MI Group, to correspond with the activation of the USASAFSB site known as "Teufelsberg". The operations plan was designed to provide counterintelligence support to the project through the utilization of sources, either among the local work force or through personnel located in establishments frequented by the work force. Because the local work force was too transient in nature to effectively insert a source before they completed work on site, source recruitment efforts were concentrated on individuals who associated with ASA personnel at local entertainment establishments and at social functions. Initially through coordination with the S-2, USASAFSB, a list of establishments frequented by USASAFSB personnel was prepared and attempts were made to introduce sources into some of the establishments. We presently have six sources under the Filman project who have provided limited information. However, to date these sources have provided routine information of low level CI significance, primarily of interest to US Army Berlin Brigade and not to USASAFSB. In approximately 1973, USASA withdrew financial support of Filman and fiscal responsibility reverted to the 66th MI Group. The primary difficulty with the Filman project has been the peripherial nature of the sources and their difficulty in becoming accepted into ASA circles, since ASA personnel appear to associate in fairly close knit ASA circles. In short, peripheral sources have provided only peripheral leads.

CLASSIFIED BY: Cdr, 66th MI Group
EXEMPT FROM GDS OF EO 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON: Notification by Originator

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY USAINSCOM POI/PA
Auth Para 4-102 DOD 5200.1R

722

INCL # 1

~~CONFIDENTIAL~~

FILED IN 1001 FILE

~~CONFIDENTIAL~~

19 SEP 1973

AEUMI-BCE
SUBJECT: Project Filman (U)

3. (U) I propose that the Filman project be cancelled, that permission be granted to recruit ASA personnel within USASAFSB, and that the Aggressive Defensive Source Acquisition Program (ADSAP) be used as the vehicle to provide [illegible] counterespionage support to USASAFSB. A brief description of ADSAP and general ADSAP MOI is attached as Inclosure. This would enhance CI coverage of USASAFSB by providing more flexibility within the framework of one source program, access to the target areas and target personalities, a wider range of operations for sources, and more streamlined administrative procedures for the management of sources. Current Filman sources will be converted to the ADSAP program. Sources will be preferably recruited within the target activity to provide information on personalities and activities. Additional sources will be recruited on the periphery or outside of the target sites in order to enhance overall CI coverage. Once it has been determined where a possible shortfall of information occurs, a concerted effort will be made to obtain sources who can provide that information. Indiscriminant selection and recruitment of sources will be avoided and emphasis will be placed on a prospective source's ability to fulfill the requirements levied on him. 766th MID will provide the S-2, USASAFSB with the desired qualifications for personnel to be utilized in the program and he will be requested to screen present personnel assigned to his unit to determine those best qualified for recruitment. ADSAP will not supplant the S-2, USASAFSB program of internal informants, but will augment his present activities. A target analysis will be prepared by this Detachment in coordination with the S-2, USASAFSB. Information solely of a suitability nature, will be reported directly to the S-2, USASAFSB. All other information will be reported in accordance with reporting requirements, as outlined in LOI 6-TD, 66th MI Group.

4. (U) Preliminary discussions, conducted in August 1975, with the Commander, USASAFSB, the Deputy Chief of Staff, Security, USASA Headquarters, Arlington Hall, Virginia, and the Commander, 66th MI Group, indicated a favorable response to the above proposal.

5. (U) This Detachment requests your comments, recommendations, and approval of the above proposal.

1 Incl
as

ALLYN C. HOULTRY
LTC, MI
Commanding

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

823

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

AGGRESSIVE DEFENSIVE SOURCE ACQUISITION PROGRAM (ADSAP)

ADSAP concerns itself with two categories of human sources as defined by 66th MI Group LOI Number 6-TD. These two source categories are Conventional and Confidential. The ADSAP is a CI threat information collection program and sources recruited under this program should not be recruited for coverage of a specific CE target. Sources are recruited within and on the periphery of sensitive installations and activities by combining both active and passive measures to counter the information collection capability of hostile intelligence services (HoIS) operating against US Forces. The passive measures are designed to protect defense information from unauthorized disclosure or compromise, while the aggressive measures are designed to obtain information which will lead to the detection and neutralization of HoIS efforts directed against US Forces.

General ADSAP EEI:

a. Detection of suspicious activities, undue inquisitiveness or obvious lack of good security practices on the part of or involving US Forces personnel.

b. Identification of US Forces personnel who closely and continually associate with foreign nationals having connections with Soviet Bloc countries.

c. Identification of US forces personnel who make unauthorized or frequent authorized travel to Soviet Bloc countries.

d. Identification of US Forces personnel who have continued contact with local national personnel.

e. Detection of disaffected personnel.

f. Identification of US Forces personnel whose activities and/or character weaknesses either individually or in a combination constitute a clear and significant threat to US Forces in that they have rendered the US Forces connected personnel susceptible to exploitation by HoIS. Susceptibility to HoIS exploitation because of adverse suitability factors should be coupled with at least one of the foregoing indicators of possible HoIS interest. Specific suitability factors which could render US Forces personnel vulnerable to HoIS exploitation would be excessive indebtedness or recurring financial difficulties; unexplained affluence; conduct such as criminal, immoral or homosexual acts which could render

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

the individual susceptible to pressure; current and past mental and emotional instability; unusual work habits that do not conform to the daily pattern of fellow employees, sudden unexplained changes in working or social habits; sexual misconduct; infidelity; marital problems; trading on the interzonal routes or otherwise exhibiting linguistic capabilities with Soviet or other bloc personnel in unauthorized situations.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

OCT 1975

IAEA-I

SUBJECT: Aggressive Operational Support Acquisition Program (ALSAP) (U)

Commander
US Army Security Agency
ATTN: DCSSEC
Arlington Hall Station
Arlington, Virginia 22212

(U) 1. (C) Attached is a copy of a letter received on 19 September 1975 from Commander, 766th Military Intelligence Detachment, 66th MI Group, entitled "Project FILHAN". The letter is self explanatory but can be summarized as follows: Counterintelligence support to USASAFS Berlin has been conducted since 1970 under the provisions of FILHAN. Although FILHAN was satisfactory in concept, it suffered from a lack of precise support definition, particularly in source acquisition and reporting.

(U) 2. (C) Cdr, 766th MID, proposes an ALSAP support arrangement which would provide more direct source access to USASA personnel and direct control of source coverage of actual or potential espionage approaches. Cdr, USASAFS Berlin concurs in the concept and desires to implement the program. COL Holden was briefed on the program during his visit to Berlin in August 1975 and concurred in the proposal. [illegible], DA ACSI, and [illegible], [illegible], were also briefed in September 1975 and supported the concept.

(U) 3. (C) Request your concurrence in cancellation of Project FILHAN and adoption of the ALSAP by USASAFS Berlin/766th MID. Appropriate safeguards will be maintained with regard to withdrawal of USASA sources should hostile intelligence [illegible] a USASA soldier. Request a reply as soon as possible so we can begin negotiating a new Memorandum of Understanding with 66th MI Group.

FOR THE COMMANDER:

1 Incl
as

GERALD J. [illegible]
MAJ, MI
Asst Adjutant

Classified by CDR USASACS
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON NATIONAL SECURITY INTEREST

726

Copy furnished CI Spt Tm USASA

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
UNITED STATES ARMY SECURITY AGENCY
ARLINGTON HALL STATION
ARLINGTON, VIRGINIA 22212

IACG

20 OCT 1975

SUBJECT: Aggressive Defensive Source Acquisition Program (ADSAP) (U)

Commander
USASA Field Station, Berlin
APO New York 09742

1. (U) Reference IAEB-I Letter, dated 7 October 1975, Subject: Aggressive Defensive Source Acquisition Program (ADSAP) (U).

2. (C) I concur in cancellation of Project FILMAN and initiation of the Aggressive Defensive Source Acquisition Program by the 766th MID, 66th MI Group. A copy of the completed Memorandum of Understanding will be provided to this HQ, ATTN: DCSSEC.

for WILLIAM I. ROLYA
Brigadier General, USA
Commanding

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by DoD Dir 5200.1-R(2)
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Date of Document

727

INCL # 3

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOIPO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Request for Termination of ICIP Operation CANTER RIDE (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 5 May 1976

ACTION REQUIRED

To obtain formal ACSI approval for termination of subject ICIP.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without resource to other sources.)*

1. (C) Background:

a. By ltr, 25 Feb 75, subject: CANTER RIDE (U), CDR, USAINTA requested approval for ICIP OPLAN CANTER RIDE (U). The OPLAN provided for the insertion of an MI Warrant Officer in cover status into the Advance Sensors Directorate of the US Army Missile Command (USAMICOM), Redstone Arsenal, Alabama. This specialized CI support was requested by CG, USAMICOM, to enhance the security of the Directorate and determine the extent, if any, of hostile intelligence penetration of Redstone Arsenal. The OPLAN was approved by the ACSI on 4 Mar 75.

b. By 1st Ind, 8 Apr 76, subject as above, CDR, USAINTA advised that on 23 Feb 76, the ACSI gave verbal approval for termination of subject ICIP. The CDR, USAINTA recommended formal termination approval.

2. (C) Discussion:

a. After a thorough review, it has been determined that subject ICIP has successfully accomplished its objective.

b. CI security support is being provided the USAMICOM by the ~~902d MI Gp by the~~ 902d MI Gp Redstone Resident Office, under the provisions of its Direct Support Comprehensive Counterintelligence Program (DSCCR).

c. This action furnishes formal approval to CDR, USAINTA to terminate ICIP CANTER RIDE (U)

3. (U) Recommendation: That the 2d Ind, (TAB A) be approved and signed by the ACSI.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DEV		6 as revised
			DIR		
			EX		
			ACSI		
			DISPATCHED (DTG)		
			CDR, USAINTA		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

Classified by [illegible] GENERAL DECLASSIFICATION [illegible]

ACTION OFFICER (Name, grade, phone and signature)

M. S. BRANNAN/53501 M. Brannan 728

EXEMPTION CATEGORY 2

DECLASSIFY ON 31 Dec 2006

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

Page 2221 of 3957

~~CONFIDENTIAL~~

DAMI-DOH (2 Apr 76) 2d Ind
SUBJECT: Request for Termination of ICIP Operation CANTER RIDE (U)

DA, OACofS for Intelligence, ATTN: DAMI-DOH, Washington, DC 20310 1 MAY 1976

TO: Commander, US Army Intelligence Agency, Fort Meade, Maryland 20755

ICIP CANTER RIDE is formally terminated as recommended.

FOR THE DIRECTOR OF INTELLIGENCE OPERATIONS:

(Sgd) John L. Heiss III

JOHN L. HEISS III
Colonel, GS
Chief, HUMINT Division

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

729

4

Regraded Unclassified
When Separated
Classified Enclosure

~~CONFIDENTIAL~~

MIIA-GPB-AC(SP) 2 April 1976

SUBJECT: Request for Termination of ICIP Operation CANTER RIDE (U)

Commander
U. S. Army Intelligence Agency
ATIN: MIIA-SO
Fort Meade, Maryland 20755

1. (U) ~~(C)~~ After a thorough review, it has been determined that ICIP Operation CANTER RIDE has successfully accomplished its objective. To continue the operation utilizing SCOPI Source IC-B-083 would be an improper utilization of an MI warrant officer, and would increase the potential for compromise as long as the insert Source remains in the target area.

2. (U) ~~(C)~~ On 18 February 1976, I visited Major General Turnmeyer, Commander, U. S. Army Missile Command, Redstone Arsenal, Alabama. During the visit, Major General Turnmeyer requested a recommendation concerning the continuation of the operation. I indicated that there was no known indication of compromise, but in view of the above, recommended that the operation be terminated and Source extracted as soon as the personnel system would permit. Major General Turnmeyer expressed his deep appreciation for the information previously provided through the operation, and while expressing his complete concurrence that the operation had successfully met its objective, readily agreed that it should be terminated at once and the Source be extracted.

3. (U) ~~(C)~~ The above information was passed by my staff to members of the Support Detachment, USAINTA, and LTC Grimes, Commander, Special Operations Detachment, USAINTA, on 19 February 1976. Brigadier General Thompson, Commander, USAINTA, was informed of the above on 20 Feburary 1976 and Major General Aaron, ACSI, DA, on 23 February 1976.

4. (U) ~~(C)~~ On 23 and 27 February 1976, the 902d MI Group requested USAINTA assistance in the reassignment of Source IC-B-083. As a result of actions completed by the Support Detachment, USAINTA, Source is in receipt of reassignment orders with an expected PCS date of 8 April 1976.

CDR USAINTA
...SIFICATION
...ER 11652
DECLASSIFIED ON: 31 DEC 2006

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

730

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

MIIA-GPB-AC(SP) 2 April 1976
SUBJECT: Request for Termination of ICIP Operation CANTER RIDE (U)

5. (U) Comprehensive counterintelligence security support is also being provided to the U. S. Army Missile Command by the Redstone Resident Office, 902d MI Group, under the provisions of 902d MI Group Pamphlet 381-3, subject: Direct Support Comprehensive Counterintelligence Program (DSCCP) (U), to be published. The DSCCP, an all-source, multi-discipline threat concept which is being developed for use throughout the 902d MI Group, will continue in support of the U. S. Army Missile Command concurrent with the termination of the ICIP Operation.

6. (U) In view of the above, request formal approval of the termination of ICIP Operation CANTER RIDE.

HASSEL L. PARKER
Colonel, MI
Commanding

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

MIIA-SO-SA (2 Apr 76) 1st Ind (C)
SUBJECT: Request for Termination of ICIP Operation CANTER RIDE (U)

HEADQUARTERS, U. S. ARMY INTELLIGENCE AGENCY, Fort Meade, Maryland 20755

TO: HQDA (DAMI-DOH/LTC HAENDLE), WASH DC 20310

1. ~~(C)~~ As indicated by paragraph 2 of the basic letter, the 902d Military Intelligence Group and the Commanding General of the US Army Missile Command determined in February 1976 that the primary objective of ICIP CANTER RIDE had been accomplished and the operation should be terminated. On 20 February 1976 verbal approval of termination was given by the CDR, USAINTA- and by the ACSI on 23 February 1976.

2. ~~(C)~~ Counterintelligence security support is being provided to the US Army Missile Command by the 902d MI Group under its Direct Support Comprehensive Counterintelligence Program (DSCCP) as described in paragraph 5 of the basic letter. Arrangements have been made for the extraction and reassignment of the insert source used in this operation. Source will be debriefed and terminated subsequent to his 8 April 1976 reporting date by the 902d MI Group, which is also his new unit of assignment.

3. (U) Recommend formal approval of the termination of ICIP CANTER RIDE.

WILLIAM I. JENNINGS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH/PARA 1-603 DoD 5200.1-R

Classified by: Cdr USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
31 Dec 2006

732

~~CONFIDENTIAL~~

DOWNGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PA AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

ACTION SHEET

SUBJECT	CONTROL NUMBER
CDR USAINSCOM FOI/PA AUTH PARA 1-603 DoD 5200.1-R Request for Termination of ICIP Operation CANARY EFFORT (U)	
	OFFICE SYMBOL: DAMI-DOH; SUSPENSE:
	DATE: 6 May 1976

ACTION REQUIRED

To obtain formal ACSI approval for Termination of subject ICIP.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) ~~(C)~~ Background:

a. Subject ICIP was established several years ago to support Army organizations at Fort Ritchie, MD.

b. In Sep 75, the reorganization and redesignation of the US Army Communications Command (USACC) - CONUS as the 7th Signal Command resulted in a realignment of target areas of ICIP CANARY EFFORT (U), and increased coverage to the Telecommunications Directorate, the Alternate Joint Command Center (AJCC) the Alternate National Military Command Center (ANMCC), the Alternate National Command Center Support Directorate (ANMCCSD) and the East Coast Telecommunications Center (ECTC). Three sources and a Project Case Officer were used in this ICIP.

c. By 1st Ind, 8 Apr 76, subject as above, CDR USAINTA advised that on 23 Feb 76, the ACSI gave verbal approval for termination of subject ICIP and recommended that subject ICIP be given formal termination approval.

2. (U) ~~(C)~~ Discussion:

a. ICIP CANARY EFFORT (U) was chosen by the CDR, 902d MI Group to be replaced by an overt comprehensive all-source, multi-discipline security support concept as defined in 902d MI Group Pamphlet 381-3, subject: Direct Support Comprehensive Counterintelligence Program, to be published.

b. The ICIP sources previously supporting the operation were terminated without prejudice during Feb 76. The Great Skills Project Case Officer was released from duties on 1 Mar 76.

c. Supported commanders were briefed on CANARY EFFORT termination during Mar 76, and assured that this action in no way relieved the 902d MI Group of the responsibility for continued overt, all-source, multi-discipline support subsequent to 31 Mar76.

(Continue on plain bond)

IMPLICATIONS	CINFO YES ☐ NO ☐	PRIM PROGS YES ☐ NO ☐	BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		6 MAY revised
			DIR		
			EX		
			ACSI		
			DISPATCHED (DTG)		
			CDR, USAINTA		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

Classified by _____
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

ACTION OFFICER *(Name, grade, phone and signature)*

M. S. BRANNAN/53501 M. Brannan 733

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

Page 2226 of 3957

CONFIDENTIAL

DAMI-DOH
SUBJECT: Request for Termination of ICIP Operation CANARY EFFORT (U)

d. This action provides formal approval to CDR, USAINTA to terminate ICIP CANARY EFFORT (U).

3. (U) Recommendation: That the 2d Ind, (TAB A) be approved and signed by the ACSI, DA.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

~~CONFIDENTIAL~~

DAMI-DOH (2 Apr 76) 2d Ind
SUBJECT: Request for Termination of ICIP Operation CANARY EFFORT (U)

DA, OACofS for Intelligence, ATTN: DAMI-DOH, Washington, DC 20310

TO: Commander, US Army Intelligence Agency, Fort Meade, Maryland 20755

ICIP CANARY EFFORT is formally terminated as recommended.

FOR THE DIRECTOR OF INTELLIGENCE OPERATIONS:

2 Incl
nc

JOHN L. HEISS III
Colonel, GS
Chief, HUMINT Division

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY USAINSCOM POI/PA
Auth Para 4-102 DOD 5200.1R

735

~~CONFIDENTIAL~~

Regraded Unclassified
When Separated from
Classified Inclosures

Page 2228 of 3957

~~CONF~~

MIIA-GPB-AC(SP) 2 April 1976

SUBJECT: Request for Termination of ICIP Operation CANARY EFFORT (U)

Commander
U. S. Army Intelligence Agency
ATTN: MIIA-SO
Fort Meade, Maryland 20755

1. (U) References:

a. USAINTA Letter, MIIA-SO-SA, subject: Change in ICIP CANARY EFFORT Support (U), dated 27 Jan 76, with 902d MI Group 1st Ind, MIIA-GPB-AC(SP), dated 29 Jan 76.

b. 902d MI Group Letter, MIIA-GPB-AC(SP), subject: Termination of ICIP Operation CANARY EFFORT (U), dated 3 March 1976.

2. (U) As outlined in the above references, copies of which have been provided under separate cover, I have chosen ICIP Operation CANARY EFFORT to be replaced by an overt comprehensive all-source, multi-discipline security support concept as defined in 902d MI Group Pamphlet 381-3, subject: Direct Support Comprehensive Counterintelligence Program, to be published. Toward this end, confidential ICIP sources previously supporting the operation were terminated without prejudice during the month of February 1976. The Great Skills Project Case Officer was released from duties in support of the operation on 1 March 1976.

3. (U) The termination of the ICIP Operation was coordinated by my staff with LTC Grimes, Commander, Special Operations Detachment, USAINTA, on 19 February 1976. The oral approval of the termination was gained from Brigadier General Thompson, Commander, USAINTA, and Major General Aaron, ACSI, DA, on 20 and 23 February 1976 respectively. Supported commanders were briefed on the termination of the operation during March 1976 in conjunction with the regularly scheduled quarterly ICIP briefings, and assured that this action in no way relieved the 902d MI Group of the responsibility for continuing overt, all-source, multi-discipline support subsequent to 31 March 1976.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

736

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

MIIA-GPB-AC(SP) 2 April 1976
SUBJECT: Request for Termination of ICIP Operation CANARY EFFORT (U)

4. (U) In view of the above, request formal approval of the termination of ICIP Operation CANARY EFFORT.

HASSEL L. PARKER
Colonel, MI
Commanding

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

2

737

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

MIIA-SO-SA (2 Apr 76) 1st Ind (C)
SUBJECT: Request for Termination of ICIP Operation CANARY EFFORT (U)

HEADQUARTERS, U. S. ARMY INTELLIGENCE AGENCY, Fort Meade, Maryland 20755

TO: HQDA (DAMI-DOH/LTC HANDLE), WASH DC 20310

1. (U) References 1a and 1b of basic letter are attached as Enclosures 1 and 2, respectively.

2. (U) ~~(C)~~ As noted in paragraph 2 and 3 of basic letter, although ICIP Operation CANARY EFFORT was terminated effective 31 March 1976, counter-intelligence support will continue to be provided under the concepts of the 902d Military Intelligence Group Direct Support Comprehensive Counterintelligence Program, to be published. Verbal approval of this termination was given by the CDR, USAINTA, on 20 February 1976, and the ACSI on 23 February 1976.

3. (U) ~~(C)~~ Confidential sources utilized in this ICIP have been terminated.

4. (U) Recommend formal approval of the termination of ICIP CANARY EFFORT.

2 Incl
as

WILLIAM I. JENNINGS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by Cdr USAINTA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON: 31 Dec 2006

738
3

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 26 Mar 76

ACTION REQUIRED: To obtain approval of the quarterly ICIP report

MEMORANDUM FOR RECORD (*Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without resource to other sources.*)

1. (U) BACKGROUND: On 8 Feb 72, the Under Secretary of the Army requested that the VCSA provide a quarterly report on all ICIP operations.

2. (U) DISCUSSION:

a. During the past quarter there were no significant changes in number of operations or activities within operations. Reports of questionable suitability and security hazards were passed to the supported commands.

b. Memorandum at TAB A transmits summaries of ICIP operations through the VCSA to the Under Secretary of the Army for second quarter FY 76.

3. (U) RECOMMENDATION: That the Memorandum at TAB A be approved and signed by the ACSI.

(Continue on plain bond)

IMPLICATIONS: CINPO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		29 MAR 76
			DIR		31 Mar 76.
			EX		
			ACSI		
			DISPATCHED (OTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER (*Name, grade, phone and signature*)
R.V. Haendle
LTC Haendle/56159

739 3280-76

DOWNGRADED/DECLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

DOWNGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

[redacted]

DAMI-DOH

MEMORANDUM THRU: VICE CHIEF OF STAFF, UNITED STATES ARMY

FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) (U)--
INFORMATION MEMORANDUM

1. (S) During the past quarter, six of the currently active Internal Counterintelligence Program (ICIP) operations provided information on incidents involving personnel suitability and conditions reflecting poor security practices or weaknesses. Reports of these relatively minor conditions were furnished the commanders of the supported commands who took immediate corrective action.

2. (U) The total number of active ICIP operations remains at nine. Summaries of activity in these operations during the last quarter are inclosed.

9 Incl
as (C)

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

AUSA DA

31 Dec 96

740

[redacted]

DEPART[illegible]T OF THE ARMY
OFF[illegible]CE OF THE ASSISTANT [illegible]IEF OF STAFF FOR INTELLIGENCE
REFERRAL SLIP

ROUTING		ATTENTION OF
✓	DAMI-ZX	✓ Col Jones
	AO	DEVELOP ACSI POSITION
	AOM	
	AOP	
	AOS	COORDINATE WITH
	DO	
	DOA	
	DOH	COPY FURNISHED TO
	DOL	
	DOS	
	FI	REPLY TO
	FII	
	FII-E	
	FII-S	ACSI ACTION ASSIGNED TO
	FII-W	
	FIR	
	FIT	PROVIDE ASSISTANCE AS REQUIRED TO
	FL	
	IG	
	PB	
	SD	NOTE AND RETURN
	SG	
	SS	
	TA	INFORMATION
	TS	✓
	TSI	
	TSS	REMARKS
	TSS-C	✓ Pls see Col Jones's
	TSS-R	(OUSA) cmt, next unde.
	TSS-S	Will task DO to do.
	TST	
	TST-C	
	TST-S	

FROM [illegible] JAMES P. DINNIMAN 741 DATE
DAMI-JA MAJ, GS TELEPHONE
ACSI SACO 56967/52027 18 Aug 76

ACSI Form 379
22 JAN 76 3840-X REMAINS WITH DOCUMENT

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

DAMI-DOH

MEMORANDUM THRU: ~~VICE CHIEF OF STAFF, UNITED STATES ARMY~~

FOR: ~~UNDER SECRETARY OF THE ARMY~~ NOTED USA Date 12 APR 1976
COL John A. Todd, Exec., SAUS

SUBJECT: Internal Counterintelligence Program (ICIP) (U)--
INFORMATION MEMORANDUM

1. During the past quarter,* six of the currently active Internal Counterintelligence Program (ICIP) operations provided information on incidents involving personnel suitability and conditions reflecting poor security practices or weaknesses. Reports of these relatively minor conditions were furnished the commanders of the supported commands who took immediate corrective action.

2. (U) The total number of active ICIP operations remains at nine. Summaries of activity in these operations during the last quarter are inclosed.

9 Incl
as

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

* OCT-DEC 75

Noted by the Under Secretary of the Army with comment: "On next quarter's review, please provide an analysis (of each ICIP for the past year) to include statistics."

742

JOHN A. TODD
Colonel, GS
Executive

Classified by ACSI DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 62
DECLASSIFY ON 31 Dec 76

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DAMI-DOH

MEMORANDUM THRU: VICE CHIEF OF STAFF, UNITED STATES ARMY

FOR: UNDER SECRETARY OF THE ARMY

SUBJECT: Internal Counterintelligence Program (ICIP) (U)--
INFORMATION MEMORANDUM

1. ~~(C)~~ During the past quarter, six of the currently active Internal Counterintelligence Program (ICIP) operations provided information on incidents involving personnel suitability and conditions reflecting poor security practices or weaknesses. Reports of these relatively minor conditions were furnished the commanders of the supported commands who took immediate corrective action.

2. (U) The total number of active ICIP operations remains at nine. Summaries of activity in these operations during the last quarter are inclosed.

9 Incl
as ~~(S)~~

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by ACSI DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 8-2
DECLASSIFY ON 31 Dec 96

743

~~CONFIDENTIAL~~

[redacted]

(U) CANARY EFFORT: (OACSI Revalidation - 4 Feb 75)

a. Location: Fort Ritchie, MD.

b. Confidential Source Utilization: Three confidential sources.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) During the reporting period, adverse suitability information (indebtedness, drug or alcohol abuse, moral improprieties and mental instability) was reported concerning 17 individuals assigned sensitive duties. Monitoring continues; a limited investigation has been requested on one of the individuals.

(2) This ICIP had previously identified alleged users of narcotics. As a result of an investigation conducted by USACIDC, 13 of these individuals were apprehended and charged with drug violations. Eleven of these 13 had security clearances and had access to the Alternate Joint Command Center.

e. Operational Status:

(1) On 18 December, the Project Liaison Officer (PLO) presented a Quarterly Progress Report to the Commander, US Army Communications Command (USACC). On 30 December 1975, the PLO presented the Quarterly Progress Report to the Commander, Fort Ritchie; Commander, USACC Site R Telecommunications Center; and the Deputy ACSI&S, 7th Signal Command. All expressed appreciation and continued support for the ICIP.

(2) At the request of the Director, Administrative Services, JCS, the portion of this operation in support of the Alternate National Military Command Center was terminated.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

744

[redacted]

~~CONFIDENTIAL~~

2. (U) CANINE PLATE: (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD), Romulus, NY.

b. Confidential Source Utilization: None.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status:

During the period, one conventional source was terminated due to his transfer from the area. One source is under consideration for recruitment. He is in the Maintenance Division, Directorate for Special Weapons (DSW). DSW is the primary SAD activity being supported by this ICIP. On 21 December 1975, the PLO provided the Quarterly Briefing Report to COL Alden L. Cox, CDR, Seneca Army Depot.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

3. (U) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal, AL.

b. Confidential Source Utilization: One.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Adverse suitability information pertaining to a GS-12 civilian physicist with access to Secret information who was assigned to the Optical Guidance Technology Office (OGTO), indicated that he probably was the catalyst for the sexually-oriented gatherings of OGTO employees which prompted a Sep 74 AR 15-6 investigation of OGTO personnel ordered by the CG, USAMICOM. As a result of that investigation, the present ICIP operation was initiated. The employee, who is apparently obsessed with sex has had numerous extra-marital liaisons during the last five years. He transferred to the Infrared Technology Office, Advanced Sensors Directorate, a highly sensitive office, in Aug 74. The Source, who obtained information by elicitation, was successful in identifying him only in recent weeks. The employee's departure from OGTO apparently broke up the clique and Source could uncover no new evidence of such activities among remaining OGTO employees. Near the close of the reporting period, the employee applied for a position in Japan. The Commander, USAMICOM, was provided a summary of the information on the employee for appropriate command action.

(2) Source identified an Army 1LT who was attempting to civilianize his duty position. The individual is a naturalized citizen who was born in Shanghai, China. His security clearance was based on a favorable NAC only.

e. Operational Status: On 10 October 1975, the Commander, 902d MI Group and the Project Liaison Officer briefed MG George E. Turnmeyer, the newly assigned Commander, USAMICOM. MG Turnmeyer affirmed his approval of the operation. In a subsequent briefing on 10 November 1975, MG Turnmeyer was apprised of the information reported in sub-paragraph d(1) above. It was concluded that since the operation had provided the information initially sought, it is now necessary to refocus the effort to emphasize security matters rather than suitability problems.

REGRADED UNCLASSIFIED
ON SEP -5 1996
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

746

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

4. (C) CANVAS TAX: (OACSI Revalidation - 4 Feb 75)

a. Location: Sierra Army Depot (SIAD), US Army Materiel Command, Herlong, CA.

b. Confidential Source Utilization: One.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status:

One individual is under assessment for use as a confidential source. The quarterly progress report to SIAD officials was delayed until after the Christmas holidays. It is expected that the report will be presented sometime in January 1976.* The Commander and staff officers knowledgeable of the ICIP continue to provide their support.

*RPT SUBMITTED IN FEB 76; TO BE IN NEXT ICIP REPORT.
WRH

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

747

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

5. (U) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC.

b. Confidential Source Utilization: None.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) As a result of information gained concerning a suicide attempt by an Army NCO assigned to PTC a Limited Investigation was initiated. The investigation revealed that the NCO has a large number of outstanding debts, has lied on loan applications, and recently ordered a 1976 automobile which will cost in excess of five thousand dollars. Interviews concerning the NCO revealed alleged drug usage and homosexuality. USAINTA directed that the NCO be interviewed concerning the allegations against him. The NCO has been assigned to the Logistics Branch, PTC, pending results of the Limited Investigation.

(2) Adverse suitability information was reported on two additional NCOs assigned to PTC. Based on medical reports and rebellious attitudes one NCO was released from the Army by board action. The second NCO was reassigned to another Branch within the command and his access to classified information was suspended for 90 days pending resolution of adverse suitability information. The NCO after a night of heavy drinking at the Ft Meyer NCO Club, began hitting his wife when she tried to arouse him after he had "passed out." The wife filed assault charges with the Military Police and withdrew them later. The PTC Commander counselled the NCO on his drinking and marital problems and assigned him duties where he has no access to classified information.

e. Operational Status:

On 18 Dec 1975, the Project Liaison Officer (PLO), CENSUS TIME, presented the Quarterly Progress Briefing to COL Donald E. Clark, CDR, PTC. The PLO, CANARY EFFORT, was also present at the briefing. In a re-evaluation of the target priorities within PTC, COL Clark requested that the PTC element of the Army Operations Center and the Hoffman Telecommunications Center be covered by ICIP sources. Accordingly, the OPLAN for CENSUS TIME will be changed to include these targets.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

6. (U) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories (HDL), Adelphi, MD.

b. Confidential Source Utilization: None.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Suitability information concerning an employee of the Woodbridge Research Facility (WRF), a branch of HDL located in Woodbridge, VA, involved a problem of alcohol abuse. After counseling, the employee is undergoing a rehabilitation program.

(2) From 7 October to 6 November 1975, a courtesy penetration test of HDL's Adelphi Facility was conducted. The penetrations succeeded in revealing several security weaknesses and the supported command has taken corrective actions to remedy them. A number of the Security Guards were transferred and guard procedures were changed. A new magnetic coded badge has been approved for purchase in FY 77. The PLO will also give a lecture to the HDL Guard Force on the penetration test and ways to foil attempted penetrations.

e. Operational Status:

On 3 December 1975, the PLO presented the Quarterly Progress Report to COL Thomas McGregor, CDR, HDL. Also present at the briefing were MAJ Kenneth F. Keller and Mr. James F. Yeick, Security Officer, HDL.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

749

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

7. (X) GONDOLA STAR: (OACSI Revalidation - 11 Jul 75)

a. Location: Aberdeen Proving Ground (APG), Aberdeen, MD.

b. Confidential Source Utilization: Eight.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained.

(1) Sources reported several instances of foreign contact by military and DOD civilian personnel in the supported activity. In one instance a citizen of the Federal Republic of Germany was assigned on an exchange program to work in the US Army Human Engineering Laboratory (HEL) until Sep 76. The source, who provided information on an employee's travel to Poland and Czechoslovakia in 1975, provided additional information on the employee's plans to travel to those countries again in 1976. A report of a civilian DOD employee at Edgewood Arsenal with some unexplained periods of time in his background prompted a request for a Limited Investigation from the supported command.

(2) The source who reported on travel to the USSR in 1975 of a man and wife DOD employees of the supported activities at HEL and the US Army Materiel Systems Analysis Activity (USAMSAA) provided information on plans of the couple to take another tour to Russia in 1976.

(3) Sources reported allegations of questionable suitability factors involving eight employees assigned to the supported command. These unsubstantiated allegations consisted of five incidents of extramarital relations, one suggestion of other immoral conduct, one case of mental instability and one allegation of a fraudulent claim on a TDY voucher. Efforts are underway to substantiate or refute the reported allegations.

(4) Sources reported five instances of security weaknesses or poor security practices. These five instances consisted of two unattended offices in which security containers were left open, a CONFIDENTIAL document left unsecured over a three day weekend, poorly controlled access to a classified scientific conference at USAMSAA, and movement of the Ground Warfare Division of USAMSAA into a building in which no technical survey had been conducted prior to the move. These were brought to the attention of the appropriate security officials in the supported activities and corrective actions were taken.

e. Operational Status:

(1) On 1 Dec 75, the PLO presented the initial ICIP briefing to MG Patrick W. Powers, CDR, US Army Test and Evaluation Command (TECOM), and COL William H. Tucker, Jr., Chief of Staff, TECOM.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 2243 of 3957

CONFIDENTIAL

(2) On 18 Dec 75, the PLO gave the Quarterly Progress Briefing to COL Kenneth L. Stahl, CDR, Edgewood Arsenal, on those activities pertaining to the Edgewood Arsenal portion of the ICIP GONDOLA STAR.

(3) On 19 Dec 75, the PLO presented a Quarterly Progress Report on those activities of the Aberdeen Proving Ground which are supported by the ICIP to COL Alvin D. Ungerleider, CDR, APG. Mr. Harry A. Mencke, Installation Intelligence Officer, APG, was also present at the briefing.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

751

~~CONFIDENTIAL~~

8. ~~(C)~~ LENS HOLDER: (OACSI Revalidation - 4 Feb 75)

a. Location: White Sands Missile Range (WSMR), NM.

b. Confidential Source Utilization: Two confidential sources were utilized during the reporting period.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status:

One individual is under assessment as a confidential source in USA Missile Test and Evaluation Directorate, WSMR. On 2 December 1975 the Project Liaison Officer presented the Quarterly Progress Report to MG O. L. Tobiason, CG, WSMR. The following personnel were also present at the briefing: LTC Charles I. Davis, Chief, Security Office, WSMR; CPT Marcel Hull, SAIC, Ft Bliss Resident Office, 525th MI Gp; GS 13 William F. Arket, Chief, Intelligence Division, WSMR; and GS 13 Shigeru Tsubota, Deputy Operations Officer, 525th MI Gp, Presidio of Monterey, California.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

~~SECRET~~

9. ~~(S)~~ LENTIL MONKEY: (OACSI Revalidation - 4 Feb 75)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Five confidential sources.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Two instructors of the Bulgarian Language Department who are man and wife, and who previously had been accused by other members of the Bulgarian Department of having contacts with the Bulgarian Intelligence Service have changed their status during the quarter. Details of their histories have been provided the Federal Bureau of Investigation. The husband has accepted a teaching position with the State Department and left DLI. The wife remained in DLI as an instructor.

(2) An instructor of the Czechoslovakian Language Department reportedly is planning to resign from DLI in 1976, take her retirement pay in a lump sum and return to Czechoslovakia with her two sons.

b1 Per FBI

There are no indications that he intends to return to Czechoslovakia. This information has been passed to the FBI.

(3) A DLI employee, presently involved with the Hebrew Project, is reported to be maintaining close contact with the Israeli Consulate in San Francisco. The employee, an alien with an impressive background, including possible intelligence activities, has also applied for employment with the National Security Agency (NSA). Information presently known to Army Intelligence has been made available to NSA.

e. Operational Status:

(1) Five confidential sources were utilized during the quarter; one source was terminated due to graduation. A total of 12 individuals are under assessment as possible new sources, including two Technical Language Assistants. In addition to the five confidential sources, there are 23 confidential sources providing coverage of nine language departments and the DLI staff.

Regraded SECRET
ON 20 Mar 1998
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

~~SECRET~~

753

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(2) The PLO presented the Quarterly Progress Report on 16 Dec 75 to COL Samuel L. Stapleton, Commandant, DLI. Also attending the briefing were COL William F. Strobridge, CDR, 525th MI Group; CPT Brendon A. Xiques, SAIC, Ft Ord Resident Office, 525th MI Group; and Mr. James Green, Acting Security Officer, DLI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

754

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

DAMI-DOH

MEMORANDUM THRU: ~~VICE CHIEF OF STAFF, UNITED STATES ARMY~~

FOR: ~~UNDER SECRETARY OF THE ARMY~~ NOTED USA 2 APR 1976
Date.....
COL John A. Todd, Exec., SAUS

SUBJECT: Internal Counterintelligence Program (ICIP) (U)--
INFORMATION MEMORANDUM

1. (U) ~~(C)~~ During the past quarter,* six of the currently active Internal Counterintelligence Program (ICIP) operations provided information on incidents involving personnel suitability and conditions reflecting poor security practices or weaknesses. Reports of these relatively minor conditions were furnished the commanders of the supported commands who took immediate corrective action.

2. (U) The total number of active ICIP operations remains at nine. Summaries of activity in these operations during the last quarter are inclosed.

9 Incl
as (C)

HAROLD R. AARON
Major General, GS
ACofS for Intelligence

REGRADED UNCLASSIFIED
ON 5 SEP 1997
BY USAINSCOM POMPA
Auth Para 4-102 DOD 5200.1R

Noted by the Under Secretary of the Army with comment: "On next quarter's review, please provide an analysis (of each ICIP for the past year) to include statistics."

755

JOHN A. TODD
Colonel, GS
Executive

* OCT-DEC 75 WSH

Classified by ACSI DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 02
DECLASSIFY ON 31 Dec 76

~~CONFIDENTIAL~~

10 March 76

DPM-DO

Plse have AO call or see me.

756

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
REFERRAL SLIP

ROUTING		ATTENTION OF
	DAMI-Z	LTC Haenette
	AO	DEVELOP ACSI POSITION
	AOM	
	AOP	
	AOS	COORDINATE WITH
	DO	
	DOA	
	DOH	COPY FURNISHED TO
	DOL	
	DOS	
	FI	REPLY TO
	FII	
	FII-E	
	FII-S	ACSI ACTION ASSIGNED TO
	FII-W	
	FIR	
	FIT	PROVIDE ASSISTANCE AS REQUIRED TO
	FL	
	IG	
	PB	
	SD	NOTE AND RETURN
	SG	
	SS	
	TA	INFORMATION
	TS	
	TSI	
	TSS	REMARKS
	TSS-C	Contact ZX re attached
	TSS-R	
	TSS-S	
	TST	
	TST-C	
	TST-S	

FROM
DAMI-JA Maj Dinniman

TELEPHONE 757
56967/52027

DATE 10 MAR

ACSI Form 379
22 JAN 76

REMAINS WITH DOCUMENT

ROUTING AND TRANSMITTAL SLIP		ACTION
1 TO HAGNDLE/ERSONSOLO	INITIALS	CIRCULATE
	DATE	COORDINATION
2	INITIALS	FILE
	DATE	INFORMATION
3	INITIALS	NOTE AND RETURN
	DATE	PER CONVERSATION
4	INITIALS	SEE ME
	DATE	SIGNATURE

REMARKS

In addition - all items to be typed on same machine.

Do NOT use this form as a RECORD of approvals, concurrences, disapprovals, clearances, and similar actions

FROM	DATE
758	PHONE

OPTIONAL FORM 41
AUGUST 1967
GSA FPMR (41CFR) 100-11.206

GPO: 1973 O-525-336 5041-101

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 5 Mar 76

ACTION REQUIRED: To obtain appproval of the quarterly ICIP report

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) Background: On 8 February 1972, the Under Secretary of the Army requested that the VCSA provide a quarterly report on all ICIP operations.

2. (U) Discussion:

a. During the past quarter there were no significant changes in number of operations or activities within operations. Reports of questionable suitability and security hazards were passed to the supported commands.

b. Memorandum at TAB A transmits summaries of ICIP operations through the VCSA to the Under Secretary of the Army.

3. (U) Recommendation: That the Memorandum at TAB A be approved and signed by the ACSI.

(Continue on plain bond)

IMPLICATIONS — CINFO: YES ☐ NO ☐ | PRIM PROGS: YES ☐ NO ☐ | BUDGET: YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			GS		
			DEP		
			DIR		5 MAR 76
			EX		
			ACSI		
			DISPATCHED (DTG)		
SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET					

ACTION OFFICER (Name, grade, phone and signature)

LTC Haendle/56074

2359-76 759

ACSI FORM 28, 13 Sep 71

CONFIDENTIAL

REGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED INCLOSURES

REGRADED CLASSIFIED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

2. (C) CANINE PLATE: (OACSI Revalidation - 4 Feb 75)

a. Location: Seneca Army Depot (SAD), Romulus, NY

b. Confidential Source Utilization: None.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: During the period, one conventional source was terminated due to his transfer from the area. One source is under consideration for recruitment. He is in the Maintenance Division, Directorate for Special Weapons (DSW). DSW is the primary SAD activity being supported by this ICIP. On 21 December 1975, the PIO provided the Quarterly Briefing Report to COL Alden L. Cox, CDR, Seneca Army Depot.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

760

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

3. ~~(C)~~ (U) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal, AL.

b. Confidential Source Utilization: One.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Adverse suitability information pertaining to a civilian employee indicates that the employee is possibly the central figure who was the catalyst for events and allegations which led to the AR 15-6 investigation and initiation of this ICIP operation.

(2) Source continues his observations of employee who is a Jordanian by birth and concerning who information was furnished last quarter, but no new information of significance was developed.

(3) Source identified an Army 1LT who was attempting to civilianize his duty position. The individual is a naturalized citizen who was born in Shanghai, China. His security clearance was based on a favorable NAC only.

e. Operational Status: On 10 October 1975, the Commander, 902d MI Group and the Project Liaison Officer briefed MG George E. Turnmeyer, the newly assigned Commander, USAMICOM. MG Turnmeyer affirmed his approval of the operation. In a subsequent briefing on 10 November 1975, MG Turnmeyer was apprised of the information reported in sub-paragraph d(1) above. It was concluded that since the operation had provided the information initially sought, it is now necessary to refocus the effort to emphasize security matters rather than suitability problems.

REGRADED UNCLASSIFIED
ON SEP - 8 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

761

~~CONFIDENTIAL~~

CONFIDENTIAL

CANTER RIDE (U)

3. d.

(1) Adverse suitability information pertaining to a civilian GS-12 employee, b6, GS-12, the Optical Guidance Technology Office (OGTO), indicated that he probably was the catalyst for the sexually oriented gatherings in OGTO which prompted a Sep 74 AR 15-6 investigation of OGTO personnel ordered by the CG, USAMICOM. As a result of that investigation, the present ICIP operation was initiated. The employee, apparently obsessed with sex, has had numerous extra-marital liaisons during the last five years. b6 transferred to the Infrared Technology Office, Advanced Sensors Directorate in Aug 74, but the Source, who obtained information by elicitation, was successful in identifying him only in recent weeks. b6 departure from OGTO apparently broke up the clique and Source could uncover no new evidence of such activities among remaining OGTO employees. Near the close of the reporting period, b6 applied for a position in Japan. The Commander, USAMICOM, was provided a summary of information on b6

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

CONFIDENTIAL

~~CONFIDENTIAL~~

4. ~~(U)~~ CANVAS TAX: (OACSI Revalidation - 4 Feb 75)

a. Location: Sierra Army Depot (SIAD), US Army Materiel Command, Herlong, CA.

b. Confidential Source Utilization: One.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: One individual is under assessment for use as a confidential source. The quarterly progress report to SIAD officials was delayed until after the Christmas holidays. It is expected that the report will be presented sometime in January 1976. The Commander and staff officers knowledgeable of the ICIP continue to provide their support.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

763

~~CONFIDENTIAL~~

5. (C) CENSUS TIME: (OACSI Revalidation - 4 Feb 75)

a. Location: Pentagon Telecommunications Center (PTC), US Army Communications Command (USACC), The Pentagon, Washington, DC.

b. Confidential Source Utilization: None.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) As a result of information gained concerning a suicide attempt by an Army NCO assigned to PTC a Limited Investigation was initiated. The investigation revealed that the NCO has a large number of outstanding debts, has lied on loan applications, and recently ordered a 1976 automobile which will cost in excess of five thousand dollars. Interviews concerning the NCO revealed alleged drug usage and homosexuality. USAINTA directed that the NCO be interviewed concerning the allegations against him. The NCO has been assigned to the Logistics Branch, PTC, pending results of the Limited Investigation.

(2) Adverse suitability information was reported on two additional NCOs assigned to PTC. Based on medical reports and rebellious attitudes one NCO was released from the Army by board action. The second NCO was reassigned to another Branch within the command and his access to classified information was suspended for 90 days pending resolution of adverse suitability information. C. *

e. Operational Status:

On 18 December 1975, the Project Liaison Officer (PLO), CENSUS TIME, presented the Quarterly Progress Briefing to COL Donald E. Clark, CDR, PTC. The PLO, CANARY EFFORT, was also present at the briefing. In a re-evaluation of the target priorities within PTC, COL Clark requested that the PTC element of the Army Operations Center and the Hoffman Telecommunications Center be covered by ICIP sources. Accordingly, the OPLAN for CENSUS TIME will be changed to include these targets.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

764

~~CONFIDENTIAL~~

CENSUS TIME (U)

5. d.

(2) The NCO, after a night of heavy drinking at the Ft Meyer NCO Club, began hitting his wife when she tried to arouse him after he had "passed out." The wife filed assault charges with the Military Police and withdrew them later. The PTC Commander counselled the NCO on his drinking and marital problems and assigned him duties where he has no access to classified information.

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

765

Incl 5

[redacted]

6. (U) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories (HDL), Adelphi, MD.

b. Confidential Source Utilization: None.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Suitability information surfaced on a (WRF) employee's problem with alcohol abuse. After counseling the employee is undergoing a rehabilitation program.

(2) From 7 October to 6 November 1975, a courtesy penetration test of HDL's Adelphi Facility was conducted. The penetrations succeeded in revealing several security weaknesses and the supported command has taken corrective actions to remedy them. A number of the Security Guards were transferred and guard procedures were changed. A new magnetic coded badge has been approved for purchase in FY 77. The PLO will also give a lecture to the HDL Guard Force on the penetration test and ways to foil attempted penetrations.

e. Operational Status: On 3 December 1975, the PLO presented the Quarterly Progress Report to COL Thomas McGregor, CDR, HDL. Also present at the briefing were MAJ Kenneth F. Keller and Mr. James F. Yeick, Security Officer, HDL.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

766

[redacted]

~~CONFIDENTIAL~~

CENTAVO KID (U)

6. d.

(1) Woodbridge Research Facility (WRF), a branch of HDL located in Woodbridge, VA.

* (1) Suitability information concerning an employee of the Woodbridge Research Facility (WRF), a branch of HDL located in Woodbridge, VA, involved a problem of alcohol abuse. After counseling, the employee is undergoing a rehabilitation program.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

767

~~CONFIDENTIAL~~

Encl 6

~~CONFIDENTIAL~~

7. (C) GONDOLA STAR: (OACSI Revalidation - 11 Jul 75)

a. Location: Aberdeen Proving Ground (APG), Aberdeen, MD.

b. Confidential Source Utilization: Eight.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Sources reported several instances of foreign contact by military and DOD civilian personnel in the supported activity. In one instance a citizen of the Federal Republic of Germany was assigned on an exchange program to work in the US Army Human Engineering Laboratory (HEL) until Sep 76. The source, who provided information on an employee's travel to Poland and Czechoslovakia in 1975, provided additional information on the employee's plans to travel to those countries again in 1976. A report of a civilian DOD employee at Edgewood Arsenal with some unexplained periods of time in his background prompted a request for a Limited Investigation from the supported command.

(2) The source who reported on travel to the USSR in 1975 of a man and wife DOD employees of the supported activities at HEL and the US Army Materiel Systems Analysis Activity (USAMSAA) provided information on plans of the couple to take another tour to Russia in 1976.

(3) Sources reported eight allegations of questionable suitability factors involving employees assigned to the supported activity. Due to the lack of substantive information, the behavior of the individuals will be monitored.

(4) Sources reported five instances of security weaknesses or poor security practices. These were brought to the attention of the appropriate security officials in the supported activities for corrective action.

e. Operational Status:

(1) On 1 Dec 75, the PLO presented the initial ICIP briefing to MG Patrick W. Powers, CDR, US Army Test and Evaluation Command (TECOM), and COL William H. Tucker, Jr., Chief of Staff, TECOM.

(2) On 18 Dec 75, the PLO gave the Quarterly Progress Briefing to COL Kenneth L. Stahl, CDR, Edgewood Arsenal, on those activities pertaining to the Edgewood Arsenal portion of the ICIP GONDOLA STAR.

(3) On 19 Dec 75, the PLO presented a Quarterly Progress Report on those activities of the Aberdeen Proving Ground which are supported by the ICIP to COL Alvin D. Ungerleider, CDR, APG. Mr. Harry A. Mencke, Installation Intelligence Officer, APG, was also present at the briefing.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

GONDOLA STAR (U)

7. d.

(3) * ~~Activities,~~ US Army Materiel Systems Analysis Activity (USAMSAA) and Edgewood Arsenal.

(4) ** These five instances consisted of two unattended offices in which security containers were left open, a CONFIDENTIAL document left unsecured over a three day weekend, poorly controlled access to a classified scientific conference at USAMSAA, and movement of the Ground Warfare Division of USAMSAA into a building in which no technical survey had been conducted prior to the move. These were brought to the attention of the appropriate security officials in the supported activities and corrective actions were taken. ''

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Incl 7

[redacted]

8. (U) LENS HOLDER: (OACSI Revalidation - 4 Feb 75)

a. Location: White Sands Missile Range (WSMR), NM

b. Confidential Source Utilization: Two confidential sources were utilized during the reporting period.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained: None.

e. Operational Status: One individual is under assessment as a confidential source in USA Missile Test and Evaluation Directorate, WSMR. On 2 December 1975 the Project Liaison Officer presented the Quarterly Progress Report to MG O. L. Tobiason, CG, WSMR. The following personnel were also present at the briefing: LTC Charles I. Davis, Chief, Security Office, WSMR; CPT Marcel Hull, SAIC, Ft Bliss Resident Office, 525th MI Gp; GS 13 William F. Arket, Chief, Intelligence Division, WSMR; and GS 13 Shigeru Tsubota, Deputy Operations Officer, 525th MI Gp, Presidio of Monterey, California.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

Page 2263 of 3957

~~SECRET~~

~~CONFIDENTIAL~~

9. (~~S~~) (~~C~~) LENTIL MONKEY: (OACSI Revalidation - 4 Feb 75)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Five confidential sources.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Two instructors of the Bulgarian Language Department who are man and wife, and who previously had been accused by other members of the Bulgarian Department of having contacts with the Bulgarian Intelligence Service have changed their status during the quarter. Details of their histories have been provided the Federal Bureau of Investigation. The husband has accepted a teaching position with the State Department and left DLI. The wife remained in DLI as an instructor, ~~but her contract was to expire on 31 Dec 75.~~

(2) An instructor of the Czechoslovakian Language Department reportedly is planning to resign from DLI in 1976, take her retirement pay in a lump sum and return to Czechoslovakia with her two sons.

b1 Per FBI

There are no indications that he intends to return to Czechoslovakia. This information has been passed to the FBI.

(3) A DLI employee, presently involved with the Hebrew Project, is reported to be maintaining close contact with the Israeli Consulate in San Francisco. The employee, an alien with an impressive background, including possible intelligence activities, has also applied for employment with the National Security Agency (NSA). Information presently known to Army Intelligence has been made available to NSA.

e. Operational Status:

(1) Five confidential sources were utilized during the quarter; one source was terminated due to graduation. A total of 12 individuals are under assessment as possible new sources, including two Technical Language Assistants. In addition to the five confidential sources, there are 23 confidential sources providing coverage of nine language departments and the DLI staff.

Regraded ~~SECRET~~
ON 20 MAR 1998
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

~~CONFIDENTIAL~~ 111

~~SECRET~~

~~CONFIDENTIAL~~

(2) The PLO presented the Quarterly Progress Report on 16 Dec 75 to COL Samuel L. Stapleton, Commandant, DLI. Also attending the briefing were COL William F. Strobridge, CDR, 525th MI Group; CPT Brendon A. Xiques, SAIC, Ft Ord Resident Office, 525th MI Group; and Mr. James Green, Acting Security Officer, DLI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

7 12

~~CONFIDENTIAL~~

[redacted]

DEPARTMENT OF THE ARMY
HEADQUARTERS
U. S. ARMY INTELLIGENCE AGENCY
FORT MEADE, MARYLAND 20755

MIIA-SO-SA

JAN 13 1976

SUBJECT: Quarterly Reporting of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOH/LTC HAENDIE)
WASH DC 20310

(U)

1. During the 2d Quarter, FY 1976, six of the currently active Internal Counterintelligence Program (ICIP) operations provided information on incidents involving suitability and conditions reflecting poor security practices, hazards, or weaknesses. These reports, though they involved individual items of a relatively minor nature, were passed immediately to the supported commanders who have taken corrective action. The discovery of these conditions and actions taken have served to enhance the security of the supported facilities. The total number of active ICIP operations at the close of the period was nine.

2. (U) Summaries reflecting the details of the information reported and the status of each of the nine operations are inclosed.

9 Incl
as

WILLIAM I. JENNINGS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(U)
1. ~~(C)~~ CANARY EFFORT: (OACSI Revalidation - 4 Feb 75)

a. Location: Fort Ritchie, MD

b. Confidential Source Utilization: Three confidential sources.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) During the reporting period adverse suitability information concerning 17 individuals assigned sensitive duties within the target areas was reported. The adverse information which involved indebtedness, alcohol abuse, drug abuse, moral improprieties, and mental instability, was brought to the attention of the ICIP Coordinator for CANARY EFFORT. Activities of all the individuals are being monitored, and the 7th Signal Command has requested a limited investigation of one of the individuals.

(2) During the period 13 military personnel assigned to Fort Ritchie were apprehended and charged with drug violations as a result of a drug investigation conducted by the US Army Criminal Investigation Division Command (USACIDC). Of the 13 individuals apprehended, 11 possessed security clearances and had access to the Alternate Joint Command Center (AJCC). Six of those apprehended were members of the 572d Military Police Company (Security) and performed sensitive duties at the AJCC. The Project Liaison Officer (PLO), CANARY EFFORT, had previously identified those individuals apprehended as alleged users of narcotics.

(3) The supported Command took action to suspend access to classified information of eight individuals based on information originally surfaced by the ICIP. These were all involved in suitability situations as outlined in d(1), above.

e. Operational Status:

(1) On 17 November 1975, a newly assigned Project Case Officer (PCO), a member of the GREAT SKILLS Program, began his duties in conjunction with CANARY EFFORT.

(2) On 9 December 1975, the PLO established a 902d MI Group Liaison Office at Fort Detrick, MD. This office will provide greater flexibility for the PLO in carrying out his duties in connection with the East Coast Telecommunications Directorate (ECTC), which is at Fort Detrick and is one of the activities supported by the ICIP.

Regraded UNCLASSIFIED on
3 Dec 07
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

~~CONFIDENTIAL~~ 774

~~CONFIDENTIAL~~

CONFIDENTIAL

(3) On 18 December 1975, the PLO of CANARY EFFORT presented the Quarterly Progress Report to COL Donald E. Clark, Commander, US Army Communications Command (USACC) Operations Command at the USACC Pentagon Telecommunications Center. The PLO for ICIP CENSUS TIME was also present at the briefing.

(4) On 19 December 1975, the PLO presented a SAEDA/Threat/Security Awareness briefing to personnel assigned to the Alternate Joint Communications Center (AJCC), Site R.

(5) On 30 December 1975, the PLO presented the Quarterly Progress Report to the supported commands with the following in attendance: COL Harold G. deMoya, CDR, Ft Ritchie; COL John S. Eberle, CDR, USACC Site R Telecommunications Center; and Mr. Joseph J. Carroll, Deputy ACSI&S, 7th Signal Command and Ft Ritchie. Colonels Clark, deMoya, Eberle and Mr. Carroll expressed their appreciation and continued support for the ICIP.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

Page 2268 of 3957

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

(U) CANTER RIDE: (OACSI Approval - 4 Mar 75)

a. Location: US Army Missile Command (USAMICOM), Redstone Arsenal, AL

b. Confidential Source Utilization: One

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) The source utilized in this operation has provided information of an adverse suitability nature on a civilian employee of the Optical Guidance Technology Office (OGTO), Advance Sensors Directorate (ASD), which indicate the employee is possibly the central figure who was the catalyst for the events and allegations during the Sep 74 AR 15-6 investigation which led to the initiation of the operation. This information has been provided the Commander, USAMICOM, in a Summary of Information. The CDR, USAMICOM, is considering what future action will be taken on the employee, if any. Evaluation of information provided on eight of the co-workers of the above employee indicates no further investigation with regards to their suitability is required at this time.

(2) The source is continuing his observation of the ASD employee who is a Jordanian by birth but learned no new information of significance during the period. Information on this individual was reported previously in the 1st Qtr, FY 76.

(3) Source identified an Army 1LT who was attempting to civilianize his duty position. The individual became of CI interest when it was learned that he is a naturalized citizen, born in Shanghai, China, with a security clearance granted on the basis of a favorable NAC only.

e. Operational Status:

(1) On 10 Oct 75, COL Stubblebine, CDR, 902d MI Group, accompanied by the PLO, MAJ Gipson, briefed the newly assigned CDR, USAMICOM, MG George E. Turnmeyer, on the operation with the USAMICOM Chief of Staff, COL Arthur G. Lange, Jr., in attendance. The USAMICOM officials were provided a copy of the EEI used in the operation and an update of the information provided by Source. MG Turnmeyer affirmed his approval of the operation.

(2) In a separate session on 10 Oct 75, COL Stubblebine briefed COL William P. Gojsza, Deputy Director, US Army Missile Research, Development and Experimental Laboratory (USAMRDEL), on Source's role in the operation since COL Gojsza is Source's immediate supervisor in Source's "part-time" cover duty as the USAMRDEL Administrative Officer.

Page 2269 of 3957

(3) On 10 Nov 75, COL Stubblebine and the PLO briefed MG Turnmeyer and Dr. McDaniel, Director, USAMRDEL, on an operational update and the 902d MI Group recommendations for continuation of the operation. After presenting the information contained in sub-paragraph d, above, conclusions were reached to the effect that since the operation had provided the information initially sought, it is now necessary to refocus the EEI, emphasizing security aspects rather than suitability matters. New EEI will be formulated with the supported command and the 902d MI Group.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

777

~~SECRET~~

~~CONFIDENTIAL~~

6. (S) CENTAVO KID: (OACSI Revalidation - 4 Feb 75)

a. Location: Harry Diamond Laboratories (HDL), Adelphi, MD

b. Confidential Source Utilization: None.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) The Technical Director, HDL, received a postcard request from a person unknown to him which asked for information on "Dirty Work," by the CIA. The card, with pertinent explanatory remarks, was provided to the Central Intelligence Agency.

(2) No new incidents of aircraft overflights were reported at any HDL facilities during the reporting period. Two overflight incidents were reported at the Woodbridge Research Facility (WRF), Woodbridge, VA, during the 1st Quarter, FY 76.

b1 Per FBI

(3) Suitability information surfaced on a WRF employee's problem with alcohol abuse. After counseling the employee is undergoing a rehabilitation program.

(4) From 7 October to 6 November 1975, a courtesy penetration test of HDL's Adelphi Facility was conducted. The penetrations succeeded in revealing several security weaknesses and the supported command has taken corrective actions to remedy them. A number of the Security Guards were transferred and guard procedures were changed. A new magnetic coded badge has been approved for purchase in FY 77. The PLO will also give a lecture to the HDL Guard Force on the penetration test and ways to foil attempted penetrations.

e. Operational Status:

On 3 December 1975, the PLO presented the Quarterly Progress Report to COL Thomas McGregor, CDR, HDL. Also present at the briefing were MAJ Kenneth F. Keller and Mr. James F. Yeick, Security Officer, HDL.

Regraded SECRET
ON 20 MAR 1998
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

~~SECRET~~

778

~~CONFIDENTIAL~~

7. (U) GONDOLA STAR: (OACSI Revalidation - 11 Jul 75)

a. Location: Aberdeen Proving Ground (APG), Aberdeen, MD.

b. Confidential Source Utilization: Eight.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Sources reported several instances of foreign contact by military and DOD civilian personnel in the supported activity. In one instance a citizen of the Federal Republic of Germany was assigned on an exchange program to work in the US Army Human Engineering Laboratory (HEL) until Sep 76. The source who provided information on an employee's travel to Poland and Czechoslovakia in 1975 provided additional information on the employee's plans to travel to those countries again in 1976. USAINTA is debriefing the employee. A report of a visit by one British and three Canadians to Edgewood Arsenal in early Dec 75 was checked and it was determined that the visit had been properly cleared and coordinated. A report of a civilian DOD employee at Edgewood Arsenal with some unexplained periods of time in his background prompted a request for a Limited Investigation from the supported command.

(2) The source who reported on travel to the USSR in 1975 of a man and wife DOD employees of the supported activities at HEL and the US Army Materiel Systems Analysis Activity (USAMSAA) provided information on plans of the couple to take another tour to Russia in 1976.

(3) A source reported one instance in which the HEL received a request for bibliographies of HEL publications from the Institute of Experimental Psychology, Slovak Academy of Sciences, Bratislava, Czechoslovakia. The Director, HEL, advised the requester that copies of the bibliographies were no longer available for distribution to the public. HEL suggested that future requests be submitted through the Czechoslovakian Embassy to the National Technical Information Services, Springfield, VA.

(4) Sources reported eight allegations of questionable suitability factors involving employees assigned to the supported activity. Due to the lack of substantive information to substantiate the reports, the behavior of the individuals will be monitored.

(5) Sources reported five instances of security weaknesses or poor security practices. These were brought to the attention of the appropriate security officials in the supported activities for corrective action.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

779

e. Operational Status:

(1) On 1 Dec 75, the PLO presented the initial ICIP briefing to MG Patrick W. Powers, CDR, US Army Test and Evaluation Command (TECOM), and COL William H. Tucker, Jr., Chief of Staff, TECOM.

(2) On 18 Dec 75, the PLO gave the Quarterly Progress Briefing to COL Kenneth L. Stahl, CDR, Edgewood Arsenal, on those activities pertaining to the Edgewood Arsenal portion of the ICIP GONDOLA STAR.

(3) On 19 Dec 75, the PLO presented a Quarterly Progress Report on those activities of the Aberdeen Proving Ground which are supported by the ICIP to COL Alvin D. Ungerleider, CDR, APG. Mr. Harry A. Mencke, Installation Intelligence Officer, APG, was also present at the briefing.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~ SECRET

9. ~~(S)~~(C) LENTIL MONKEY: (OACSI Revalidation - 4 Feb 75)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Five confidential sources.

c. Information Obtained or Reported on Non-Affiliated Civilians: None.

d. Useful Information Obtained:

(1) Two instructors of the Bulgarian Language Department who are man and wife, and who previously had been accused by other members of the Bulgarian Department of having contacts with the Bulgarian Intelligence Service have changed their status during the quarter. Details of their histories have been provided the Federal Bureau of Investigation. The husband has accepted a teaching position with the State Department and left DLI. The wife remained in DLI as an instructor but her contract was to expire on 31 Dec 75.

(2) An instructor of the Czechoslovakian Language Department reportedly is planning to resign from DLI in 1976, take her retirement pay in a lump sum and return to Czechoslovakia with her two sons.

b1 Per FBI

There are no indications that he intends to return to Czechoslovakia. This information has been passed to the FBI.

(3) A DLI employee, presently involved with the Hebrew Project, is reported to be maintaining close contact with the Israeli Consulate in San Francisco. The employee, an alien with an impressive background, including possible intelligence activities, has also applied for employment with the National Security Agency (NSA). Information presently known to Army Intelligence has been made available to NSA.

e. Operational Status:

(1) Five confidential sources were utilized during the quarter; one source was terminated due to graduation. No new sources have been recruited due to the Feb 76 departure of the PCO for an overseas assignment. No new PCO has been designated. A total of 12 individuals are under assessment as possible new sources, including two Technical Language Assistants. Formal recruitment is being delayed pending assignment of a new PCO. In addition to the five confidential sources, there are 23 conventional sources providing coverage of nine language departments and the DLI staff.

Regraded SECRET
ON 20 MAR 1998
By CDR USAINSCOM FOI/PO
Auth Para 6-601 DOD 5200.1R

~~CONFIDENTIAL~~ SECRET

(2) The Commandant, DLI, has established a security briefing program for all incoming students as part of their initial orientation. The PLO participates in this briefing, giving a lecture which emphasizes the lack of security clearances and the need-to-know of the instructors, previous cases of security incidents at DLI, and examples of reportable security situations. Navy, Marine, Air Force, and civilian students attend these briefings as well as Army personnel. Two such briefings were given during the reporting period.

(3) On 5 Dec 75, MAJ Richard Erickson, DLI Security Officer, departed DLI for a new assignment. His replacement will arrive in mid-Feb 76. Mr. James Green, DLI Personnel Security Specialist, is acting Security Officer pending arrival of the designated Security Officer.

(4) The PLO presented the Quarterly Progress Report on 16 Dec 75 to COL Samuel L. Stapleton, Commandant, DLI. Also attending the briefing were COL William F. Strobridge, CDR, 525th MI Group; CPT Brendon A. Xiques, SAIC, Ft Ord Resident Office, 525th MI Group; and Mr. James Green, Acting Security Officer, DLI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2275 of 3957

REGRADED UNCLASSIFIED ON SEP 5 1997 BY CDR USAINSCOM FOIPO AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 20 February 1976

ACTION REQUIRED: To acquire ACSI approval of OPLAN for ICIP CARELESS TOKEN (U) by signature on approving correspondence.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) ~~(C)~~ BACKGROUND: (U)

a. (U) ~~(C)~~ From correspondence between USAINTA and DCSI, USAREUR, it was learned that the 66th MI Group was providing ICIP support to Detachment N, US Army Security Agency Field Station, Augsburg, FRG. The support had been requested by the Commander, USASA Field Station, Augsburg and approved by DCSI, USAREUR and the Commander, USASA, Arlington Hall, VA.

b. (U) In an exchange of messages with DCSI, USAREUR, DAMI-DOH advised the DCSI of the existing policy pertaining to ICIP's in CONUS and the requirement to furnish quarterly reports to the Under Secretary of the Army. In light of the ACSI's policy to personally review all new ICIP's, DCSI, USAREUR decided to forward the OPLAN for ICIP CARELESS TOKEN (U) for ACSI review. The operation is already ongoing and approved by appropriate USAREUR and USASA officials.

2. (U) ~~(C)~~ DISCUSSION: (U)

a. (U) ~~(C)~~ The OPLAN for ICIP CARELESS TOKEN (U) is designed to detect and counter vulnerability to espionage by USASA personnel assigned to an isolated USASA detachment in the vicinity of the FRG/CSSR border. Standard ICIP procedures have been employed using recruited sources, a Project Liaison Officer and a Project Control Officer.

b. (U) By separate action, a policy letter to all Army Intelligence commands will be prepared to assure that ICIP policy is established and reporting requirements to the Under Secretary are met.

USAREUR continuation of the ICIP inside

3. (U) RECOMMENDATION: That the 5th Indorsement approving the OPLAN at TAB A be signed by the ACSI.

(Continue on plain bond)

IMPLICATIONS	CINFO	YES ☐	NO ☐	PRIM PROGS	YES ☐	NO ☐	BUDGET	YES ☐	NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		
			DIV		23 Feb 76
			DIR		24 Feb 76
			EX		
			ACSI	for	25 FEB [illegible]
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

ACTION OFFICER *(Name, grade, phone and signature)*
LTC Haendle/56159 T. V. Haendle 783

ACSI FORM 28, 13 Sep 71

1933-76

~~CONFIDENTIAL~~

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

~~CONFIDENTIAL~~

DAMI-DOH (30 Jun 75) 5th Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

HQDA, Office of the Assistant Chief of Staff for Intelligence, The Pentagon, Washington, DC 20310

TO: Commander, US Army Europe and Seventh Army, ATTN: DCSI, APO New York 09403

1. (U) Continuation of your ICIP CARELESS TOKEN (U) under the May 1975 Operations Plan earlier approved at your Headquarters in support of US Army Security Agency, Field Station, Augsburg, is approved.

2. (U) As indicated in earlier correspondence, a Memorandum to the Under Secretary of the Army is prepared quarterly by the Office of the Assistant Chief of Staff for Intelligence, DA Staff which includes a brief summary of developments and status of each ongoing ICIP. Field input is requested by the 15th of the month following the end of each calendar year quarter.

1 Incl
nc

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by_____
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 3
DECLASSIFY ON_____

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
UNITED STATES ARMY SECURITY AGENCY
ARLINGTON HALL STATION
ARLINGTON, VIRGINIA 22212

IASEC

30 JUN 1975

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Commander
US Army Security Agency
Field Station, Augsburg
APO New York 09458

1. (U) Reference IAEASC Letter dated 10 June 1975, Subject: Internal Counterintelligence Program (ICIP) (C).

2. (C) I have reviewed the proposal to initiate an Internal Counterintelligence Plan within Detachment N by the 66th MI Group and approve. It is essential that this Headquarters and Deputy Commander USASA Europe be kept apprised of significant events which develop from this operation.

GEORGE A. GODDING
Major General, USA
Commanding

1 Incl
1. Operations Plan (dup)

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by [redacted]
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY [redacted]
DECLASSIFY ON [redacted]

785

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

IAEASC (30 Jun 75) 1st Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Headquarters, US Army Security Agency Field Station, Augsburg, APO New York 09458

TO: Chief, Headquarters Det - CI, 66th MI Group, ATTN: Chief SOD, APO New York 09108

1. This command concurs with comments outlined in paragraph 2 of basic letter and recommends implementation of attached plan.

2. Per previous agreement, all major actions concerning the proposed plan will be discussed with the Field Station point of contact, LTC D. G. Schofield, S2.

DONALD M. MOREAU
COLONEL, MI
COMMANDING

1 Incl
nc

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

REGRADED UNCLASSIFIED
WHEN SEPERATED FROM CLASSIFIED
INCLOSURES

~~CONFIDENTIAL~~

CONFIDENTIAL

AEUMI-M-SOD (30 Jun 1975) 2d Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

DA, Special Operations Detachment, 66th Military Intelligence Group, APO New York 09108
11 July 1975

TO: Commander, 66th Military Intelligence Group, ATTN: AEUMI-T-CE, APO New York 09108

1. (U) SUBJECT Operations Plan has been coordinated with and approved by US ASA, Arlington Hall Station and USASA Field Station Augsburg. Attention is invited to paragraph 2 of 1st Indorsement designating LTC D. G. Schofield, S2, USASA Field Station Augsburg as the ASA point of contact.

2. (U) The following members of Special Operations Detachment are knowledgeable of the OPLAN:

a. Harold L. Roberts, GS-13, 19 May 1975

b. Philip D. Kinsatt, Major, 19 May 1975

c. Ben Davis, GS-12, 20 May 1975

d. Ted R. Snediker, GS-12, 21 May 1975

1 incl
nc

HAROLD L. ROBERTS
GS-12 ESP
Detachment Chief

CLASSIFIED BY Para 46, AR 381-12, 18 Oct 1974
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Approval of ACSI DA

DOWNGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

Page 2280 of 3957

~~CONFIDENTIAL~~

19 JUL 1975

AEUMI-T-CE (30 Jun 1975) 3rd Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Headquarters, 66th Military Intelligence Group, APO 09108

TO: Deputy Chief of Staff, Intelligence, USAREUR and Seventh Army,
ATTN: AEAGB-CI(SO) (Mr. Roseto), APO 09403

1. (U) References:

a. Message, AEAGB-CI(SO), DCSI, USAREUR, DTG 151640Z Jul 75 (U), Subject as above.

b. Message, SSO Intelligence Agency, DTG 011540Z Jul 75 (C), Subject as above, retransmitted.

c. PONECON, Mr. Roseto (DCSI USAREUR) and Mr. Kirk (this headquarters), 15 July 1975, concerning Subject.

d. Message, AEUMI-T-CE, this headquarters, DTG 071622Z Feb 75 (C), Subject as above.

2. (C) In accordance with references 1a and b, above, and provisions of the attached approved Operations Plan (OPLAN), coverage of the target facility will be implemented immediately. Routine liaison visits to the target facility have revealed that the expected drawdown of personnel for reasons stated in reference 1d, above, is already underway and personnel strength is expected to be reduced by 50% by October 1975; therefore, as discussed in reference 1c, above, prompt implementation of the ICIP OPLAN is considered essential in reducing possible adverse effects of the above and resulting personnel turbulence.

3. (U) A copy of the Quarterly Status Report will be provided to your headquarters in accordance with paragraph 2 of reference 1a, above.

FOR THE COMMANDER:

Robert T. Browne

1 Incl
nc

ROBERT T. BROWNE
COL, MI
Director of Operations

CF:
CDR, 511th MI Bn, ATTN: AEUMI-N-CE (Mr. Foss) (w/incls less OPLAN)
Chief, SOD (w/o incls)

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CLASSIFIED BY [illegible]
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY [illegible]
DECLASSIFY ON [illegible]

788

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

AEAGB-CI(SO) (30 Jun 75) 4th Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Headquarters, United States Army, Europe and Seventh Army,
Office of the Deputy Chief of Staff, Intelligence,
APO New York 09403

1975

TO: HQDA (DAMI-DOH), WASH DC 20310

1. (U) References:

a. Message, AEAGB-CI(SO), USAREUR, 171231Z September 1974, subject: Former ASA Personnel (C) (BOM).

b. Message, USAINTA, 182138Z September 1974, subject: Former ASA Personnel (C) (BOM).

c. Message, AEAGB-CI(SO), USAREUR, 191755Z June 1975, subject as above (C) (BOM).

d. Message, USAINTA, 011540Z July 1975, subject as above (C) (BOM).

e. Message, DAMI-DOH, DA, 032115Z December 1975, subject as above (C).

f. Message, AEAGB-CI(SO), USAREUR, 061755Z January 1975, subject as above (C).

2. (U) In accordance with your request in reference 1e, the attached Operations Plan for the Internal Counterintelligence Program (ICIP), CARELESS TOKEN, in support of Detachment N, US Army Security Agency, Field Station Augsburg, is furnished for ACSI review and approval. This plan was approved for implementation by ODCSI, USAREUR on 15 July 1975, prior to receipt of the new DA policy for ICIP reflected in reference 1e.

3. (U) Quarterly status reports pertaining to CARELESS TOKEN will be forwarded under separate cover.

4. (U) ODCSI, USAREUR, Action Officer is Mr David R. Smith, AEAGB-CI(SO), HM 7354 (AUTOSEVOCOM 6742).

FOR THE DEPUTY CHIEF OF STAFF, INTELLIGENCE:

A. J. IADEROSA
Colonel, GS
Chief, Counterintelligence
Division

1 Incl
nc

DOD DIR 5·5200

789

2 NOTIFICATION OF ORIGINATOR

5 ~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
UNITED STATES ARMY SECURITY AGENCY FIELD STATION, AUGSBURG
APO NEW YORK 09458

IAEASC

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

Commander
US Army Security Agency
ATTN: DCSSEC
Arlington Hall Station
Arlington, Virginia 22212

1. (U) Reference IASEC Letter (S) 3 March 1975 w/control #75 IASEC 00123.

2. (U) Inclosure 1 contains introductory letter and plan for ICIP within this command and is forwarded per paragraph 4, reference above.

3. (C) This command acknowledges the requirement for a program such as is outlined in the plan attached and recommends approval by CG, USASA. It has long been a recognized fact that US forces in Europe operate within a hostile intelligence environment, this being particularly true for USASA with its sensitive product. Initiation of the attached ICIP would provide a valuable asset in upgrading this command's internal security posture. On the negative side, the short period of continued operations at Detachment N, where the plan is to be utilized, raises the question that the effort could be better expended at another detachment or at FSA.

4. (U) Request an expeditious reply in order to inform the 66th MI Group.

1 Incl
as

DONALD M. MOREAU
COL, MI
Commanding

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by: [illegible]
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON [illegible]

790

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

OPERATIONS PLAN

SUBJECT: Internal Counterintelligence Program (ICIP)(U)

DATE: 5 MAY 1975

REPORT NO: B03130-079-75

PROJECT NO: B04142

OPLAN NO: 1-75

REFERENCES: a. Letter, AEAGB-CI(SO), dated 27 December 1974, subject: Internal Counterintelligence Program (ICIP), with 1st Ind, AEUMI-T-CE, 15 January 1975

b. Letter of Instruction (LOI) 6-TD, Source Management, HQ 66th MI Group, 14 January 1974

c. Letter, IAME-CDR, dated 16 April 1973, subject: LA FAIRE VITE Security Requirements (U), with 1st Ind, AEAGB-CI(GS), 25 April 1973 and 2d Ind, AEUMI-ISC, 31 May 1973

d. FM 30-17A (C), Counterintelligence Special Operations, February 1973

e. AR 381-12, Subversion and Espionage Directed Against the US Army and Deliberate Security Violations, 15 October 1974

1. (U) MISSION.

a. Requirement: To collect significant counterintelligence information through the utilization of overt liaison contacts and Confidential Recruited Sources (CRS) assigned to Detachment N, US Army Security Agency Field Station Augsburg (USASAFSA), located at Rimbach (UQ4555), Federal Republic of Germany (FRG) (hereafter referred as the target), and who are specifically targetted against personnel security vulnerabilities of assigned target personnel and hostile intelligence activities directed against the target.

b. Objective: To provide responsible commanders and supervisors of US Army Security Agency Europe (USASAE) a concentrated program designed to detect, eliminate or neutralize:

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

PADA
CLASSIFIED BY 4b, AR 381-12, 15 Oct 74
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON Approval of ACSI-DA

~~CONFIDENTIAL~~

Page 2284 of 3957

CONFIDENTIAL

(1) Espionage, sabotage, subversion or deliberate security violations against the target or the personnel assigned thereto.

(2) Disloyalty, disaffection and security weaknesses prevalent among personnel assigned to the target.

(3) Individuals in sensitive positions who, by character weaknesses or personal conduct, render themselves vulnerable to coercion or blackmail by a Hostile Intelligence Service (HoIS), either in their present assignment or at a later date. The foregoing includes drug and alcohol abuse.

c. Base of Operations: Headquarters, 511th Military Intelligence Battalion, Fuerth (PW4402), FRG.

2. PERSONNEL.

a. Source Personnel: Not yet selected. Spotting and assessing has commenced, however, no selections will be made prior to approval of this Plan.

(1) MOS: A minimum of two USASAMSA personnel, assigned to the target and meeting most of the following criteria, will be required:

(a) Male, between the ages of 21 and 35 years

(b) Unmarried (or "geographical bachelor")

(c) Have own Privately Owned Vehicle (POV) or the intent and independent means to purchase one shortly

(d) Have a desire and agree to a regular pattern of travelling away from the immediate target area during extended breaks from duty

(e) Friendly and likeable disposition, and ability to make friends, and to relate to and enjoy the confidences of co-workers

(f) Trustworthy, reliable and discreet

(g) Ability to take directions

(h) Willing to consume alcoholic beverages without habitually becoming intoxicated

(i) No record of derogatory information, to include character deficiencies

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

(j) Reasonable amount of intelligence and a high degree of common sense

(k) Above average sense of loyalty to duty and country and a strong dedication to duty assignment

(l) Career-oriented, or not yet decided whether to remain in the Army

(m) DEROS not earlier than one year from recruitment as a CRS

(2) Support Sources: It is not anticipated that any support sources will be required in this operation. If the operation develops to a degree of complexity requiring support sources, this Plan will be revised accordingly.

b. US Army Intelligence (USAI) Personnel:

(1) Project Liaison Officer (PLO):

(a) The PLO will be responsible for Overt Liaison Contacts and the spotting and assessing of potential CRS at the target. A Special Agent assigned to Resident Office Regensburg (ROR), 511th MI Battalion, will function as PLO consistent with ROR having area responsibility for the target area and liaison responsibility to the target.

(b) Designee: S/A Ronald Crawford, who has experience in both counterintelligence and collection activities, to include source handling; his DEROS is 1976.

(2) Project Control Officer (PCO):

(a) The PCO will be responsible for the recruitment and controlling of CRS engaged in this operation. The PCO will be assisted by an Assistant PCO as required.

(b) Designee: PCO - S/A John W. Carpenter, CE Section, 511th MI Battalion, who is an experienced counterintelligence operative with prior source handling duties. His DEROS is October 1975. A qualified replacement as PCO will be selected well in advance.

(3) Additional Special Agents assigned to the 511th MI Battalion, or other elements of the 66th MI Group, may from time to time be required during the tenure of this operation for the assessment and/or recruitment of selected CRS.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2286 of 3957

CONFIDENTIAL

Operations Plan, BO3130-079-75

(4) Supervision for the conduct and operating control of this operation within the 511th MI Battalion will be vested in the Chief, Counterespionage (CE) Section. Designee: S/A Donald A. Foss, Chief, CE Section, will also be the 511th MI Battalion's designated representative for any coordination with Commander, USASAFSA, Augsburg (PC4060), FRG, as may be needed.

(5) Broad Battalion operational monitorship control and policy guidance are vested in the Battalion Operations Officer/Assistant Operations Officer.

(6) The Director of Operations, Headquarters, 66th MI Group, will be responsible for the operational control of this ICIP, will coordinate all ICIP activities with the ICIP Control Officer, ODCSI, USAREUR, and with the Commander, USASAFSA, and will levy requirements on other subordinate counterintelligence (CI) elements of the 66th MI Group regarding this operation as may be appropriate. The ICIP Control Officer, Headquarters, 66th MI Group, will be Mr. Earl L. Kirk, Section Chief, CE Branch, Director of Operations.

3. (C) COVER AND DOCUMENTATION:

a. b1

(1) b1

(2) b1

b. b1

4 794

CONFIDENTIAL

b1

c.

b1

4 (U) ~~(C)~~ EXECUTION:

a. Background:

(1) The geographic location, isolation and highly sensitive mission of the target make it of logical interest to HoIS, particularly the CSSR Intelligence Service (CIS). Some magnitude of this threat is revealed in recent activities involving former ASA personnel travelling to the CSSR shortly after release from active duty, the association of target personnel with Czech nationals residing in the target area, and the presence of semi-official Czech representatives, e.g., Skoda automobile firm, in the target area.

(2) Past investigations and counterintelligence special operations concerning the target and assigned personnel have resulted in the conclusion that the very nature of the target, through its remote location, and its assigned personnel, who frequently keep to themselves during off-duty hours, requires a member of the target unit itself to answer the EEI covered by this Plan. There are no other US installations in the vicinity, and all target personnel live on the economy or in leased Government quarters, and frequent local public establishments and associate with local residents to a predominate degree. Many residents of the target area have family or ethnic ties with residents of the CSSR and there is considerable legal travel across the border in the target area, both by FRG and CSSR residents. Shift work at the target provides for periodic long breaks by assigned personnel between shifts, and their activities and whereabouts during these break periods are virtually impossible to ascertain and are practically unknown to the target facility commander.

(3) HoIS are known to collect data, including personalia, character traits, weaknesses and possible motivating points on USASA personnel wherever they can be located for possible use at a later date when the individual may be assigned to a location or headquarters facility affording a high degree of access to sensitive information.

(4) Headquarters, USASA, Arlington Hall, Virginia has expressed amenability to use of ASA personnel by elements of the 66th MI Group for purposes of counterintelligence support to USASAE.

Page 2288 of 3957

~~CONFIDENTIAL~~

(5) Reference c provided information concerning the scheduled automation of the target and the subsequent withdrawal of all but five to ten maintenance personnel and security guards. The construction and equipment installation was originally scheduled to be completed and the automated site operational by 1 July 1975, with a possible additional delay of 60 days beyond that date.

b. Concept:

(1) The cultivation and use of overt liaison contacts and the spotting, assessing and recruiting of non-ASA assigned personnel in the target area will continue in effect and be expanded as necessary and require no prior approval under this Plan. Recruitment and utilization of any ASA-assigned personnel as CRS will be initiated on approval of this Plan. No CRS will be recruited under this Plan prior to the completion of appropriate name traces, to include the USAIRR.

(2) Two separate and distinct methods of spotting, assessing and recruiting of CRS will be employed simultaneously, as follows:

(a) The PLO will spot and assess potential sources assigned to the target during visits to the target described in paragraph 3a(2), above. The PLO will pass potential lead information to the PCO, and will continue to furnish any additional available information concerning the individual or his status, as determined. Appropriate name traces and agency checks will be conducted on target members prior to contact by the PLO. Additional checks deemed desirable on target personnel by the PLO will be initiated by the PLO. The PCO will prepare LDR on each potential CRS and on approval will arrange to meet the potential source away from the target area, using an appropriate guise, for further assessment and possible recruitment. All subsequent meetings between the [illegible] and the PCO will be conducted under secure, covert conditions and will be away from the target area.

(b) Coordination with and arrangement for S-2, USASAFSA, assistance in screening records of newly arrived personnel scheduled for assignment to the target, in order to identify those individuals of possible interest; to have selected individuals available for assessment by representatives of the 511th MI Battalion or other elements of the66th MI Group, prior to their assignment to the target; and to assist in necessary personnel actions to delay or reassign selected individuals in order that source coverage of the target can be effected. It time permits, sources recruited in this manner prior to actual arrival at the target will be given initial training and briefing concerning security implications, and arrange for bonafides and meeting arrangements with the PCO at a later date.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Operations Plan, DO3130-079-75

c. CRS Activities in the Target Area: CRS will perform their normal military duties while covertly and discreetly attempting to answer the following EEI, both from on-duty contacts and experience and from off-duty associates:

(1) Identification of target personnel who closely and continuously associate with foreign nationals having connection with Communist countries of the world.

(2) Identification of target personnel who perform authorized or unauthorized travel to Communist countries of the world, including those who may travel after they are released from active duty.

(3) Detection of disaffected target personnel.

(4) Detection of target personnel whose activities and/or character weaknesses render them vulnerable to blackmail or HoIS exploitation.

(5) Detection of target personnel whose activities are indicative of potential defection or desertion.

(6) Detection of personnel who have memberships in or associates with members of organizations, clubs, groups or activities which pose actual or potential threats to the security of the target activity.

d. Security Considerations:

(1) Individuals who are approached for recruitment who decline to function as CRS will be asked to sign security statements which clearly state that it is unlawful to make any unauthorized disclosure concerning the recruitment approach or the activity under this Plan.

(2) Individuals who are approached for recruitment prior to their arrival at the target, and who decline to function as CRS, will be considered for assignment to some location other than the target, if circumstances and military priorities permit.

(3) No CRS nor potential CRS will be made aware of the source relationship with any other individual in this operation.

(4) All CRS will be met under covert conditions, away from the target area; under conditions that will provide maximum security against inadvertent disclosure of the source relationship.

(5) Separate and plausible cover stories for status and for action will be prepared with each CRS to provide a logical reason for regular meetings between CRS and the PCO.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2290 of 3957

(6) Each CRS will be provided sufficient training in security and meeting arrangements so as to minimize possibilities of compromise of the source relationship.

(7) In the event of compromise of a CRS and/or the nature of this operation, termination of the source will follow under such conditions ns are warranted by the circumstances of the compromise. In the event of a compromise, denial of USAI involvement will be achieved where plausible.

(8) Under no circumstances will the command element at the target activity be made aware of the existence of this operation or of the source relationship between any CRS and the PCO.

(9) Local National Investigators (LNI) employed by the 66th MI Group will not be made aware of the existence of this Plan, nor of the source relationship with any CRS.

(10) Knowledgeability of this Plan, to include the identity of the target, will be kept to a strict minimum, and only those individuals with a strict "need to know" will be made cognizant. A knowledgeability roster of all persons with knowledge of this operation will be maintained.

(11) Under no circumstances will the PLO reveal USAI recruitment interest to any target personnel, nor will he offer any recruitment assistance to any prospective CRS.

e. Production:

(1) The Commander, USASAFS Augsburg will be informed of all credible information developed within the target, except as indicated in (2) and (3), below.

(2) Suitability information will be evaluated in light of the tenor of information and the status of the individual to whom it pertains, and if considered of major importance or of significance to this operation, will be forwarded by Agent Report to the Commander, 66th MI Group, ATTN: AEUMI-T-CE.

(3) Information pertaining to or identifying overt or covert sources will not normally be passed as individual items to the supported command without specific DCSI USAREUR approval.

(4) Commander, 511th MI Battalion will submit to the Commander, 66th MI Group, ATTN: AEUMI-T-CE, a Quarterly Status Report containing a summary of the operational progress and source activity covered in this Plan.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

Operations Plan, EO3133-079-75

(5) Periodic briefings of the Commander, USASAFS Augsburg concerning the operational highlights and progress of the program will be conducted by designated personnel from Headquarters, 66th MI Group.

5. (C) COMMUNICATIONS:

a. b1

b. b1

c. b1

d. b1

6. (C) TRAINING: b1

a. b1

b. b1

CONFIDENTIAL

c. b1

d. b1

e. b1

f. b1

7. (C) FINANCE AND LOGISTICS:

a. Finance:

(1) b1

(2) b1

(3) b1

(4) b1

(5) b1

(6) b1

b. Logistics: No special logistics or equipment requirements are foreseen at this time. If such requirements arise, an appropriate Annex to this Plan will be submitted for approval.

8. (U) TERMINATION:

a. The duration of this Plan will be for an indefinite period, or until such time that it is determined that the sensitivity of the target

CONFIDENTIAL

800 [redacted]

CONFIDENTIAL

and/or the drawdown of assigned personnel at the target no longer warrants continuation of the operation.

b. Termination of CRS will be in accordance with current source regulations.

9. COORDINATION:

a. This Plan will be coordinated with Chief, Special Operations Detachment, 66th MI Group prior to coordination with Commander, USASAFS Augsburg.

b. This Plan will be coordinated with Commander, USASAFS Augsburg prior to submission to DCSI, USAREUR and Headquarters, USASA for concurrence.

c. Coordination of this Plan with Headquarters, USASA will be accomplished by the US Army Intelligence Agency, Fort Meade, Maryland prior to final approval for implementation of this Plan by DCSI, USAREUR.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

801

CONFIDENTIAL

OPLAN 1-75, Subject: ICIP (U)
ANNEX A - FINANCE

1. (C) 4th Qtr - FY 75

a. b1

b. b1

c. b1

d. b1

e. b1

2. (C) FY 76

a. b1

b. b1

c. b1

CONFIDENTIAL

d. b1

3. ~~(C)~~ Additionally, the following will apply:

a. b1

b. b1

803

~~CONFIDENTIAL~~

DAMI-DOH

Internal Counterintelligence Program (ICIP) (U)

20 February 1976

1. (U) Purpose: To acquire ACSI approval of OPLAN for ICIP CARELESS TOKEN (U) by signature on approving correspondence.

2. (U) Facts Bearing on the Case: (U)

a. (C) From correspondence between USAINTA and DCSI, USAREUR, it was learned that the 66th MI Group was providing ICIP support to Detachment N, US Army Security Agency Field Station, Augsburg, FRG. The support had been requested by the Commander, USASA Field Station, Augsburg and approved by DCSI, USAREUR and the Commander, USASA, Arlington Hall, VA.

b. (U) In an exchange of messages with DCSI, USAREUR, DAMI-DOH advised the DCSI of the existing policy pertaining to ICIP's in CONUS and the requirement to furnish quarterly reports to the Under Secretary of the Army. In light of the ACSI's policy to personally review all new ICIP's, DCSI, USAREUR decided to forward the OPLAN for ICIP CARELESS TOKEN (U) for ACSI review. The operation is already ongoing and approved by appropriate USAREUR and USASA officials.

2. (U) DISCUSSION: (U)

a. (C) The OPLAN for ICIP CARELESS TOKEN (U) is designed to detect and counter vulnerability to espionage by USASA personnel assigned to an isolated USASA detachment in the vicinity of the FRG/CSSR border. Standard ICIP procedures have been employed using recruited sources, a Project Liaison Officer and a Project Control Officer.

b. (U) By separate action, a policy letter to all Army Intelligence commands will be prepared to assure that ICIP policy is established and reporting requirements to the Under Secretary are met.

3. (U) RECOMMENDATION: That the 5th Indorsement approving the OPLAN at TAB A be signed by the ACSI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

LTC Ehendle/56159

804

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DAMI-DOH (30 Jun 75) 5th Ind
SUBJECT: Internal Counterintelligence Program (ICIP) (U)

5 FEB 1976

HQDA, Office of the Assistant Chief of Staff for Intelligence, The Pentagon, Washington, DC 20310

TO: Commander, US Army Europe and Seventh Army, ATTN: DCSI, APO New York 09403

1. (C) Continuation of your ICIP CARELESS TOKEN (U) under the May 1975 Operations Plan earlier approved at your Headquarters in support of US Army Security Agency, Field Station, Augsburg, is approved.

2. (U) As indicated in earlier correspondence, a Memorandum to the Under Secretary of the Army is prepared quarterly by the Office of the Assistant Chief of Staff for Intelligence, DA Staff which includes a brief summary of developments and status of each ongoing ICIP. Field input is requested by the 15th of the month following the end of each calendar year quarter.

HAROLD [illegible]
Major General, GS
ACofS for Intelligence

1 Incl
nc

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

805

Classified by ACSI, DA
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 2006

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY, EUROPE and SEVENTH ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, INTELLIGENCE
APO 09403

3 FEB 1976

AEAGB-CI(SO)

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

HQDA (DAMI-DOH)
WASH DC 20310

1. (U) References:

a. Operations Plan, 66th MI Group, 5 May 1975, subject as above (C).

b. Message, DAMI-DOH, DA, 032115Z December 1975, subject as above (C).

c. Message, AEAGB-CI(SO), USAREUR, 061755Z January 1976, subject as above (S).

2. (U) Attached are two Quarterly Status Reports pertaining to the Internal Counterintelligence Program (ICIP) CARELESS TOKEN in support of Detachment N, US Army Security Agency, Field Station Augsburg. Copies have been provided the S2 of the support unit.

3. (U) ODCSI, USAREUR, Action Officer is Mr David R. Smith, AEAGB-CI(SO), HM 7354 (AUTOSEVOCOM 6742).

FOR THE DEPUTY CHIEF OF STAFF, INTELLIGENCE:

2 Incl
as

A. J. IADEROSA
Colonel, GS
Chief, Counterintelligence Division

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CLASSIFIED BY DAMI-DOH
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF E.O. 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 2006

~~CONFIDENTIAL~~

806

~~CONFIDENTIAL~~

16 FEB 1976

AEAGB-CI(SO)

SUBJECT: Internal Counterintelligence Program (ICIP) (U)

HQDA (DAMI-DOH)
WASH DC 20310

1. (U) References:

a. Operations Plan, 66th MI Group, 5 May 1975, subject as above (C).

b. Message, DAMI-DOH, DA, 032115Z December 1975, subject as above (C).

c. Message, AEAGB-CI(SO), USAREUR, 061755Z January 1976, subject as above (S).

2. (U) Attached are two Quarterly Status Reports pertaining to the Internal Counterintelligence Program (ICIP) CARELESS TOKEN in support of Detachment N, US Army Security Agency, Field Station Augsburg. Copies have been provided the S2 of the support unit.

3. (U) ODCSI, USAREUR, Action Officer is Mr David R. Smith, AEAGB-CI(SO), HM 7354 (AUTOSEVOCOM 6742).

FOR THE DEPUTY CHIEF OF STAFF, INTELLIGENCE:

2 Incl
as

A. J. IADEROSA
Colonel, GS
Chief, Counterintelligence
Division

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

31 DEC 2006

807

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
511TH MILITARY INTELLIGENCE BATTALION
66TH MILITARY INTELLIGENCE GROUP
APO 09696

AEUMI-N-CE
B03130-518-75

24 October 1975

SUBJECT: Internal Counterintelligence Program (ICIP)
(QUARTERLY STATUS REPORT) (QSR)

Commander
66th Military Intelligence Group
ATTN: AEUMI-T-CI (EXCLUSIVE FOR ICIP CONTROL OFFICER)
APO 09108

1. (U) References:

a. OPLAN, 511th MI Battalion, AEUMI-N-CE, 1-75, 1 May 1975

b. AEAGB-CI(SO), DTG 151640Z July 1975, ICIP

2. (U) This is the first ICIP Quarterly Status Report, in accordance with references, covering the period ending 15 October 1975.

3. General:

a. Activity at the target is in the drawdown stage, pending automation in early 1976 under the LA FAIRE VITE Program. Since 1 July 1975, personnel manning has been reduced to about 50 percent of previous target strength; most personnel have been reassigned to USASAFS Augsburg. In June 1975, an official release was made by letter to the Buergermeister (mayor) of Rimbach, which provided details of the withdrawal. Portions of the letter were reportedly published in area newspapers. A copy of the English translation of the letter to the mayor's office is attached as Inclosure 1.

b. Contrary to the letter inclosure, it appears that some target personnel in excess of the programmed approximately seven (7) individuals who will maintain and guard the automated site, may remain in the area for varying periods up to 1 July 1976. These include all personnel who

CLASSIFIED BY: [illegible] AR 601-12, 120 ci 74
EXEMPT FROM [illegible] CLASSIFICATION
SCHEDULE [illegible] ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY UPON NOTIFICATION OF ACSI, DA

808

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

AEUMI-N-CE 24 October 1975
SUBJECT: Internal Counterintelligence Program (ICIP)

are scheduled for DEROS or ETS in FY76 as funding is not available for two PCS moves in a single fiscal year. No figures were available at the time of the QSR preparation as to how many personnel would be affected, nor had it been determined what would be their duties during the approximate period 1 March-30 June 1976.

c. The USAF communications site (6913th USAF Security Squadron) located in the same area is scheduled to close at about the same time the target is automated; no USAF personnel will remain in the area. As far as can be determined, the French and Bundeswehr sites will continue to operate.

d. The seven or eight personnel scheduled to remain at the target permanently will be billeted at the top of Mount Hoherbogen, in a newly constructed building, adjacent to the present operational area. The senior individual will be an NCO, grade E6 or E7, who will probably have one of the supervisory communications equipment maintenance MOS's. Other personnel stationed there will be equipment and antenna array repair and maintenance specialists and guards. All personnel will be single or unaccompanied. At the writing of this report, none of the permanent party had been selected.

4. Operational Matters:

a. SMLM-F makes a reconnaissance of the Rimbach area approximately once a month. The sightings usually involve travel along the PRA perimeter roading leading north and south out of Rimbach. Perimeter roads of PRAs, excluding Autobahnen, are off limits to SMLM-F vehicles. On 3 June 1974, a SMLM-F vehicle was disabled on the access road leading to the target operational site, well within a PRA, and was assisted by a Chief Warrant Officer assigned to the target, who was not aware of the correct PRA boundary. There have been no SMLM-F detentions in the area, and none are likely, since the closest Military Police are located at Hohenfels Training Area (HTA), 80 kilometers away.

b. In March 1975, during a liaison visit with MAJ Richard Douma, the target commander, the PLO was advised that b6 b6 had been transferred to Ramstein, FRG after appearing before a board to face charges of homosexuality.

c. In April 1975, SP4 b6 reported a possible SAEDA incident (Group Case 75-061P); during the subsequent investigation it was determined she had reported to Field Office Augsburg a similar approach by the same individual a year earlier. Target personnel were dubious as to the veracity of statements made by b6 who was transferred to USASAFS, Augsburg on 1 August 1975.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

809

~~CONFIDENTIAL~~

[redacted]

AEUMI-N-CE 24 October 1975
SUBJECT: Internal Counterintelligence Program (ICIP)

d. In May 1975, MAJ Douma advised the PLO that some of the target personnel had a tendency to talk too openly about their jobs in public, and that his solution had been constant reiteration to unit personnel on the dangers of loose talk. No specifics were provided on individuals concerned. The PLO did not press for details as he considered it a command matter. MAJ Douma believed the security posture of the target was steadily improving.

e. The preliminary investigation of b6 continued, however, in low key due to the lack of credible specific allegations. b6 operates the Hoherbogen Restaurant, situated near the target administrative area. He allegedly travels regularly to CSSR to visit relatives and to attend dog shows. Target personnel patronize the restaurant regularly, primarily because of its convenient location. b6 was never reliably reported to have shown undue curiosity about target operations and personalities, but remains, nevertheless, well-informed because of overheard conversations of target personnel-customers. In June 1975, b6 told the PLO he was not looking forward to the departure of the Americans because he would have to "put up" with local German customers, who were much more troublesome than target personnel. In October 1975, b6 remarked to MAJ Douma that he had made several trips to Augsburg to negotiate the purchase of a tavern there. b6 said he intended to sell the Hoherbogen Restaurant and move to Augsburg, where he will open a tavern/restaurant two kilometers from the "ASA kaserne." Activity of b6 will continue to be monitored in the Rimbach area, and if he moves to Augsburg, he should be made a target of continuing interest by Field Office Augsburg.

f. In July 1975, CPT (Chap) b6 Protestant Chaplain at HTA, advised that an individual assigned to the target had sought his spiritual guidance as a result of extreme emotional anxiety, due to his/her involvement with a group of USASA personnel who were engaged in satanic religious practices at the target. b6 revealed no details nor identities, due to the sensitivity of communications to a chaplain, however, the identity of the individual involved is believed to have been established (see para 4j, below).

g. In July 1975, two target personnel applied for Military Intelligence duties in ACGP-97. One (SP5 b6) was assisted in completion of required forms and processing/interview is in progress. The other individual (SP4 b6) will not be able to apply until December 1975, when he has 12 months remaining to DEROS. He expects to be transferred to USASAFS, Augsburg prior to that time and has been advised to initiate his processing at Field Office Augsburg.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

810

[redacted]

[redacted]

AEUMI-N-CE 24 October 1975
SUBJECT: Internal Counterintelligence Program (ICIP)

h. In July 1975, USASAFS, Augsburg requested agency checks on the German national intended spouse and relatives of SP4 b6 Subsequently, during a subject interview, b6 stated that his fiancee had contact, through an acquaintance, with b6 a photographer/ reporter for a Furth-im-Wald newspaper and that he suspected b6 was receiving money from the CSSR for photographs of facilities in the Rimbach area. b6 had no specific reason to back up his suspicion and said it was common knowledge among target personnel. b6 was the subject of a bilateral MI/MAD investigation in 1973 and 1974, during which none of the allegations of possible intelligence activity were substantiated.) b6 also said he personally was suspicious of fnu b6 a former member of the target unit, who operates "b6 Club" in Koetzting. b6 is curious as to the status of US installations at Rimbach and uses his US citizenship and former Army service as a method of gaining access to information from US Forces members who patronize his establishment. b6 and his activity was previously known to MI/MAD during the b6 investigation and not determined to warrant further investigation. b6 is a non-DoD affiliated US citizen.)

i. In July 1975, USASAE, Augsburg requested agency checks in Koetzting on b6 and b6, who were friendly with target personnel and who had become knowledgeable of classified defense information as a result of this relationship. There was no indication any of the b6 had attempted to elicit defense information. Agency checks failed to reveal any derogatory information concerning the b6 family; b6 was a practicing dentist in Koetzting. In early August 1975, MAJ Douma advised the PLO that in early 1975, SP4 b6 and her dependent husband, b6 a US citizen, had attempted to establish a German-American Club between target personnel and the local communities. In this connection, the b6 mentioned being acquainted with a dentist in Koetzting, nfi. Nothing of consequence ever came of the attempt to form an organization. Later, date unknown, Douma was advised by Commander, Forward Operations Battalion, Augsburg (his supervisor) of a report that b6 had discussed classified information with German acquaintances. In an interview of b6 by Douma, she admitted having discussed details of LA FAIRE VITE with her husband in early 1975, and to have mentioned the project in the presence of one b6 a German national acquaintance residing in Munich. b6 was subsequently given a written reprimand in connection with the compromise. b6 mentioned nothing about any other German acquaintances, and denied compromising any classified information to any other foreign nationals. No information was made available to Douma when he was tasked by his higher headquarters to investigate the incident, as to the identity of the German acquaintances who were supposed to have received the classified defense information. b6 departed the target on 19 July 1975 for CONUS and separation from active duty.

811

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

~~CONFIDENTIAL~~

AEUMI-N-CE 24 October 1975
SUBJECT: Internal Counterintelligence Program (ICIP)

j. In August 1975, MAJ Douma advised the PLO that SP4 b6 attached to the target from the 502d ASA Group as a Czech linguist Voice Intercept Specialist (98G2LCX), had exhibited severe mental trauma immediately following the departure of a close female acquaintance from the target on 30 June 1975, and had been placed on extended leave status. b6 consulted CPT (Chap) b6 at HTA and the USASAFS Augsburg staff chaplain, but had allegedly declined psychiatric counselling. On her return from leave, her access to classified material was to be suspended and Douma could direct b6 to receive counselling, as he was very concerned about her emotional stability. b6 had a DEROS of September 1975.

k. In August 1975, the PLO advised MAJ Douma that a German agency had reported a US soldier named b6 was trafficking in drugs in Koetzting. After the PLO provided descriptive data obtained from a FRG agency, Douma identified b6 as SP4 b6 a Russian-linguist Voice Intercept Specialist, attached from the 502d ASA Group. Douma was requested to watch b6 activities closely and pass any information to CID at HTA. b6 DEROS is June 1976, putting him in the category of those mentioned in paragraph 3b, above, who may remain at the target without any specific duties.

l. In September 1975, B58,786 (who is undergoing preliminary source assessment) advised that in approximately April 1975, a female soldier traffic analyst assigned to the target, whose name he could not recall, had compromised a TOP SECRET/CRITIC/CODEWORD message to b6, a dependent and GS-2 clerk typist in the unit administrative office. b6 had only a Confidential clearance. The compromise although known by the target commander, was not reported to USASAFS, Augsburg.

m. No specific information has been reported to indicate that Hostile Intelligence agencies are in contact with any target personnel.

5. (U) Source Activity:

a. One potential source (B58,786), has been spotted at the target and is being assessed. Name traces are not yet complete. He is scheduled for reassignment to USASAFS, Augsburg on approximately 15 December 1975. In accordance with paragraph 3b of reference a, a Lead Development Report is being prepared and will be forwarded separately, recommending his possible utilization as a defensive installation source in Augsburg.

b. The lack of identification of any personnel who will make up the permanent party at the target has inhibited any meaningful spotting/assessing activity to date.

REGRADED UNCLASSIFIED
SEP -5 1997
ON
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

5 812

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

AEUMI-N-CE 24 October 1975
SUBJECT: Internal Counterintelligence Program (ICIP)

6. (C) Comments:

a. The PLO was indoctrinated for SI on 9 October 1975. Request Special Operations Detachment determine if any more Quarterly Security Inspections are scheduled for target, and arrange for prior notification and coordination so that the PLO may accompany the inspecting team. Any insight gained into security problem areas not evident from routine liaison contacts would be of great value to the PLO in accomplishment of his mission.

b. The PLO has reported that he is unable to pursue a more aggressive approach with the target commander concerning identities of personnel who will remain at the target, without arousing suspicion as to his true motives. Request Special Operations Detachment attempt to identify those individuals as soon as the determination is made.

c. The short period remaining of continued operations at the target raises the question as to whether the project would be justified at that location in the long term. As presently visualized, according to available information, any source recruited at the target would be primarily reporting on six or seven other personnel, with whom he is living in a very close, restrictive environment. It can be expected the majority of the information reported will be of an adverse suitability nature. Further, it can be expected that with target automation, Hostile Intelligence efforts at the target will take a lower priority inasmuch as product expolitation through the human exploitable factor will no longer be present. The Commander, USASAFS, Augsburg raised some of these points when reference a was staffed through his office.

1 Incl
as

FADLO M. MASSABNI
LTC, MI
Commanding

Tel: Nbg Mil (2621)-6446/Foss

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

6 813

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
SEVENTH ARMY TRAINING CENTER MILITARY COMMUNITY
OFFICE OF THE INSTALLATION COORDINATOR, RIMBACH
APO New York 09173

IAEaCF-B

5 June 1975

Herr Burgermeister Bachl
Community of Rimbach

1. The purpose of this letter is to advise you, and therefore all Rimbach community officials and businessmen, of a projected change in the US military posture and presence in the community of Rimbach, Mount Hoherbogen, and the surrounding area.

2. The American military community in this area now consists of elements of both the United States Army and the United States Air Force, as well as a significant number of wives and dependent children. The total American population currently is just over three hundred people.

3. Commencing in August 1975, the American community will decrease in size, with the largest majority of our people departing on or about 1 November and 15 December respectively. By 1 March 1976 there will be approximately seven US Army personnel and probably no wives and children remaining in the area. They will live in a US Army owned facility on top of Mount Hoherbogen (on Eckstein Ridge).

4. This transformation is the result of a programmed technical change in the American communications function located in this area.

5. At this time, and with this announcement, please accept my personal gratitude, as well as that of the US Army and the US Air Force, for the understanding and warmth which has been so graciously extended to the American military forces and their families over these many years by you, the Rimbach Community Official Staff, and the entire community of Rimbach. We will do all that we can to insure that the small force remaining continues to appreciate and help maintain the relationship that we have enjoyed.

RICHARD DOUMA
MAJ, MI
Installation Coordinator

814

[redacted]

DEPARTMENT OF THE ARMY
511TH MILITARY INTELLIGENCE BATTALION
66TH MILITARY INTELLIGENCE GROUP
APO 09696

AEUMI-N-CE
B03130-061-76

23 January 1976

SUBJECT: CARELESS TOKEN (U)
(Quarterly Status Report)

WARNING NOTICE: SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED (WNINTEL)

Commander
66th Military Intelligence Group
ATTN: AEUMI-T-CI (EXCLUSIVE FOR ICIP CONTROL OFFICER)
APO 09108

1. (U) References:

a. OPLAN, 511th MI Battalion, AEUMI-N-CE, 1-75, 1 May 1975.

b. AEAGB-CI(SO), DTG 151640Z Jul 75, ICIP.

c. AEUMI-N-CE, B03130-518-75, 24 October 1975, ICIP.

2. (U) This Quarterly Status Report is submitted in accordance with references a and b and covers the period ending 15 January 1976.

3. (U)~~(C)~~ General:

a. Operational activity continues in the drawdown stage, on schedule. The transfer of the first increment of Company B and attached operational personnel to USASAFS Augsburg (USASAFSA) has been completed, reducing the strength on 15 January 1976 to 63 assigned, 22 attached, 3 TDY and 20 dependent wives and children. In addition, 22 personnel will depart the target during January and an additional 34 will depart by mid-February. All Company B personnel will have departed by 31 March. During the latter part of February and March 1976, Company B personnel will shut down the present operations, service and prepare equipment for shipment and perform general repair and utility duties relating to present operations. Action by USASAFSA to move all Company B personnel when essential duties are completed has alleviated a potential problem of having sensitive personnel remaining in the area with much free time. The final day of operation of the snack bar was to be 17 January, and the small PX and commissary annexes are to close by mid-February. With these closures, the closest shopping facilities are in Regensburg, Hohenfels and Grafenwoehr.

REGRADED UNCLASSIFIED
ON 5 SEP 1997
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

815

[redacted]

CLASSIFIED BY: Para 4h, AR 381-12, 180ct74
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE [illegible] EO 11652
EXEMPT [illegible] 2
DECLASSIFY ON: DETERMINATION OF ACSI, DA

~~CONFIDENTIAL~~

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

23 January 1976

b. Due to the shortage of PCS funds and DA reassignment restrictions, USASAFSA offered curtailment or extension options to those personnel scheduled for discharge or separation prior to 31 March 1976. Many chose curtailment, and some of those requested European separations. Identities of those to be separated in USAREUR have not been determined, pending approval of the requests.

c. Eight dismounted vans remain at the target and the Seventh Army Training Center (SATC) Engineer Office, Grafenwoehr (QA0911) has announced bids for their removal or destruction. The vans represent a total present value of $40,000 to the US Government and Property Disposal officials are reluctant to destroy the vans as they have a high resale value in Europe. It is expected that in the near future a contractor will have personnel at the target, either removing or dismantling the vans.

d. All of the LA FAIRE VITE (LFV) personnel have arrived at the target. The NCOIC is SFC [b6] All team members are assigned to the Supply and Maintenance Company (SMC), Support Battalion, USASAFSA. [b6] is a Cryptographic Equipment Repair Supervisor (MOS 32G), has over 13 years service with USASA, is married (no children) and resides with his wife, [b6] nee: [b6] US citizen, at [b6] [b6] is 35 years old, a native of Colorado and expects to remain at the target until his normal DEROS in November 1978. [b6] mother is a naturalized US citizen, born in Germany; her father is employed as a Systems Engineer at American Forces Network (AFN), Frankfurt (MA7749). [b6] appears to be highly proficient and has exhibited a positive attitude toward his assignment. PLO contacts to date have indicated Helus will be cooperative and receptive to MI support and contact. On the most recent visit to the target (15 January 1976), [b6] was reportedly on TDY attending an unidentified training course at USASAFSA. He is scheduled to return to the target by mid-February 1976.

e. Other members of the LFV team are identified as follows:

(1) SP5 Terry P. Pack, [b6] DEROS February 1978

(2) SP5 [b6] DEROS/ETS April 1978

(3) SP4 [b6] DEROS/ETS February 1977

(4) SP4 [b6] DEROS/ETS April 1978

(5) SP4 [b6] DEROS/ETS April 1978

(6) SP4 [b6]

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

[redacted]

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

23 January 1976

f. The team began on-site training on 13 December 1975. All of the personnel in paragraph 3e above, are Intercept Receiving System Repairmen (MOS 33C) or Intercept Recording System Repairmen (MOS 33D). All are single or unaccompanied; none admitted to having any girl friends living in the target area, or any that they intended to have move into the area. In general, the LFV team members appear to be security conscious. They have been at the target long enough to become familiar with some of the USASA "haunts" (Hoherbogen Restaurant in Rimbach (UQ4553) and the Ratskeller and Ambergerhof Restaurants in Furth-im-Wald (UQ4364)), and have been eager to acquire information on places of intelligence interest or with a bad reputation.

g. The target has a German shepard dog, "Sam" which is partially attack-trained and does not react well to strangers, females and blond males (SP5 Pack has particular difficulty in getting close to the dog). "Sam" reportedly was beaten and generally mistreated by previous owners, and his attack training has given him just enough knowledge to be dangerous.

h. Electrical power at the target will continue to be provided by the Pilsen Power Grid. Once activated, the site will have a 22 Kilovolt self-regulating generator with a 14-day gasoline supply for backup/emergency use. Water must be trucked to the site and sewage removed from a holding tank. Both water and sewage tanks are planned for 14-day capacity. A German firm, as yet unidentified, from Brueck (UQ0458) has contracted to service the holding tank and to truck in water from the Rimbach public water works. Emergency fire service will be provided by the Neukirchen-Heilig Blut (UQ5258) Volunteer Fire Department, 15 kilometers away, with an unknown reaction time. Medical assistance will be provided by the German civilian hospital in Koetzting (UQ4349); air evacuation by helicopter is possible through the MEDIVAC capability at SATC, Grafenwoehr. APO mail will be addressed to Post Office boxes at USASAFSA, will be re-packaged and sent through German mail channels to: Remote Site LFV, SFC [b6] 8491 Rimbach. [b6] will pick up mail daily from the Rimbach post office.

i. The site will have three communications channels:

(1) Direct AUTOSEVOCOM to USASAFSA Control Center

(2) Non-Secure "order wire" to USASAFSA Control Center

(3) German commercial phone (Class B) (09947-302) through the Neukirchen-Heilig Blut exchange.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

817

[redacted]

~~CONFIDENTIAL~~

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

23 January 1976

j. Target personnel will live in the "Chateau" located adjacent to the Operations Building. The newly constructed "Chateau" consists of a common area: living room, kitchen and recreation facilities, with couches, television, stereo and a pool table; and adjacent sleeping quarters. Personnel will be allowed guests in the common area. The Commander, SMC has advised b6 he may hire a local cook if the team members agree. b6 would like to hire his wife for this activity, as she will otherwise be unemployed. This solution appears to have a distinct advantage over hiring a local area national.

k. Two team members will be on duty at the site, 24 hours a day. Present plans call for the issue of .45 caliber pistols and ammunition, but it has not yet been determined where the weapons and ammunition will be stored. In the event of attempted penetrations of the area, personnel have been instructed to lock all entrances and remain inside the building. b6 has been advised that elements of the 3d Squadron, 2d Armored Cavalry Regiment (2ACR) at Camp May, Regen (UQ6326), 43 kilometers, may have a reaction capability, reaction time unknown. 2ACR elements patrol the CSSR border area near the site and may be capable of a short reaction time. Joint defense plans have been discussed with two other military units in the same immediate area, Fernmeldesektor F of the FRG Armed Forces and Detachment D of the French Forces. Both counterparts appeared eager to form joint defense plans, but the non-NATO status of the French precluded USASA from negotiating at the local level. The problem reportedly was identified to USASAFSA. Each member of the team will have one key to the entrance gate which will be kept locked at all times after the German contractor personnel have departed the site. The operations building, a SI-area, is equipped with heat and sound-sensitive alarm systems and alarms also sound in the event of power loss or equipment malfunction. The German contractor engaged in construction work at the site will remove approximately 1.5 meters of rock from the end of the ridge near the tower to enlarge the antenna scanning area. This work cannot be completed during the winter months and is expected to be finished by May 1976. Explosives cannot be used due to the sensitivity of installed equipment in the immediate area.

l. On 15 January 1976, the PLO met the LFV Project Officer from the USASA Systems Agency, Vint Hill Farms, Warrenton, Virginia, who was visiting the target. He explained that the following relay towers in the LFV system are unmanned by USASA personnel:

Seibersdorf	TQ97624600
Landshut	TP94688240
Bonstetten	PU26906739
Dachau	PU80735466
Wasserkuppe*	NA66489456
Wildflecken*	NA56258478
Brandhof**	PV26258873

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

8 / 8

~~CONFIDENTIAL~~

[redacted]

AEUMI-N-CE 23 January 1976
SUBJECT: CARELESS TOKEN (U)

Heidenheim**	PV28953095
Schwanberg**	NA91890879

*Army location occupied by non-USASA personnel

** USAF installation

The present SOP gives little information on the remote towers as far as security is concerned. In general, the remote towers are tall antennas with small buildings at the base. Each building has a door that is supposed to be kept locked. If someone enters one of the buildings an alarm light goes on in the central control area at USASAFSA. Telephones with open speakers are located in each building, so that if the alarm lights go on in the central area, duty personnel can pick up a phone and ask who is there. Arrangements have reportedly been made with local police, details unknown, to keep a close watch on all the remote towers, but the Project Officer was unaware what action the police were to take concerning trespassers. Anyone gaining access to the building at a remote tower could, with the proper equipment, tap the open service line and the scrambled traffic lines. While tapping the traffic lines would yield nothing but meaningless letter/number groups, they might have some value to a Hostile Intelligence Service. The isolation of several of the remote towers makes them susceptible to sabotage as the loss of a tower in the relay system renders that segment of the system useless.

4. (C) Operational Matters:

a. Reference paragraph 3j, above: USASA has not planned any electronic sweep of the SI area or the common room now that the German contractor has completed installation of the wiring. b6 asked if the PLO could arrange for an electronic sweep of the entire area as future visitors may want to use the common area for conferences. The PLO was non-committal and no action will be taken unless a formal request is received.

b. Reference paragraph 4g of reference c: On 8 December 1975, the First Sergeant of Company B advised that SP5 b6 was no longer interested in ACGP-97 duties and that his application papers should be destroyed. SP4 b6 the other individual interested in ACGP-97 will remain at the target until February 1976 and his application is being processed with PLO assistance.

c. Reference paragraph 4e, reference c: b6 is moving to Augsburg on about 1 February 1976 and will be operating the Cafe-Restaurant "Sonne", 9 Hauptstrasse, Augsburg-Bergheim (PU3554), telephone: 97524. b6 has passed out the name and address of his new establishment to target

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

Page 2312 of 3957

[redacted]

AEUMI-N-CE 23 January 1976
SUBJECT: CARELESS TOKEN (U)

personnel who are moving to Augsburg, and he has been actively soliciting their future patronage. There have been no indications that b6 has attempted to elicit information from target personnel, however his proximity to the target and the regular customers from the target at his establishment, the Hoherbogen Restaurant, have resulted in him being well-informed about ongoing transfers, the drawdown and future operations in the target area. All members of the LFV team are aware of MI interest in b6 It is expected that the Hoherbogen Restaurant will be leased by another party and remain open. No information is presently available on the new lessee.

d. Reference paragraphs 4f and 4j, reference c, the information provided is clarified as follows: SP4 b6 formerly attached to the target from the 502d ASA Group, contacted the Army Chaplain at the Hohenfels Training Area (HTA) for spiritual guidance when she became depressed after developing a strong emotional attachment to another female soldier who had departed the target. b6 was counselled and subsequently reassigned to USASAFSA. b6 had nothing to do with the "satanic religious practices" referenced in paragraph 4f, reference c. That matter was not known to involve any target personnel and all personnel known to be involved with alleged "satanic religious practices" are assigned or attached to the 207th ASA Company, HTA and discussion of the incident is not germane to this report.

e. Reference paragraph 4k, reference c: SP4 b6, due to be transferred to USASAFSA is considered by his supervisors to be a potential troublemaker in the organization. He has been behaving strangely, which may be attributable to injuries he received in a 1974 motorcycle accident. b6 was reprimanded by the Company B Commander for signing a guard property receipt with the name "Mickey F--King Mouse." He has also been involved in a questionable transaction with a German national involving a motorcycle.

f. Target personnel reported no SMLM activity in the area since approximately September 1975. The PLO will recommend that the nearby German Army unit advise target personnel whenever a SMLM vehicle is reported in the area. It is known that German Military Counterintelligence (MAD) advises Fernmeldesektor F whenever a SMLM vehicle is reported in the area. The PLO will provide assistance to the LFV team in formulating a SMLM SOP. One team member had no SMLM card and none of the team members contacted on 15 January 1976 were certain of what action to take if a SMLM vehicle was sighted in the target area. None of those individuals could recall having received a meaningful SMLM briefing since arriving in USAREUR.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

820

[redacted]

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

23 January 1976

g. The PLO gave a short SAEDA briefing to LFV team members (less b6) on 15 January 1976 and requested their cooperation in identifying risk spots, suspicious incidents, undue curiosity and other SAEDA-related matters.

h. In October or November 1975, date unknown, an individual was sighted measuring the perimeter fence of the target from the outside. He was challenged and he rapidly retreated into the wooded area and could not be located. The incident was allegedly reported to USASAFSA and it was later concluded that the individual probably was a Bundespost (German Post Office) employee, since a Bundespost truck had been seen near the site that day, and the matter was considered settled. The incident was not reported to MI when it occurred, and only became known on 15 January 1976 during casual conversation. It was emphasized to LFV team members that available MI support can only be effective if all incidents, however minor, are reported in a timely manner. In the above instance, it was not determined how the unidentified individual was concluded to be a Post Office employee, but in any event, it appeared from information available that the activities as described were suspicious and warranted further investigation.

i. On 16 November 1975, two ranking representatives of the CSSR firm SEMEX, a subsidiary of the state-owned auto manufacturing firm SKODA visited the SEMEX offices in Furth-im-Wald concerning a planned program to import CSSR tractors into the FRG via SEMEX. Despite the fact that their business was in Furth-im-Wald and there was an abundance of hotel rooms in that town, the two individuals made reservations at the Hotel Kolmerhof in Rimbach for the night of 16-17 November. They departed for Munich (PU9135), FRG the following day. Nothing of a suspicious nature was noted during the visit, but represertatives from SEMEX have been identified in the past engaged in low-level intelligence activity on behalf of the CSSR Intelligence Service. On 25 November 1975, inquiries at the target revealed that no unit personnel regularly patronized the Kolmerhof Hotel, although it was located directly across the street from the Company B administrative area, because of its higher prices and it catered to a clientele able to spend more money than most target members. On occasion, the hotel did hold dances and some target personnel had been known to attend.

j. On 13 December 1975, SSG b6 Company B, was reported as missing after spending an evening drinking at a tavern in Voggendorf (UQ4453). Unit personnel, assisted by local police, searched the area thoroughly and he was finally found the following day after having reportedly spend the night in the quarters of a female member of the unit. The incident was reported to MI by the target in a timely manner and close coordination was maintained with unit supervisory personnel, Military Police, and the local police during the search action.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2314 of 3957

~~CONFIDENTIAL~~

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

23 January 1976

5. (C) Source Activity:

a. B58,786 advised that the behavior of b6 (paragraph 4e, above) had deteriorated, possibly due to physical problems arising from his 1974 motorcycle accident. In the accident, b6 was gored by a wire fence and his neck was heavily scarred despite several plastic surgery operations. Some spinal damage also occurred and b6 was on medication and frequently complained of headaches. He could not concentrate, argued with supervisors and had developed a short attention span. Lead questioned b6 suitability for continued assignment to sensitive duties.

b. B58,786 was encouraged to patronize the Hoberbogen Restaurant more often, in order to maintain continuity to the limited investigation, pending b6 intended move to Augsburg. Lead was to determine if b6 acted in a suspicious manner. This activity was designed to assist in the assessment of the Lead's potential. This action was not out of character as Lead patronized the restaurant occasionally and knows b6 Lead was not targetted against b6 nor was MI committed to reimburse Lead for any expenses incurred.

c. Local agency and 201 file checks on LFV team members are being submitted as a separate action. Name traces will be conducted on all team members.

6. (C) Comments:

a. No support is required from Special Operations Detachment, except for a portion of the actions outlined in paragraph 5c, above (to be submitted).

b. Reference paragraph 3b, above, if members of Company B obtain European separations, whether or not they remain in the target area, they could pose a similar situation to that which occurred in July 1974 when a former member of Company B, who had a post-separation travel restriction, travelled to CSSR within a few days after his European separation. The PLO will arrange with Commander, Company B for SAEDA briefings and appropriate warnings on travel restrictions to all target personnel receiving European separations.

c. Reference paragraph 3 1 above, local police having jurisdiction over the areas of the LFV remote towers within the 511th MI Battalion area will be contacted to determine what they have been told about the towers and what measures they are taking pertaining to tower security.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 2315 of 3957

AEUMI-N-CE
SUBJECT: CARELESS TOKEN (U)

23 January 1976

d. That portion of the comments in paragraph 6c, reference c that pertain to the possible limited results of this operation after target automation, remain valid. Considering these limitations, the thrust of the operation will be directed at developing threat information directed against the target and target personnel.

for Adam A. Smith, GS-13
FADLO M. MASSABNI
LTC, MI
Commanding

Tel: Nbg Mil (2621)-7165/Foss

REGRADED UNCLASSIFIED
ON SEP 15 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2316 of 3957

DAMI-DOH
Cdr, USAINTA
ATTN: MIIA-SO

ICIP GONDOLA STAR (U)
DAMI-DOH

LTC Haendle/gr/56159

1. Reference DF, this office, subject: Quarter ICIP Reports, dated 17 Dec 75.

2. Attached for your information and appropriate action is a copy of ACSI Form 28 (less tabbed inclosures), dated 14 Jan 76, which reflects ACSI, DA approval for the continuation of ICIP GONDOLA STAR (U) as an ongoing operation.

3. Request the Commander, 902d MI Group inform interested parties at the installation supported by the ICIP of the ACSI's decision to continue the operation.

FOR THE DIRECTOR OF INTELLIGENCE OPERATIONS:

1 Incl
as (CONFIDENTIAL)

L. A. SPIRITO
Colonel, GS
Chief, HUMINT Division

REGRADED UNCLASSIFIED
ON 19 OCT 2006
BY USAINSCOM FOI/PA
Auth Para 4-102 DOD 5200.1R

824

ACTION SHEET

CONTROL NUMBER

SUBJECT: Review of Internal Counterintelligence Program (ICIP) GONDOLA STAR (U)

OFFICE SYMBOL: DAMI-DOH

SUSPENSE:

DATE: 14 Jan 76

ACTION REQUIRED: To obtain ACSI decision for continuation or termination of subject ICIP.

MEMORANDUM FOR RECORD. *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) BACKGROUND: (U)

a. During the last quarter of calendar year 1974, the ACSI directed the termination of 12 of 19 ongoing ICIP operations. The operations terminated were those which were less productive or conducted at installations of lesser sensitivity. Among those terminated was the ICIP GONDOLA STAR at Aberdeen Proving Ground/Edgewood Arsenal, MD. (A subsequent new operation increased the total ongoing ICIPs to eight.)

b. After reviewing correspondence initiated by the Commander, APG and indorsed by the Commander, Test and Evaluation Command and the Commander, Army Materiel Command, which recommended the ICIP GONDOLA STAR be continued, the ACSI reinstated the operation for a period of six months on 11 Jul 75 (TAB B).

c. In a memorandum for the Under Secretary of the Army dated 16 Sep 75, which provided the quarterly ICIP report for the second quarter calendar year 1975 (TAB C), the ACSI reinstated the operation for a period of six months and indicated a final determination would be made in January 1976 as to whether or not the operation should continue.

2. (U) (C) DISCUSSION: (U)

a. (U) At TAB A the Special Assistant to the Commander, USAINTA, provided an analysis of the ICIP GONDOLA STAR covering the period July thru December 1975. He recommended that the operation be retained as a meaningful adjunct to the security program at Aberdeen Proving Ground/Edgewood Arsenal, MD.

b. (U) (C) Three of the activities targeted by the ICIP are designated Critical Sensitive by USAINTA: Edgewood Arsenal, US Army Ballistics Laboratory and the US Army Materiel Systems Analysis Activity. During the six month period under review, two new confidential sources were recruited within these activities. Additional casual sources and CIRLS were also identified.

(Continue on plain bond)

IMPLICATIONS — CINFO YES ☐ NO ☐ | PRIM PROGS YES ☐ NO ☐ | BUDGET YES ☐ NO ☐

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
	Warning Notice. Sensitive Intelligence Sources and Methods Involved		BR		
			DEV		15 JAN 76
			DIR		15 Jan 76
			EX		
			ACSI		
			DISPATCHED (DTG)		

~~REGRADED UNCLASSIFIED ON 5 SEP 1997 BY USAINSCOM FOI/PA Auth Para 4-102 DOD 5200.1R~~

Classified by JCSI DA

EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF E.O. 11652

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

ACTION OFFICER *(Name, grade, phone and signature)*: LTC Haendle/56159 N. V. Haendle 825

EXEMPTION CATEGORY 2

DECLASSIFY ON 3 Dec 2006

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

536-76

[redacted]

DAMI-DOH
SUBJECT: Review of Internal Counterintelligence Program (ICIP) GONDOLA STAR (U)

c. (U) Much of the information reported in this operation continues to be related to personnel security activities with emphasis on personnel character weaknesses. However, although the ICIP did not uncover meaningful counterespionage information during the period under review, overall, GONDOLA STAR compares favorably to the other eight ongoing operations in scope and coverage of the Critical Sensitive activities at the installation.

3. (U) Recommendation: That the ACSI approve the continuation of ICIP GONDOLA STAR as an ongoing operation.

APPROVED [redacted] 16 Jan 96

DISAPPROVED _____

SEE ME _____

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOIA/PA
AUTH PARA 1-603 DoD 5200.1-R
AUTH P

[redacted]

826

[redacted]

WARNING NOTICE: Sensitive Intelligence Sources & Methods Involved

MIIA-SO-SA (17 Dec 75)
SUBJECT: ICIP GONDOLA STAR (U)

TO HQDA (DAMI-DOH/ LTC HAENDLE) WASH DC 20310

FROM CDR, USAINTA Special Operations Detachment Ft Meade, MD 20755

DATE [redacted] Mr Hime/2401/id

CMT 2 (C)

1. (U) References:

a. ACSI DA Letter, DAMI-DOH, subject: Retention of Internal Counterintelligence Program (ICIP) (U), 11 July 1975.

b. Draft ACSI letter, DAMI-DOH, subject same as ref 1a, submitted with 902d MI Group request for reinstatement of GONDOLA STAR in June 1975.

2. (U) In compliance with paragraph 4, CMT 1, comments and recommendations concerning ICIP GONDOLA STAR are submitted herewith. Subsequent to the ACSI revalidation of ICIP Operation GONDOLA STAR (U), as provided by reference 1a above, the following actions have been taken:

a. A thorough study and review of the operation was conducted. As a result of that study, it was determined that Edgewood Arsenal (EA), the US Army Ballistics Research Laboratory (BRL), and the US Army Materiel Systems Analysis Activity (AMSAA) were Critical Sensitive (CS) activities in that order of priority; with the US Army Test and Evaluation Command (TECOM), US Army Human Engineering Laboratory (HEL) and the Materiel Testing Directorate (MTD), Aberdeen Proving Ground (APG), having a sensitivity of Highly Sensitive (HS), and so designated in that priority of support. It was the goal of the operation during the last six months to provide confidential source personnel support to the three CS target areas. With the recruitment of two additional confidential sources in AMSAA during the last six months, this short-range objective was met.

b. Additionally, ten casual sources and five counterintelligence recruitment leads have been identified. Although it is the long-range objective of the operation to provide confidential source coverage to all of the targets presently identified, it is the short-range goal to recruit additional confidential sources within the Critical Sensitive targets while concurrently spotting for additional leads during the next six months. The 902d MI Group has manpower resources, to include an experienced "Great Skills" Agent Handler, to support this operation.

c. Items of counterintelligence interest reported to the supported activities in response to established EEI by source personnel have included seven incidents of foreign contact of military and DOD civilian personnel, six incidents of foreign travel by military and DOD civilian personnel, one report of solicitation by a foreign organization, three reports of identification of alien enlistees, fourteen reports of possible unsuitability of personnel in positions with access to classified

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

827

[redacted]

[redacted]

MIIA-SO-SA
SUBJECT: ICIP GONDOLA STAR (U)

material, and eighteen reports of possible security weaknesses, violations or hazards. The above information has provided five leads for the CE Branch, Special Operations Detachment, USAINTA; has led to the request for two limited investigations by the supported commands; has caused one DOD civilian to undergo a "fitness for duty" examination to include a psychiatric evaluation; and has caused reviews of security procedures and the issuance of security warnings by security officials at APG/EA. Details of the above reports are contained in Quarterly Progress Reports (attached as Inclosures 1 and 2).

3. (U) COL Ungerleider, CDR, APG; COL Stahl, CDR, Edgewood Arsenal, and MG Powers, CDR, US Army Test and Evaluation Command, APG, have received separate briefings on the status of ICIP Operation GONDOLA STAR. All have indicated their complete satisfaction with the support provided by the operation, and have enthusiastically indicated their desire that the operation be continued.

4. (U) The previously reported threat to APG/EA as contained in the report of the 1974 SAVE conducted at BRL and the threat to CBR information, equipment and weapons as outlined in reference 1b above remain valid.

5. (U) The operational objectives are being met. The operation is providing the information required and desired.

6. (U) Recommendation: Retain ICIP Operation GONDOLA STAR as a meaningful adjunct to the security program at Aberdeen Proving Ground/ Edgewood Arsenal, MD.

2 Incl
as

WILLIAM I. JENNINGS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

B28

[redacted]

Page 2321 of 3957

DISPOSITION FORM

CONFIDENTIAL

For use of this form, see AR 340-15; the proponent agency is The Adjutant General's Office.

REFERENCE OR OFFICE SYMBOL	SUBJECT
DAMI-DOH	Quarterly ICIP Reports (U)

TO CDR, USAINTA
ATTN: MIIA-SO
FT MEADE MD 20755

FROM DAMI-DOH

DATE 17 DEC 1975 CMT 1

LTC Haendle/mjb/56159

1. (U) Reference, message, DAMI-DOH, 032115Z Dec 75.

2. (C) Attached for your files is a copy of the INFORMATION MEMORANDUM to the Under Secretary of the Army (less inclosures) which forwarded summaries of the nine on-going CONUS ICIP operations as submitted by your headquarters. The summary pertaining to a proposed ICIP by the 66th MI Group in support of USASA was not included in this submission. Upon receipt of a response to the above referenced message, a decision will be made whether to include that operation in the next quarterly report.

3. (C) In staffing the Quarterly ICIP Report within OACSI, the Acting Director of Intelligence Operations noted that many of the summaries of on-going actions contained too many details of individual character/behavior issues. In future quarterly reports suitability-type information pertaining to individuals covered by the ICIP project should be either eliminated or summarized in general comments.

4. (C) On a separate matter, when the ACSI reinstated the ICIP CONDOLA STAR in July 1975, he indicated he would review the ICIP in six months to determine if significant information had been developed to warrant continuation of the project. It is requested that your headquarters conduct a review of this ICIP and furnish your comments and recommendations to this office by 9 January 1975.

FOR THE DIRECTOR OF INTELLIGENCE OPERATIONS:

1 Incl
as

L. A. SPIRITO
Colonel, GS
Chief, HUMINT Division

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

829

Classified by ACSI DA
EXEMPT FROM GEN[illegible] CLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 Dec 05

CONFIDENTIAL

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS, 902D MILITARY INTELLIGENCE GROUP
FORT MEADE, MARYLAND 20755

ICIP QUARTERLY PROGRESS REPORT NUMBER 4

Period: 1 July 1975 to 30 September 1975

WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED

1. (U) Identity: GONDOLA STAR (U).

2. (C) Supported Command: HQ, Aberdeen Proving Ground (APG), MD, and critical sensitive (CS) and highly sensitive (HS) tenant activities at APG subordinate to the major command, US Army Materiel Command, Alexandria, VA.

3. (C) Targets:

a. Edgewood Arsenal, Edgewood Area, APG.

b. US Army Ballistic Research Laboratories, Aberdeen Area, APG.

c. US Army Materiel Systems Analysis Activity, Aberdeen Area, APG.

d. HQ, US Army Test and Evaluation Command, Aberdeen Area, APG.

e. US Army Human Engineering Laboratory, Aberdeen Area, APG.

f. Materiel Testing Directorate of APG, Aberdeen Area, APG.

4. (C) Coverage:

a. Source	Target Covered	Contacts	Number/Type of Reports Produced
(1) Confidential Sources			
(a) IC-B-005	3c	3	2 Contact reports
(b) IC-B-010	3a	5	4 Contact reports 1 Agent Report
(c) IC-B-030	3e	4	3 Contact reports 6 Agent reports
(d) IC-B-032	3a	9	6 Contact reports 7 Agent reports

Classified by USAINTA Reg 381-100-1
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 2005
Incl 1

830 [redacted]

~~CONFIDENTIAL~~

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 4
Period: 1 July 1975 to 30 September 1975

(e)	IC-B-053	3a	4	3 Contact reports
(f)	IC-B-064	3b	4	3 Contact reports 2 Agent reports
(g)	IC-B-079	3a	4	3 Contact reports 2 Agent reports
(h)	IC-B-080	3c	5	4 Contact reports 3 Agent reports

(2) Conventional Sources: Conventional sources utilized during the reporting period consisted of those casual and official contacts made by the Project Liaison Officer in the furtherance of his ICIP duties. These contacts consisted of, but were not limited to, those reported in paragraphs 4a(3), 4b and 4c below. The Project Liaison Officer also had limited or one-time contact with other individuals of the supported activity's work-force. These contacts did not significantly contribute to the counterintelligence coverage of the supported activities, but did serve to project the presence of Military Intelligence in the area. These contacts also contributed significantly to the establishment of a pool from which conventional and confidential sources can be developed. No conventional sources have been tasked to gather specific essential elements of information. However, all conventional sources are made aware of the Project Liaison Officer's overt ("Military Intelligence Special Agent") duties and the type of information of interest to all security officials. No conventional sources have been key-sheeted. Those individuals who provide reportable information and express a desire to remain anonymous will be key-sheeted at the time they make their desire known.

(3) Casual Sources:

(a)	b7(d)	3f	3	0
(b)	b7(d)	3b	3	0
(c)	b7(d)	3a	2	0
(d)	b7(d)	3a	1	0

b.	Liaison Contacts	Agency	Contacts	Reports Produced
(1)	Aberdeen RO	FBI	8	0
(2)	Barracks D	MD State Police	5	0

REGARDED UNCLASSIFIED
ON SEP 15
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1-R

2 831

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 4
Period: 1 July 1975 to 30 September 1975

(3)	Sheriff's Ofc	Harford County	5	2 Agent reports
(4)	Sheriff's Ofc	Cecil County	1	0
(5)	Police Dept	Aberdeen, MD	4	2 Agent reports
(6)	Police Dept	Bel Air, MD	2	2 Agent reports
(7)	Police Dept	Havre de Grace, MD	3	2 Agent reports
(8)	Provost Marshal	PMO, APG	12	0
(9)	CID	APG	39	0
(10)	Intel Office	APG	57	2 Agent reports
(11)	MPI	PMO, APG	21	0
(12)	Security Ofc	EA, APG	14	0
(13)	Security Ofc	BRL, APG	7	1 Agent report
(14)	Security Ofc	AMSAA, APG	6	1 Agent report
(15)	Security Ofc	TECOM, APG	3	0
(16)	Security Ofc	HEL, APG	2	0
(17)	Security Ofc	MTD, APG	9	0
(18)	CPO	HQ, APG	13	2 Agent report

c. CIRIS

	Name	Phase of Development	Placement/Access
(1)	b6	Vetting started	3a
(2)	b6	Vetting started	3a

5. (FOUO) Statistics:

a. ICIP Reports:	Furnished Group HQs	Furnished Sptd Cmd	Subtotal	FY Total
(1) Spot Reports:	0	0	0	0

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

3 832 [redacted]

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~
~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 4
Period: 1 July 1975 to 30 September 1975

(2)	SOI:	0	0	0	0
(3)	IIR:	0	0	0	0
(4)	Agent Reports:	35	N/A	35	35
(5)	Lead Development Reports:	1	N/A	1	1
(6)	Contact Reports:	28	N/A	28	28
(7)	Basic Source Data Reports:	2	N/A	2	2
(8)	Other:				
	MFR:	8	N/A	8	8

Various items of information passed by word of mouth to the supported command/activities.

b.	b1	PCO	PLO	Other	Subtotal	FY Total
	b1					
c.	TDY Funds:	0	0	0	0	0
d.	Manhours:					
(1)	ICIP (GASR):	494	267	0	761	761
(2)	Other ICIP:	144	0	0	144	144
(3)	Non-ICIP:	16	354	0	370	370

6. (C) Remarks: No information was reported concerning non-affiliated civilians or organizations.

7. (C) Quarterly Briefing of Supported Command:

a. Circumstances:

(1) On 22 August 1975 COL Kenneth L. Stahl, Commander, Edgewood Arsenal (EA), Aberdeen Proving Ground (APG), MD, was brought up to date on the status of the ICIP at EA. He was informed that GONDOLA STAR had been reviewed by the Assistant Chief of Staff for Intelligence, Department

~~CONFIDENTIAL~~ 833 [redacted]
~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 4
Period: 1 July 1975 to 30 September 1975

of the Army and revalidated for another six months. At the end of the six month period, January 1976, the operation would again be reviewed. COL Stahl was reminded that MAJ Walter W. Stansberry, Former Security Officer, EA had been the ICIP Coordinator for EA and now that he had departed for reassignment a new ICIP Coordinator had to be selected and given an ICIP briefing. COL Stahl advised that he desired MAJ Stansberry's replacement, CPT Vincent J. Falconio, Security Officer, EA, be the ICIP Coordinator. COL Stahl also advised that a new deputy commander, COL Burt NMN Dall, had been assigned and he desired that COL Dall be briefed on the ICIP at EA.

(2) On 22 August 1975 CPT Vincent J. Falconio was given the initial ICIP briefing and a current status report concerning operation GONDOLA STAR (U). Falconio acknowledged his understanding of the source program and readily grasped the overall concept of ICIP. He indicated a desire to establish the best possible working relationship with the PLO. At the conclusion of the briefing Falconio executed a Security Certificate.

(3) On 17 September 1975 COL Burt NMN Dall, Deputy Commander, Edgewood Arsenal, Edgewood Area, Aberdeen Proving Ground, MD, was given the initial Internal Counterintelligence Program (ICIP) briefing. CPT Vincent J. Falconio, ICIP Coordinator, was also present during the briefing. Because COL Stahl, Commander, Edgewood Arsenal, was on annual leave, COL Dall and CPT Falconio were also given the Quarterly Progress Briefing at this time.

(4) On 24 September 1975 a Quarterly Progress Briefing was given to COL Alvin D. Ungerleider, Commander, APG, and to Mr. Harry A. Mencke, Installation Intelligence Officer, APG, the ICIP Coordinator for the Aberdeen Area, Aberdeen Proving Ground, MD.

b. Recapitulation of Operational Progress During the Period:

(1) During the first quarter of FY 1976, considerable effort was expended to reactivate and expand ICIP coverage at APG following the termination of Project GONDOLA STAR on 31 March 1975 and subsequent revalidation of the Project by the ACSI on 11 July 1975. During the latter half of July 1975, the six confidential sources which were being utilized prior to 31 March 1975 were recontacted and reactivated; one confidential source, whose recruitment had been postponed because of the termination of the project, was recruited on 5 August 1975; a Lead Development Report on an additional confidential source was submitted and approved, and this source was recruited on 4 September 1975. These two confidential sources were the first recruited in the US Army Materiel Systems Analysis Activity, a critical sensitive activity at APG.

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

834

Page 2327 of 3957

CONFIDENTIAL

ICIP QUARTERLY PROGRESS REPORT NUMBER 4
Period: 1 July 1975 to 30 September 1975

(2) The Project Liaison Officer (PLO) re-established liaison contacts in local, state and federal agencies in addition to maintenance of his contacts with the ICIP coordinators and security officers of those activities receiving ICIP support at APG. The PLO also established new casual sources in critical areas of the ICIP-supported activities at APG and vetted two new CIRIs to the point of submission of NAC requests. Some progress was made in improving the ratio of ICIP to non-ICIP duties of the PLO, who is also—during this reporting period—the only special agent of the Aberdeen RO; this ICIP to non-ICIP ratio has been a weak area of Project GONDOLA STAR since its reactivation in 1972. A favorable trend was established as the quarter progressed, as reflected by the fact that during July 1975 the PLO's duty hours were 45 ICIP and 172 non-ICIP, during August 1975 they were 94 ICIP and 115 non-ICIP, and during September 1975, 122 ICIP and 67 non-ICIP.

c. Significent Counterintelligence Information Developed:

(1) Under the EEI, "Identification and extent of foreign contacts of military and DoD civilian personnel, with particular emphasis on Sino-Soviet bloc countries" (paragraph 1, Appendix 1 to Annex J to OP-001-74-109), the following information was developed:

(a) Source IC-B-064 reported that an unknown number of Swedish citizens would visit the US Army Ballistic Research Laboratories (BRL), APG, on 13 August 1975. Follow-up by the PLO determined that the visit had been properly coordinated.

(b) Source IC-B-080 reported that seven Swedish citizens would visit the US Army Materiel Systems Analysis Activity (AMSAA), APG, on 26 September 1975. Follow-up by the PLO determined that the visit had not been properly coordinated, but that AMSAA had taken action to insure that the Swedish visitors would not be given access to classified information until definitive guidance was received from HQ, US Army Materiel Command.

(2) Under the EEI, "Foreign travel of military and civilian personnel, either intended or completed, to Communist controlled countries, or attendance at social and official functions at which Communist country personnel are present" (paragraph 2, Appendix 1 to Annex J to OP-001-74-109), the following information was developed:

(a) Source IC-B-010 reported that GS-12 b6 a pharmocologist employed in the Biomedical Laboratory, Edgewood Arsenal, APG, had, at HER own expense, attended the Sixth Congress of the International Union of Pharmocologists (IUPHAR) which was held in Helsinki,

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

CONFIDENTIAL

CONFIDENTIAL

ICIP QUARTERLY PROGRESS REPORT NUMBER 4
Period: 1 July 1975 to 30 September 1975

Finland, 20 through 25 July 1975. During the Congress, b6 attended a luncheon hosted by a representative of the Union of Soviet Socialist Republics (USSR), who was also an official of the IUPHAR. Following the Congress, b6 took part in a five-day, IUPHAR-sponsored tour to Leningrad, USSR. Follow-up by the PLO is in progress.

(b) Source IC-B-030 reported that GS-12 b6 an employee of Human Engineering Laboratory, APG, intended to participate in a two-week tour of the Union of Soviet Socialist Republics scheduled to begin on 2 October 1975. Follow-up by the PLO determined that b6 was participating in a National Geographic Society tour and that HE had coordinated the tour with appropriate security officials.

(c) Source IC-B-032 reported that GS-12 b6 an employee of Development and Engineering Directorate, Edgewood Arsenal, APG, had visited Poland and Czechoslovakia for approximately one month in June 1975. During this visit, b6 and HIS spouse had allegedly visited relatives in Poland and Czechoslovakia. No follow-up was conducted per instructions from HQ, USAINTA.

(3) Under the EEI, "Identification of Alien Enlistees" (paragraph 6, Appendix 1 to Annex J to OP-001-74-109), the following information was developed:

(a) Source IC-B-030 reported that PFC b6, born in b6, assigned to Human Engineering Laboratory, APG, was not a citizen of the US and did not have a security clearance. Follow-up by the PLO confirmed the information and determined that the Installation Intelligence Officer (IIO), APG, was aware of b6 status.

(b) Source IC-B-030 reported that SP4 b6 born in b6 assigned to Human Engineering Laboratory, APG, was not a US citizen, did not have a security clearance, and allegedly suffered from periods of amnesia. Follow-up by the PLO confirmed the information and determined that the IIO was aware of b6 status.

(c) Source IC-B-030 reported that PFC b6, believed to have been born in b6 assigned to Human Engineering Laboratory, APG, was not a US citizen and did not have a security clearance. Follow-up by the PLO is in progress.

(4) Under the EEI, "Early detection of persons whose activities and character weaknesses render them vulnerable to hostile intelligence exploitation" (paragraph 8, Appendix 1 to Annex J to OP-001-74-109), the following information was developed:

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 [illegible] 5200.1R

[redacted] 836

CONFIDENTIAL

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 4
Period: 1 July 1975 to 30 September 1975

(a) Source IC-B-032 reported that GS-5 b6 married, a secretary in Technical Support Directorate, Edgewood Arsenal, APG, was allegedly involved in an extramarital relationship with WS-7 b6 b6 married, an employee of Technical Support Directorate. The situation is being monitored.

(b) Source IC-B-032 reported that GS-12 b6 married, employed in Development and Engineering Directorate, Edgewood Arsenal, APG, was allegedly involved in an extramarital relationship with GS-9 b6 b6 a widow, also employed in Development and Engineering Directorate. The situation is being monitored.

(c) Source IC-B-032 reported that GS-6 b6 married, a secretary in Technical Support Directorate, Edgewood Arsenal, APG, was allegedly involved in an extramarital relationship with GS-9 b6 b6 separated from his wife, employed in US Army Materiel Systems Analysis Activity, APG. The situation is being monitored.

(d) An official source of the PLO who did not want to be identified because of fear that he would lose his job, reported that LTC b6 b6 formerly assigned to US Army Materiel Systems Analysis Activity (AMSAA), now assigned to Concepts Analysis Activity (CAA), Bethesda, MD, was allegedly an alcoholic, was allegedly cohabiting with GS-8 b6 b6 an employee of AMSAA, and allegedly had had sexual intercourse with a female Captain in the Isreali Defense Forces who had been assigned as b6 interpreter when b6 was on TDY to Israel in October 1974. No follow-up action has been taken because of b6 transfer from AMSAA.

(e) Source IC-B-064 reported that GS-8 b6 an employee of AMSAA, APG, had allegedly been involved in an extramarital relationship with PL 313 federal employee, b6 Director, AMSAA, at approximately the time of the accidental death of b6 wife. The situation is being monitored.

(f) Source IC-B-079 reported that an individual, later identified as b6 a physical scientist employed in the Chemical Laboratory, Edgewood Arsenal, APG, had allegedly exhibited mental or emotional instability. Follow-up by the PLO determined that b6 had been directed to undergo a "fitness for duty" physical examination which would include a psychiatric evaluation.

(5) Under the EEI, "Security violations or hazards" (paragraph 9, Appendix 1 to Annex J to OP-001-74-109), the following information was developed:

DECLARED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

837

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 4
Period: 1 July 1975 to 30 September 1975

(a) Source IC-B-030 reported that GS-14 b6 an employee of Human Engineering Laboratory, APG, had brought HIS eight-year-old son into a controlled access area where a classified test was being conducted and remained overnight. Follow-up by the PLO determined that b6 had been counselled by HIS supervisor.

(b) Source IC-B-030 reported that carbon paper and one-time typewriter ribbon used to type classified reports in Human Engineering Laboratory, APG, had not been treated as classified waste. Follow-up by the PLO brought the situation to the attention of the security officer, HEL, who promised to take care of the situation; monitoring through IC-B-030 has not determined that any such action was taken.

(c) Source IC-B-080 reported ten(10) separate situations which constituted security violations or hazards at AMSAA. These were brought to the attention of the Security Officer, AMSAA, by the PLO.

(6) In response to the EEI, "Conduct rendering the individual vulnerable to pressure, such as homosexual, criminal, or immoral acts" (paragraph 8c, Appendix 1 to Annex J to OP-001-74-109), and "Sudden, unexplained or inadequately explained absence from work by personnel in excess of 24 hours" (paragraph 9, Appendix 2 to Annex J to OP-001-74-109), the following information was developed: The PLO was advised by an official Source at the US Army Ballistics Research Laboratories, APG, of unconfirmed rumors to the effect that b6 an employee of BRL, had been involved in trouble with the police. Follow-up by the PLO determined that seven charges ranging from possession of marijuana to grand larceny and assault and battery were on file at the Havre de Grace Police Department, Havre de Grace, MD, concerning b6 and that b6 was absent without leave.

8. (C) Actions implemented or taken by the supported command based upon the information submitted:

Subject	Type Information Developed	Action Taken	Date of Action
b6	Foreign travel	None.	
	Foreign travel	None.	
	Foreign travel	None.	
	Enlisted alien	None.	
	Enlisted alien/ amnesia	Denied clearance	Unknown
b6	Enlisted alien	None.	
	Suitability	Monitor	
	Suitability	Monitor	

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

[redacted]
838

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 4
Period: 1 July 1975 to 30 September 1975

b6	Suitability	Monitor	
	Suitability	Monitor	
	Suitability	Unknown	
	Suitability	Monitor	
	Suitability	"Fitness for duty" physical	11 Aug 75
	Security weakness	Counseled	Unknown
Security weaknesses, HEL, various		Correct	2 Sep 75
Security weaknesses, AMSAA, various		Correct	9 Sep 75
b6	Suitability	Investigate	16 Sep 75

9(U)(C) Comments, Remarks and Recommendations: Both COL Stahl and COL Ungerleider expressed their pleasure that ICIP Project CONDOLA STAR had been reinstated by the ACSI for an additional six months. Both Commanders and their designated ICIP Coordinators continue to cooperate fully with the Project Liaison Officer and his Military Intelligence chain of command. The progress of ICIP Project GONDOLA STAR, as reflected above, is directly proportional to the amount of time the PLO's other duties permit him to devote to the ICIP.

WILLIAM B. HALL
Project Case Officer

REGARDED UNCLASSIFIED
ON SEP 5
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

[redacted]

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ABERDEEN RESIDENT OFFICE
902D MILITARY INTELLIGENCE GROUP
ABERDEEN PROVING GROUND, MARYLAND 21005

ICIP QUARTERLY PROGRESS REPORT NUMBER 2

Period 1 October 1975 to 31 December 1975

WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED

1. (U) Identity: GONDOLA STAR (U).

2. (U) Supported Command: HQ, Aberdeen Proving Ground (APG), HD, and critical sensitive (CS) and highly sensitive (HS) tenant activities at APG subordinate to the major command; US Army Materiel Command, Alexandria, VA.

3. (U) Targets:

a. Edgewood Arsenal, Edgewood Area, APG.

b. US Army Ballistic Research Laboratories, Aberdeen Area, APG.

c. US Army Materiel Systems Analysis Activity, Aberdeen Area, APG.

d. HQ, US Army Test and Evaluation Command, Aberdeen Area, APG.

e. US Army Human Engineering Laboratory, Aberdeen Area, APG.

f. Materiel Testing Directorate of APG, Aberdeen Area, APG.

4. (U) Coverage:

a. Source	Target Covered	Contacts	Number/Type of Reports Produced
(1) Confidential Sources			
(a) IC-C-005	3c	3	3 Contact Reports 5 Agent Reports
(b) IC-C-010	3a	3	3 Contact Reports 6 Agent Reports
(c) IC-C-030	3e	4	4 Contact Reports 8 Agent Reports
(d) IC-C-032	3a	8	5 Contact Reports 5 Agent Reports

Classified by USAINTA REG 380-320-1
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 2005

Encl 2

840

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

~~CONFIDENTIAL~~

ABERDEEN RESIDENT OFFICE
902D MILITARY INTELLIGENCE GROUP
ABERDEEN PROVING GROUND, MARYLAND 21005

ICIP QUARTERLY PROGRESS REPORT NUMBER 2

Period 1 October 1975 to 31 December 1975

WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED

1. (U) Identity: GONDOLA STAR (U).

2. (C) Supported Command: HQ, Aberdeen Proving Ground (APG), HD, and critical sensitive (CS) and highly sensitive (HS) tenant activities at APG subordinate to the major command; US Army Materiel Command, Alexandria, VA.

3. (C) Targets:

a. Edgewood Arsenal, Edgewood Area, APG.

b. US Army Ballistic Research Laboratories, Aberdeen Area, APG.

c. US Army Materiel Systems Analysis Activity, Aberdeen Area, APG.

d. HQ, US Army Test and Evaluation Command, Aberdeen Area, APG.

e. US Army Human Engineering Laboratory, Aberdeen Area, APG.

f. Materiel Testing Directorate of APG, Aberdeen Area, APG.

4. (C) Coverage:

a. Source	Target Covered	Contacts	Number/Type of Reports Produced
(1) Confidential Sources			
(a) IC-C-005	3c	3	3 Contact Reports 5 Agent Reports
(b) IC-C-010	3a	3	3 Contact Reports 6 Agent Reports
(c) IC-C-030	3e	4	4 Contact Reports 8 Agent Reports
(d) IC-C-032	3a	8	5 Contact Reports 5 Agent Reports

Classified by USAINTA REG 380-320-1
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON 31 DEC 2005

Ind 2

840

~~CONFIDENTIAL~~

REGRADED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

CONFIDENTIAL

(e)	IC-B-053	3a	3	3 Contact Reports 2 Agent Reports
(f)	IC-B-064	3b	3	3 Contact Reports
(g)	IC-B-079	3a	3	3 Contact Reports 1 Agent Reports
(h)	IC-B-080	3c	5	4 Contact Reports 5 Agent Reports

(2) Conventional Sources: As in previous quarters the conventional sources utilized during the reporting period consisted of those casual and official contacts made by the Project Liaison Officer in the furtherance of his ICIP duties. These contacts consisted of, but were not limited to, those reported in paragraphs 4a(3), 4b and 4c below. The Project Liaison Officer also had limited or one-time contact with other individuals of the supported activities. These contacts did not significantly contribute to the counter-intelligence coverage of the supported activities, but did serve to project the presence of Military Intelligence in the area. These contacts also contributed significantly to the establishment of a pool from which conventional and confidential sources can be developed. No conventional sources have been tasked to gather specific essential elements of information. However, all conventional sources are made aware of the Project Liaison Officer's overt ("Military Intelligence Special Agent") duties and the type of information of interest to all security officials; information which denotes a security weakness or vulnerability. No conventional sources have been key-sheeted. These individuals who provide reportable information and express a desire to remain anonymous will be key-sheeted at the time they make their desire known.

(3) Casual Sources:

(a)	b1	3a	1	0
(b)	b1	3a	2	0
(c)	b1	3a	2	0
(d)	b1	3a	1	0
(e)	b1	3b	0	0
(f)	b1	3b	1	0
(g)	b1	3c	1	0

CONFIDENTIAL

~~CONFIDENTIAL~~

(h)	b1	3f	2	0
(i)	b1	3f	4	0
(j)	b1	3a	2	0

b. Liaison Contacts

	Agency	Contacts	Reports Produced
(1) Aberdeen RO	FBI	6	0
(2) Barracks D	Md State Police	3	0
(3) Sheriff's Ofc	Harford County	4	1 Agent Report
(4) Sheriff's Ofc	Cecil County	1	0
(5) Police Dept	Aberdeen, Md.	5	1 Agent Report
(6) Police Dept	Bel Air, Md.	3	1 Agent Report
(7) Police Dept	Havre de Grace, Md.	2	1 Agent Report
(8) Provost Marshal	PMO, APG	14	0
(9) CID	APG	36	1 Agent Report
(10) Intel Ofc	APG	59	1 Agent Report
(11) MPI	PMO, APG	31	1 Agent Report
(12) Security Ofc	BA, APG	15	0
(13) Security Ofc	BRL, APG	9	0
(14) Security Ofc	AMSAA, APG	5	1 Agent Report
(15) Security Ofc	HQ, TECOM, APG	5	0
(16) Security Ofc	HEL, APG	4	1 Agent Report
(17) Security Ofc	MTD, APG	9	0
(18) CPO	HQ, APG	6	3 Agent Reports
(19) Baltimore FO	DIS	24	1 Agent Report

c. CIRLS

Name	Phase of Development	Placement/Access
(1) b1	LDR Submitted	3a

b1 RITCHIE FO 1 DEC 75

842

~~CONFIDENTIAL~~

CONFIDENTIAL

ICIP QUARTERLY PROGRESS REPORT NUMBER 2
Period: 1 October 1975 to 31 December 1975

(2)	b1	Half Vetted	3a
(3)	b1	LDR Started	3a
(4)	b1	Vetting Started	3a
(5)	b1	Spotted	3a

5. ~~(FOUO)~~ Statistics:

a. ICIP Reports:	Furnished Group HQs	Furnished Sptd Cmd	Subtotal	FY Total
(1) Spot Reports:	0	0	0	0
(2) SOI:	0	0	0	0
(3) IIR:	0	0	0	0
(4) Agent Reports	45	N/A	45	80
(5) Lead Development Reports:	1	N/A	1	2
(6) Contact Reports:	28	N/A	28	56
(7) Basic Source Data Reports:	1	N/A	1	3
(8) Other:				
MFR:	7	N/A	7	15

All information for the supported activities was passed by word of mouth from the PLO.

b. b1	PCC	PLO	Other	Subtotal	FY Total
b1					
c. TDY Funds:	0	0	0	0	0
d. Manhours:					
(1) ICIP (CASE):	406	475	0	861	1642
(2) Other ICIP	116	0	0	116	260
(3) Non-ICIP:	72	187	0	259	629

4

843

CONFIDENTIAL

CONFIDENTIAL

ICIP QUARTERLY PROGRESS REPORT NUMBER 2
Period: 1 October 1975 to 31 December 1975

6. (U) Remarks: No information was reported concerning non-affiliated civilians or organizations.

7. (U) Quarterly Briefing of Supported Command:

a. Circumstances:

(1) On 1 December 1975 the initial ICIP briefing was given to MG Patrick W. Powers, Commander, US Army Test and Evaluation Command (TECOM) and COL William H. Tucker Jr., Chief of Staff, TECOM. The status of TECOM in relation to receiving ICIP support was also included in the briefing. It was pointed out that due to the limitation of resources GONDOLA STAR (U) was concentrating on three higher priority activities at APG. This was due to the three activities having a greater degree of sensitivity. Should the resource problem improve to the point where TECOM could be covered beyond routine liaison then TECOM would be immediately notified. MG Powers acknowledged his understanding of the current status of GONDOLA STAR (U).

(2) On 17 December 1975 COL Kenneth L. Stahl, Commander, Edgewood Arsenal, APG was given a Quarterly Progress Report briefing as pertains to the Edgewood Arsenal portion of Operation GONDOLA STAR (U).

(3) On 19 December 1975 COL Alvin D. Engerleider, Commander, APG was given a Quarterly Progress Report briefing as pertains to those activities located in the Aberdeen Area, APG which are supported by GONDOLA STAR (U). Mr. Harry A. Mencke Installation Intelligence Officer, APG, the ICIP Coordinator for the Aberdeen Area, APG, was also present for this briefing.

b. Recapitulation of Operational Progress During the Period: During the first quarter of FY 1976 GONDOLA STAR (U) was reactivated, two new confidential sources were recruited and efforts started to increase the ICIP coverage. In the second quarter FY 1976 efforts were made to broaden the ICIP coverage of the three priority activities designated CRITICAL SENSITIVE; Edgewood Arsenal, US Army Ballistic Research Laboratories and US Army Materiel Systems Analysis Activity. In this regard significant progress was made. Training and development of the two newly recruited confidential sources (IC-B-005 and IC-A-080) progressed and their production increased accordingly. Again during this quarter the PM had additional time available to devote to ICIP duties. This allowed the PM to more than double the time of his presence in the supported activities, as compared to previous quarters. Consequently, there was an increase in CHIS, casual sources and the activity cited in paragraph 4a(2) above.

c. Significant Counterintelligence Information Developed:

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 2
Period: 1 October 1975 to 31 December 1975

(1) Under the EEI, "Identification and extent of foreign contacts of military and DOD Civilian personnel, with particular emphasis on Sino-Soviet bloc countries" (paragraph 1, Appendix 1 to Annex J to OP-001-74-109), the following information was developed:

(a) Source IC-E-030 reported Mr. b6 a citizen of the Federal Republic of Germany was assigned on an exchange program to work in the US Army Human Engineering Laboratory until September 1976. The ICIP Coordinator was briefed, no additional action is expected.

(b) Source IC-E-005 reported SGT b6 assigned to the US Army Materiel Systems Analysis Activity, had a former wife and two children residing in the Federal Republic of Germany. The ICIP Coordinator was briefed and local files were checked.

(c) Source IC-E-032 reported additional information concerning travel by GS-12 b6 to Czechoslovakia and Poland during the summer of 1975. Additional information was also provided concerning b6 plans for another trip to those countries. ICIP Coordinator was briefed and the information was also brought to the attention of another USAINTA element. The ICIP Coordinator expects ICIP to continue to monitor b6 activities.

(d) Source IC-E-010 reported one British and three Canadian personnel visited Edgewood Arsenal during the period 1-5 December 1975. A check with the ICIP Coordinator determined the visit had been properly cleared.

(e) Source IC-E-010 reported GS-15 b6 of Edgewood Arsenal was a medical student at the American University, Beirut, Lebanon during 1971 and raised the question of how b6 was able to avoid military service with the German Army during the war. The ICIP Coordinator was briefed. The ICIP Coordinator asked to have b6 USAIRR dossier reviewed in order to attempt to answer the question. This action is pending. b6 HQA-CH-21, has indicated that an RI was requested by AFG/ DEC.2 1975

(2) Under the EEI, "Intended foreign travel of military and DOD civilian personnel to Sino-Soviet bloc countries or attendance at social and official functions at which Sino-Soviet bloc personnel are present" (paragraph 2, Appendix 1 to Annex J to OP-001-74-109), the following information was developed:

(a) Source IC-E-030 reported GS-12 b6 an employee of the Human Engineering Laboratory, and his wife, b6 an employee of the US Army Materiel Systems Analysis Activity, took a 10 to 14 day tour to Moscow and Leningrad which was sponsored by the Smithsonian Institution in Washington, DC. Since the FLO was already aware of the b6 giving notification of the trip through their chain of command and the information having already come to the attention of another element of USAINTA, no action was taken. FLO did make mention to the ICIP Coordinator that the information had also been developed through ICIP

DOWNGRADED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 2
Period: 1 October 1975 to 31 December 1975

(b) In a separate report source IC-B-030 reported the b6 intend to take another tour to Russia during the summer of 1976. This information was passed to the ICIP Coordinator.

(3) Under the EEI, "Solicitation by foreign nationals or organizations of personal and/or official information through official or non-official channels"(paragraph 4, Appendix 1 to Annex J to CP-001-74-109), the following information was developed:

(a) Source IC-[illegible]-030 reported the Human Engineering Laboratory received a written request for bibliographies of HEL publications from b6 b6 Institute of Experimental Psychology, Slovak Academy of Sciences, Kocelova 17, Bratislava, Czechoslovakia. The Director, HEL, sent a letter to b6 advising HEL no longer had copies of the bibliographies available for distribution to the public. The Director of HEL suggested b6 initiate contact through the Czechoslovak Embassy with the National Technical Information Services, 5285 Port Royal Road, Springfield, VA 22151. The ICIP Coordinator was briefed, no action is pending.

(4) Under the EEI, "Early detection of persons whose activities and character weaknesses render them vulnerable to hostile intelligence exploitation" (paragraph 8, Appendix 1 to Annex J to CP-001-74-109), the following information was developed:

(a) Source IC-B-005 reported MAJ b6 US Army Materiel Systems Analysis Activity, was divorced and cohabitating with GS-9 b6 b6 also divorced. b6 had also defaulted in support payments to his former wife. The ICIP Coordinator was briefed and ICIP is continuing to monitor the b6 situation.

(b) Source IC-B-032 reported information concerning a possible extra-marital relationship between GS-14 b6 and GS-3 b6 b6 both employees of Edgewood Arsenal. The ICIP Coordinator was briefed and ICIP was asked to continue to monitor the situation.

(c) Source IC-B-032 reported being told by a coworker that a "go-go dancer" at the NCO Club performed the function of sexual partner, presumably in exchange for monetary remuneration, for high-ranking visitors to Edgewood Arsenal. Local inquiry by the FIO determined the go-go dancer was no longer employed by the APG Club system. No information was developed to confirm or refute the information from source's coworker. The information was passed to the ICIP Coordinator who requested additional information as it becomes available.

(d) Source IC-B-010 reported information which could tend to indicate GS-15 b6 was mentally unstable. The ICIP Coordinator was briefed and a limited investigation was requested.

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

7 846

~~CONFIDENTIAL~~

REGARDED UNCLASSIFIED
ON SEP 05 1997
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 2
Period: 1 October 1975 to 31 December 1975

(e) Source IC-B-053 reported GS-12 [b6] Edgewood Arsenal, took a woman (NFI) who was not his wife to lunch almost every day since 1 November 1975. The ICIP Coordinator was briefed; no action is pending.

(f) Source IC-B-053 reported GS-14 [b6] Edgewood Arsenal, was observed on approximately a dozen occasions taking a woman, not his wife, to lunch. [b6] was observed taking three or four different women to lunch since 1 September 1975. The ICIF Coordinator was briefed; no action is pending.

(g) Source IC-B-032 reported GS-13 [b6] Edgewood Arsenal, had a reputation of a "mad scientist". Also that [b6] had bragged about having intercourse with an alleged prostitute. On a date [b6] took source to his home and offerred to take care of her financially if she would take care of his sexual needs; source declined. The ICIF Coordinator was briefed. The ICIF Coordinator is making a local inquiry in advance of requesting a Limited Investigation.

(h) Source IC-B-005 reported MAJ [b6] US Army Materiel Systems Analysis Activity, claimed $4.00 for a tip to a baggage handler on his TDY voucher when he did not give a $4.00 tip. The ICIF Coordinator was briefed, follow up action is yet to be determined.

(5) Under the EMI, "Security violations or hazards" (paragraph 9, Appendix 1 to Annex J to OP-001-74-109), the following information was developed:

(a) Source IC-B-080 reported a CONFIDENTIAL document had been left unsecured over a three day weekend. The ICIF Coordinator was briefed; follow up action is pending. (AMSAA Security Officer away TDY until 15 Dec)

(b) Source IC-B-080 reported a security container had been left open during duty hours in an unattended office at the US Army Materiel Systems Analysis Activity. The ICIF Coordinator was briefed, follow up action is pending.

(c) Source IC-B-080 reported [b6] a secretary in the US Army Materiel Systems Analysis Activity left her office unsecured and her security container open for periods of five to ten minutes while performing chores away from her office. The ICIF Coordinator was briefed, follow up action is pending.

(d) Source IC-B-080 reported attending a scientific conference at the US Army Materiel Systems Analysis Activity which had been anounced as classified. Access to the conference had not been properly controlled; however, the portion of the conference attended by source was believed to have been unclassified. The ICIF Coordinator was briefed, follow up action is pending.

(e) Source IC-B-080 reported the Ground Warfare Division of the US

Page 2341 of 3957

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 2
Period: 1 October 1975 to 31 December 1975

Materiel Systems Analysis Activity had moved to different office space. Prior to the move no technical survey was conducted to determine if there were electronic surveillance devices in the new office space. The ICIP Coordinator was briefed, follow up action is pending.

(f) Source IC-E-010 reported information relative to an adverse morale situation in the Bio-Medical Laboratory of Edgewood Arsenal. The situation was alleged to have been created by DA-level officials unjustly letting b6 take the blame publicly for DA-directed research in hallucinogenic drugs, and that DA was in fact offering b6 as a "sacrificial lamb". This information was immediately passed to the ICIP Coordinator and the Commander of Edgewood Arsenal. The commander raised several questions concerning the personalities involved and the cause of adverse morale situation. These questions were covered at the next meeting with this source and the answers were provided to the commander. The commander asked that ICIP continue to monitor the situation.

(6) In response to the objective of identifying and neutralizing threats of espionage, sabotage and subversion, Source IC-5-030 reported the Human Engineering Laboratory's receipt of two unsolicited requests for information. The requests were from the president of a company which claimed to be involved in the national effort to reduce and prevent crime. The information requested was unclassified. HEL provided the information asked for in the first request, but did not have the information to satisfy the second request. Initial investigation failed to confirm the existence of the company identified in the request. The ICIP Coordinator was briefed and HEL will not honor any further requests from this company until all checks by MI have been completed.

3. (U) Actions implemented or taken by the supported command based upon the information submitted:

Subject	Type Information Developed	Action Taken	Date of Action
b6	Foreign Connection	Monitor	
	Foreign Travel	Monitor	
	Foreign Connection & suitability	Monitor & investigate	23 December 1975
b6	Foreign Travel	None.	
	Foreign Travel	None.	
	Suitability	Monitor	
	Suitability	None	
	Suitability	None	
	Suitability	Monitor	
	Suitability	Not yet determined	

REGARDED UNCLASSIFIED
ON
BY CDR USAINSCOM FOI/PO
Auth Para 1-603 DoD 5200.1R

9 848

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

ICIP QUARTERLY PROGRESS REPORT NUMBER 2
Period: 1 October 1975 to 31 December 1975

9. (C) Comments, Remarks and Recommendations: Both commanders and their ICIP Coordinators continue to consider GONDOLA STAR (U) a significant adjunct to their security program. This Project Liaison Officer continues to receive the complete cooperation of all associated personnel of the supported activities.

Richard L. Grider
RICHARD L. GRIDER
Project Liaison Officer

REGARDED UNCLASSIFIED
SEP 05 1997
CDR USAINSCOM FOI/PO
Exm Para 1-603 DoD 5200.1R

[redacted]

849

~~CONFIDENTIAL~~

Page 2343 of 3957

THIS MUST REMAIN T O P D O C U M E N T

DOSSIER NO. ZF011946W
Vol 7 of 7 Vols

As of 18 Sep 85 (Date) all material included in this file conforms with DA policies currently in effect.

Delmar Smith 18 Sep 85
(Signature) (Date Signed)

Delmar Smith GS5
(Printed Name) (Grade)

Reviewed for Retention
Criteria UP AR 381-10
Reviewer [illegible] Date 4 Jan 93

THIS MUST REMAIN T O P D O C U M E N T

IA (HQ) Form 2214
(1 Sep 78)

Replaces MIIA Fm 315, 1 Jun 75, which may be used until supplies are exhausted.

850

C

REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

ACTION SHEET

CONTROL NUMBER

Report of Unilateral Counterintelligence Program (ICIP) Operation

OFFICE SYMBOL: DAMI-CIC

SUSPENSE:

DATE: 7 March 1979

ACTION REQUIRED

To obtain ACSI approval for termination of ICIP.

MEMORANDUM FOR RECORD *(Describe briefly the requirement, background and action taken or recommended. Must be sufficiently detailed to identify the action without recourse to other sources.)*

1. (U) BACKGROUND: INSCOM-SOD on 9 Feb 79, requested authority to terminate ICIP - LENTIL MONKEY (U) located at the Defense Language Institute (DLI), Presidio of Monterey, CA. The ICIP is an OACSI, DA program.

2. (U) DISCUSSION:

a. The ICIP is a special operational security service employing timely, effective and coordinated use of overt and covert CI sources and techniques to detect elements or factors which are detrimental to security. The primary factor which distinguishes the ICIP operation from CI support normally provided to an installation or unit by MI groups is the use of confidential sources as covert assets in the conduct of the operation.

b. Command security threats covered by the ICIP include acts of espionage, sabotage, subversion, and the activities of hostile foreign intelligence directed against [redacted] the supported command.

c. INSCOM-SOD's status report, 1st Quarter, FY 79, for ICIP Operation LENTIL MONKEY (U) reveals that the operation utilized 16 confidential sources, produced two Summaries of Information, one Source Lead Development Report, 35 Contact Reports and 40 Agent Reports. Further, a total of 1148 manhours were expended on the operation (TAB B).

d. INSCOM-SOD has suggested that a different type program would be better suited to provide the required security assistance for the DLI, i.e., a Dedicated Operations Security Support Program (DOSSP), which does not use confidential sources and which can be readily implemented by the 902d MI Group with existing personnel assets. A DOSSP is described at TAB C. The DOSSP for DLI would be tailored to satisfy local security requirements unique to DLI.

CLASSIFIED BY: [illegible] INSCOM ICIP dtd 9 Feb 79

(Continue on plain bond)

IMPLICATIONS — CINFO: YES ☐ NO ☐ — PRIM PROGS: YES ☐ NO ☐ — BUDGET: YES ☐ NO ☐

REVIEW ON: 7 March 99

COORDINATIONS			APPROVALS		
OFFICE	NAME	PHONE		INITIALS	DATE
			BR		7 Mar 79
			DEV		8 Mar 79
			DTR		9 Mar 79
			EX		
			ACSI		11 Mar
			DISPATCHED (DTG)		

SHOW ADDITIONAL COORDINATION ON REVERSE SIDE OR CONTINUATION SHEET

EXTENDED BY:

ACTION OFFICER *(Name, grade, phone and signature)*

Miss M. Brannan/x53501

851

REASON: Para 2-301, DOD 5200.1-R (circle appropriate subparagraph(s))

ACSI FORM 28, 13 Sep 71

~~CONFIDENTIAL~~

REGRADED WHEN SEPARATED FROM CLASSIFIED DOCUMENT

1 2 3 4 5 6 7 8

~~CONFIDENTIAL~~

DAMI-CIC
SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operation
Operation (U)

e. The general concept and recommendation to replace LENTIL MONKEY (U) with a DOSSP have been discussed and concurred in by Cdr, SOD, INSCOM, the Commandant and Security Officer at DLI, and 902d MI Group.

f. Basis for termination of subject ICIP and replacement by DOSSP is that information obtained from LENTIL MONKEY (U) is general in nature and can be obtained through normal security assistance to installation, ~~INSCOM-SOD's current investigative and reporting authority and most important the lack of a clear definition of physical surveillance which has caused those working the operation much concern (TAB B)~~.

g. By 1st Ind (TAB A) authority granted INSCOM-SOD for termination of LENTIL MONKEY (U).

3. (U) RECOMMENDATION: That 1st Ind (TAB A) be approved and signed.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

852

(U) LENTIL MONKEY: (QSR, 1st QTR FY 79)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Sixteen

c. Information Obtained or Reported on Non-affiliated Civilians: None

d. Useful Information Obtained:

(1) An instructor of the German Language Department (GLD) who visited East Berlin while on a trip to Europe, failed to comply with DLI regulations directing prior reporting of such visits. Two other GLD instructors may have also visited East Germany during the quarter without reporting the event.

(2) Instructors of the Polish Language Department encouraged students to attend a dance sponsored by a Polish ethnic organization in Oakland, CA in January 1979. It was stipulated, however, that the students must attend the dance in uniform.

(3) According to a report from another government investigative agency, a recently hired Russian Language Department (RLD) instructor had previously been of interest to a Yugoslavian intelligence agent working out of the Yugoslavian Consulate in San Francisco while the instructor was attending DLI as part of an exchange program in the late 1960's.

(4) Several instructors in the Chinese Mandarin Language Department (CMLD) are opposing the new Interagency Course Curriculum. Instructors have been reported to be inflating exam grades in order to present a false impression of student abilities. The students lack of language capability will be manifested once they reach field assignments and thus discredit the new course.

e. Operational Status:

(1) Sixteen confidential sources were active during the quarter. Four sources were terminated and one new source recruited. Ten conventional sources also provided information during the quarter.

(2) During the reporting period, information obtained from all sources, including that acquired from overt liaison activities, resulted in production of two Summaries of Information, 35 Contact Reports, 65 oral reports to the DLI Commandant and/or designated representatives, one Source Lead Development Report, and 40 Agent Reports. A total of 1148 manhours were expended on the ICIP during the 1st quarter.

CLASSIFIED BY CDR INSCOM
REVIEW 22 JAN 99
EXTENDED BY CDR INSCOM
REASON 2-301.3.c.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

853

(3) On 18 December 1978, the required quarterly briefing was presented to COL Thomas G. Foster III, Commandant, DLI. COL John Gargus (USAF), DLI Deputy Commandant, LTC Richard P. Kelly, DLI Executive Officer, LTC Waldo R. Webb, DLI Security Officer, and MAJ Michael A. Parkes, Commander, Fort Ord Field Office, 902d MI Group, also attended the briefing.

(4) As a result of the quarterly briefing and based on information reported during the quarter, the DLI Commandant directed the Security Officer to prepare a letter to be sent through channels to the GLD instructor who visited East Berlin (para d(1)) requesting an explanation for his failure to comply with DLI policy. Additionally, the Security Officer will intensify efforts to develop policy concerning appropriate instructor-student relationships/behavior. The Commandant also directed the DLI Information Officer to publish a notice emphasizing restrictions on military personnel participating in political and certain other events while in uniform, and the Security Officer will insure DLI unit commanders emphasize military regulations governing participation in such functions to their units.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

954

Page 2348 of 3957

~~CONFIDENTIAL~~

DAMI-CIC

Report of Internal Counterintelligence Program (ICIP) Operation

7 March 1979

To obtain ACSI approval for termination of ICIP.

1. (U) BACKGROUND: INSCOM-SOD on 9 Feb 79, requested authority to terminate ICIP - LENTIL MONKEY (U) located at the Defense Language Institute (DLI), Presidio of Monterey, CA. The ICIP is an OACSI, DA program.

2. (U) DISCUSSION:

a. The ICIP is a special operational security service employing timely, effective and coordinated use of overt and covert CI sources and techniques to detect elements or factors which are detrimental to security. The primary factor which distinguishes the ICIP operation from CI support normally provided to an installation or unit by MI groups is the use of confidential sources as covert assets in the conduct of the operation.

b. Command security threats covered by the ICIP include acts of espionage, sabotage, subversion, and the activities of hostile foreign intelligence directed against ~~or from within~~ the supported command.

c. INSCOM-SOD's status report, 1st Quarter, FY 79, for ICIP Operation LENTIL MONKEY (U) reveals that the operation utilized 15 confidential sources, produced two Summaries of Information, one Source Lead Development Report, 35 Contact Reports and 40 Agent Reports. Further, a total of 1148 manhours were expended on the operation (TAB B).

d. INSCOM-SOD has suggested that a different type program would be better suited to provide the required security assistance for the DLI, i.e., a Dedicated Operations Security Support Program (DOSSP), which does not use confidential sources and which can be readily implemented by the 902d MI Group with existing personnel assets. A DOSSP is described at TAB C. The DOSSP for DLI would be tailored to satisfy local security requirements unique to DLI.

CLASSIFIED BY: [illegible] ICIT OPD 4 FEB 79

REVIEW ON: 5 FEB [illegible]

REASON: [illegible]

1 2 3 4 5 6 7 8

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

EXTENDED BY: [illegible]

Miss M. Brannan/x53501

8 REASON: Para 2-[illegible], DOD 5200.1-R (applicable exemption)

1 2 3 4 5 6 7 8

~~CONFIDENTIAL~~

DAMI-..IC
SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operation Operation (U)

e. The general concept and recommendation to replace LENTIL MONKEY (U) with a DOSSP have been discussed and concurred in by Cdr, SOD, INSCOM, the Commandant and Security Officer at DLI and 902d MI Group.

f. Basis for termination of subject ICIP and replacement by DOSSP is that information obtained from LENTIL MONKEY (U) is general in nature and can be obtained through normal security assistance to installation; INSCOM-SOD's current investigative and reporting authority and most important the lack of a clear definition of physical surveillance which has caused those working the operation much concern (TAB D).

g. By 1st Ind (TAB A) authority granted INSCOM-SOD for termination of LENTIL MONKEY (U).

3. (U) RECOMMENDATION: That 1st Ind (TAB A) be approved and signed.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2350 of 3957

~~CONFIDENTIAL~~

DAMI-CIC (9 Feb 79) 1st Ind
SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operation (U)

HQDA, ACSI, Washington, DC 20310

TO: Commander, US Army Intelligence and Security Command, ATTN: IASO-SA, Fort George G. Meade, MD 20755

(U) Authority to terminate ICIP, LENTIL MONKEY (U) is granted.

wd all incl

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CLASSIFIED BY: INSCOM ICIT
dtd 8 Feb 79
REVIEW ON: 8 Feb 99

857

2

[redacted]

DEPARTMENT OF THE ARMY
US ARMY INTELLIGENCE AND SECURITY COMMAND
FORT GEORGE G. MEADE, MARYLAND 20755

FEB 9 1979

IASO-SA

SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operation (U)

HQDA (DAMI-CIC/Ms Brannan)
WASH DC 20310

1. (U) Submitted herewith is the status report, 1st Quarter, FY 79, for ICIP Operation LENTIL MONKEY (U). During the reporting period the operation produced two Summaries of Information, one Source Lead Development Report, 35 Contact Reports and 40 Agent Reports.

2. (U) LENTIL MONKEY (U), supporting the Defense Language Institute, Foreign Language Center (DLIFLC), Presidio of Monterey, CA, is the only CONUS ICIP being conducted. However, the type information generally developed from the project, and this Command's current investigative and reporting authority, suggest that a different type program would be better suited to provide the required security assistance for DLIFLC. A Dedicated Operations Security Support Program (DOSSP) could effectively replace the ICIP without employing confidential sources and be readily implemented by the 902d Military Intelligence Group with existing personnel assets. At inclosure two is an extract from the USAINSCOM OPSEC Support Procedures Manual which describes the DOSSP.

3. (U) The general concept and recommendations to replace ICIP LENTIL MONKEY (U) with a DOSSP have been discussed and concurred in by the Commandant and Security Officer at DLIFLC. The operational concept would be tailored to satisfy local security requirements unique to DLIFLC.

4. (U) In view of the above, request authority to terminate ICIP LENTIL MONKEY (U). Concurrent with termination of the ICIP, a DOSSP for DLIFLC will be implemented.

WILLIAM I. JENNINGS
Special Assistant (OPS)

2 Incl
as

CLASSIFIED BY CDR INSCOM
REVIEW 8 FEB 99
EXTENDED BY CDR INSCOM
REASON Para 2-301.3.c.

858
858

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

III. TYPES OF SUPPORT

1. GENERAL: This section discusses the various types of OPSEC support that are available within USAINSCOM. It should be noted that operations security is a command responsibility. Therefore, any improvements in the supported commands' OPSEC posture must be accomplished by the supported commander. USAINSCOM is unique in that the present organization integrates many of the counterintelligence/security skills that formerly were assigned to separate Army commands. As such, the Commander, USAINSCOM, has the capability to conduct a multidisciplined security evaluation of a project, activity or facility. With the divergence of skills integral to the USAINSCOM organization, the majority of problem areas that have been historically associated with OPSEC can be addressed, and with the multidisciplined approach, USAINSCOM units are able to assist supported commanders by evaluating their OPSEC posture and recommending means of improvement. This should enable the achievement of a much better security posture. The following paragraphs describe the types of support which USAINSCOM units provide.

2. [redacted] PROGRAM (DOSSP):

2-1. The DOSSP Concept: The DOSSP is a systematic, ongoing, dynamic approach to providing the local commander, operations security officials, project managers and security managers of US Army installations/units/activities/projects with meaningful operations security support in the form of timely, accurate, all source intelligence information pertaining to the real-time, multidisciplined threat posed by hostile intelligence; observed vulnerabilities of the supported element to that threat; and recommendations for appropriate corrective action to enhance operations security. This program is based on a Covering Agent (CA) in an overt continuous role of acquiring information about the supported activity and the threat thereto and providing it to the supported activity in a timely manner, while concurrently recommending practical "fixes" to reduce observed vulnerabilities.

2-2. Responsibilities: Implementation of the Dedicated Operations Security Support Program is the responsibility of each individual field element (RO/FO/Detachment) within the policies provided by the HQ, USAINSCOM. Responsibility for supervision, guidance, and comprehensiveness, rests with the Field Offices, Detachments, and Battalions within their respective areas of responsibility. Group Headquarters will provide guidance, as appropriate, monitor the overall program, acquire and disseminate threat data, and, in the case of certain key projects/activities which stretch beyond local boundaries, will provide centralized management of the overall DOSSP effort.

2-3. Target/Project Selection: Determination of who should be a recipient of DOSSP support is a continuous process of initiative, investigation, and evaluation. Such documents as the ACSI Sensitive Installation and

Page 2353 of 3957

Unit List and other sensitive activities listings are helpful, but not comprehensive. Each field element must do all within its capabilities to insure they are aware of all significant Army activities in their AOR. Once this grasp of the local environment is obtained, prioritization based on available manpower, desires of supported activities, information from intelligence channels, and perceived security sensitivity of the supported activity is made to determine if DOSSP support is appropriate. Security sensitivity is the most important aspect in determining if an activity requires support. Determination of security sensitivity must be based on the importance of the activity to US national security as well as the potential benefit to be derived by a hostile element if they were to obtain details about the activity.

2-4. Covering Agent Functions:

a. Threat: The Covering Agent must be an expert in the threat to the activity he has been detailed to support. This can be accomplished only by thorough study of national threat data, review of periodic intelligence updates, and liaison with local, state, and federal agencies, as well as their foreign equivalents, where appropriate, in order to develop local threat. Refinement of this threat to manageable size is based on a thorough knowledge of the supported command.

b. Knowledge: OPSEC support to an activity is predicated upon a thorough knowledge of that activity. There is no easy way to obtain this knowledge other than extensive research into the organization's mission, functions, and organization. An initial step in this direction is the reading of Army Regulations and Field Manuals pertaining to the activity. Briefings from activity personnel, study of organization and functions manuals, test plans, contingency and operations plans, and related documents are the means for building a comprehensive data base. Even after building this initial base, a systematic plan for obtaining data on an on going basis should be instituted, i.e., daily bulletins, test schedules, briefings, and test plan changes. While expertise in SIGSEC and IMAGERY Security by CI Agents is not required, familiarity with basic concepts is. A primary goal of the USAINSCOM OPSEC Support Program is to provide Army elements a single point of contact for obtaining MI support, be it SIGSEC, IMAGERY Security, or Counterintelligence.

c. Execution: Success in the OPSEC support area is based on the willingness of the covering agent to cast himself in the role of an all source agent and his innovative application of investigative skills in developing threat and vulnerability data, use of deductive reasoning, common sense, and gaining the confidence and respect of the personnel of the supported command. If the confidence of workers at all echelons of the supported command can be gained, their willingness to provide candid assessments of vulnerabilities within the activity will become the Covering Agent's best asset. The CA may know a lot about an activity,

Page 2354 of 3957

but the actual workers know a great deal more. Their experience makes them much more able to relate security weaknesses if they appreciate the threat.

d. Recording: Methodical recording of threat, vulnerabilities, unusual incidents, ideas, and recommendations is essential in building a successful DOSSP. This allows the CA to evaluate comprehensiveness of local hostile intelligence targeting, determine patterns, and fit together isolated incidents, and provides continuity of support as personnel are transferred. ~~A sample workbook is included as figure 1.~~

e. Reporting: Other than the maintenance of workbooks, no formal reporting requirements are imposed on covering agents except in extenuating circumstance of intense, critical stages of support. CA's will keep the chain of command informed of significant activities.

IASO-SA

SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operation (U)

HQDA (DAMI-CIC/Ms Brannan)
WASH DC 20310

1. (U) Submitted herewith is the status report, 1st Quarter, FY 79, for ICIP Operation LENTIL MONKEY (U). During the reporting period the operation produced two Summaries of Information, one Source Lead Development Report, 35 Contact Reports and 40 Agent Reports.

2. (U) LENTIL MONKEY (U), supporting the Defense Language Institute, Foreign Language Center (DLIFLC), Presidio of Monterey, CA, is the only CONUS ICIP being conducted. However, the type information generally developed from the project, and this Command's current investigative and reporting authority, suggest that a different type program would be better suited to provide the required security assistance for DLIFLC. A Dedicated Operations Security Support Program (DOSSP) would effectively replace the ICIP without employing confidential sources and be readily implemented by the 902d Military Intelligence Group with existing personnel assets. At inclosure two is an extract from the USAINSCOM OPSEC Support Procedures Manual which describes the DOSSP.

3. (U) The general concept and recommendations to replace ICIP LENTIL MONKEY (U) with a DOSSP have been discussed and concurred in by the Commandant and Security Officer at DLIFLC. The operational concept would be tailored to satisfy local security requirements unique to DLIFLC.

4. (U) In view of the above, request authority to terminate ICIP LENTIL MONKEY (U). Concurrent with termination of the ICIP, a DOSSP for DLIFLC will be implemented.

2 Incl
as

WILLIAM I. JENNINGS
Special Assistant (OPS)

CLASSIFIED BY CDR INSCOM
REVIEW 8 FEB 99
EXTENDED BY CDR INSCOM
REASON Para 2-301.3.c.

862

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
Headquarters, 902d Military Intelligence Group
Fort George G. Meade, Maryland 20755

902d MI Group Pamphlet
No. 381-3

22 April 1976

Military Intelligence
DIRECT SUPPORT COMPREHENSIVE COUNTERINTELLIGENCE PROGRAM (DSCCP) (U)

1. (U) REFERENCES: See APPENDIX A.

2. (U) PURPOSE: This pamphlet establishes policy, guidance, and standardized procedures for the conduct of all-source, multi-discipline counterintelligence support within the 902d MI Group's area of operation.

3. (U) GENERAL:

a. The Commander, 902d MI Group, has the responsibility to notify commanders of Army installations and units in the group's area of operation when:

(1) Any situation or condition exists that poses a threat to the internal security of that Army element.

(2) Any situation exists that might adversely affect the commander's capability to perform his mission.

(3) Information indicates a probable employement of military resources to counter a threat to the installation.

In order to acquire information of situations or conditions that may pose a threat to the supported commander, field elements must aggressively seek it and not wait for it to be reported through normal sequence of events. This is particularly essential for those units/installations declared to be critical sensitive.

b. The DSCCP is one of a series of graduated intensity counterintelligence programs designed to provide the proper coverage based on the security vulnerability of a particular installation. In relationship to other graduated counterintelligence programs listed in USAINTA Regulation 381-100, the DSCCP would, in certain instances, serve as a means of identifying the need for programs of greater intensity such as SVAs, or SAVEs, or, in other instances, may serve as follow-up support subsequent to such intensified services. It provides the broad spectrum of coverage to include a multi-discipline approach with provisions that the information gathered be reported expeditiously to the responsible commander. The program systematically focuses on providing threat information on the most critical area within the target installation in order to provide the required information to the supported commander.

863

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CLASSIFIED BY: CDR USAINTA
11652
31 DECEMBER 2006

~~CONFIDENTIAL~~

UNCLASSIFIED

c. This program is not synonymous with, nor is it identifiable with, the Internal Counterintelligence Program, Special Operations as defined in FM 30-17A, or the Special Covert Operational Personnel Insertion (SCOPI) as defined in USAINTA Regulation 381-100.

4. (U) CONCEPT:

a. The Direct Support Comprehensive Counterintelligence Program (DSCCP) is an overt, dedicated counterintelligence Security support program with the objective of detecting or anticipating situations and factors from any source (HUMINT/SIGINT/PHOTINT) which are or may become detrimental to the security posture of the supported installation. It employs a Direct Support Special Agent (DSSA) in an overt continuous role of acquiring information and providing it to the commander in a timely manner, while concurrently providing sound recommendations for the reduction and/or elimination of security hazards, vulnerabilities on threats posed by hostile factors.

b. The DSSA obtains the required information from overt investigative activities and from a number and variety of sources and contacts within and in the vicinity of the supported installation. Confidential sources are not utilized. He is fully supported in this task by the intervening echelons at Field Offices, Group, and USAINTA.

c. The DSCCP is a complementary service provided to the supported commander to assist him in improving the security posture of his installation. It is not intended to duplicate nor to usurp the functions and responsibilities of the G-2 or of the Security Manager.

5. (U) RESPONSIBILITIES:

a. The Commander, 902d MI Group, is the approving authority for all DSCCP operations conducted within the group's area of operation.

b. The S3, 902d MI Group is responsible for the following:

(1) Coordinating the selection of units/installations as candidates for DSCCP with the appropriate USAINTA staff elements.

(2) Monitoring DSCCP operations on a continuing basis and periodically informing appropriate USAINTA staff elements of their progress.

(3) Conducting an annual review of each DSCCP operation to determine if it is still necessary and if so, to asure that it remains viable.

c. Field Office Commanders are responsible for the following:

(1) Initiating proposed DSCCP operations for installations located within their areas of operation.

UNCLASSIFIED

(2) Conducting DSCCP operations within their area after approval by the Group Commander and coordination with the supported commanders.

(3) Designating the DSSA for each DSCCP operation, providing follow-up support, and arranging for DSSA clearance and access to compartmented information as required.

(4) Briefing of the supported commanders on the results of DSCCP operation at regular intervals per mutual agreements.

(5) Establish procedures to maintain continuity of the program during absences of the DSSA. When possible, an alternate DSSA will be assigned.

(U) PROCEDURES AND SCOPE:

a. (U) The designation of installations or Army elements as candidates for the DSCCP will be a coordinated action between the Field Office Commander and the supported commander. In some cases, the action may be directed by the Group Commander or USAINTA following a request for special counterintelligence support from a major commander. Regardless of the origin of the request, DSCCP operations will always be conducted with the full consent and knowledge of the supported commander.

b. (U) The selection of installations to be considered for the DSCCP must be discriminatory and based on a genuine need for this manpower intensive service in order to avoid over-commitment of assets. The target installation must be one that is on the ACSI Sensitive Installation and Unit List (SIUL) and one that is a potential or actual target of hostile intelligence services. It is recognized that some field offices and resident offices have numerous sensitive installations in their area, many of which may be categorized as critical. Therefore, it is essential that each FO/RO maintain a listing of these installations in order of priority. In determining the order of priority, factors such as mission sensitivity, and impact of compromise on the security of the United States, etc., will all have to be analyzed and a value judgement must be made based upon actual knowledge of the local conditions, as to which installation has a greater need for special support. The installations heading the list will get first consideration.

c. (U) Proposed concept will be submitted to the Group Commander by letter for approval. The letter will indicate the installation commander's concurrence in the program. The concept will contain a listing of missions, sensitivities, and those internal and external factors which may pose a threat to the installation. Vulnerabilities to human sources,

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

communications intercept, overhead and ground photography, and other appropriate technical/scientific factors will be included if known. This information will be extracted from the target analysis (Para 7a) or from the SVA if one has been completed. The concept must address actions to be taken to detect and counter these threats.

d. (U) Occasional expenditures of ICF in support of this program is authorized and will be processed in compliance with the provisions of AR 381-141 and USAINTA Regulation 381-1. Recurring expenditures will be supported by a formal request for authority if such expenditures are anticipated.

e. (U) The conduct of investigations of and storage of information concerning persons and organizations not affiliated with the Department of Defense are prohibited unless authorized under the provisions of AR 380-13.

7. (U) GUIDELINES:

The actions listed below are considered to be minimum essential for the implementation of this program and are not to be considered as all-encompassing. They should be modified as appropriate to meet situations and needs peculiar to the supported installation. Common sense and experience will likely dictate additional or supplementary means to be employed in order to successfully attain the objective.

a. (U) Conduct a target analysis of the unit/installation to identify, in order of priority, the most critical and vulnerable areas and the multi-discipline threats to which they are exposed. Reference will be made to the following: USAINTA Security Support Bulletins, "THREAT" Manuals, completed SVA/SAVE Reports, CI Survey and Inspection Reports, PM/MP Crime Statistics and Incident Reports, and Communications Security Reports, when available and applicable. The original copy of the analysis will be maintained at the FO/RO level. Appropriate data will be extracted and included in the initial Quarterly Progress Report. The analysis should be reviewed and updated periodically in subsequent Quarterly Progress Reports.

b. (U) Assign a mature, experienced MI Special Agent as a Direct Support Special Agent (DSSA) to provide all-source direct support to the supported commander or his designated representative. The DSSA must become intimately knowledgeable of the supported command's mission, functions, security status and vulnerabilities. As the program will be overt in nature, the DSSA will be known as the primary USAINTA point of contact to all within the supported units/installations. The DSSA will require a TOP SECRET clearance and an SI/SAO special access.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

22 April 1976

c. (U) (~~S~~) The task of the DSSA is to develop a sufficient number of sources of information to provide the best possible coverage to the unit/installation and personnel of the element to detect security vulnerabilities, and make sound recommendations for their reduction and/or elimination. The DSSA should work closely with the security manager to coordinate appropriate matters and to avoid duplication of effort. However, care should be taken not to duplicate or usurp functions and responsibilities rightfully assigned to the security manager.

(1) Human sources of information will include Conventional Sources (Incidental, Casual, and Official) and Liaison Contacts as described in Chapter 6, FM 30-17. Confidential Human Sources will not be utilized. Anonymity may be provided through the provisions of the Privacy Act of 1974 when the source so requests. The association between the DSSA and Conventional Sources or Liaison Contacts will not normally be classified.

(2) Maximum use will also be made of Documentary and Technical/Materiel Sources to include, but not be limited to, SATRAN Messages, Department of the Army intelligence publications and/or bulletins; USAINTA Security Support Bulletins and "THREAT" Manuals; SAVE/SVA reports; Military Police Reports, and Serious Incident Reports. Special attention should be paid to message traffic concerning alerts, advisories or warnings concerning events or situations affecting the supported command.

d. (U) (~~S~~) A contact card file will be maintained at the supporting office to identify conventional sources and liaison contacts. This file will be integrated into the existing contact card file already established for use in the routine mission of the FO/RO. It must be readily available for DSSA personnel at all times. Individual cards will be annotated when the contact is in support of a specific DSCCP operation. LACs will be conducted on casual sources with the results reflected in the contact card file.

e. (U) (~~S~~) Consideration should be given to conducting a systematic review of the dossiers of personnel occupying key and sensitive positions to insure that all such personnel have been properly cleared and to determine if unresolved security matters exist. This issue will be discussed with the supported commander if such a review is deemed necessary, the DSSA should recommend that the commander undertake the action. If the commander requests that the review be conducted by the DSSA, then the matter will be referred to group headquarters where resolution will be made in conjunction with the appropriate USAINTA staff elements. The DSSA may assist the supported command in the review of dossiers but may not take any investigative action to resolve issues. He will advise the supported command to submit requests to USAINTA whenever investigative action is indicated.

f. (U) Reporting of Information:

(1) (U) To the local commander: Information of counterintelligence interest affecting the security posture of the unit/installation will be reported to the supported commander or his designated representative in a timely and complete manner. The information may be reported orally, by Agent Report format, or by Summary of Information (SOI) format, as appropriate. While most items of information will be passed on an oral basis only, there may be certain instances when the commander will desire written reports from the DSSA to be later attached as backup information to his Request for Investigation. In these instances, ARs containing the adverse allegation may be passed when the full consent of the sources of the information has been obtained. However, when a source of information desires confidentiality, to protect the source, the DSSA can then pass in the information only on an oral basis or by SOI format. Regardless of the manner in which the information was passed to the supported command, a report of the information provided to the supported command will be summarized in the Quarterly Progress Report to this headquarters with an indication of the actions taken by the supported command (see Para 7h below).

(2) (U) Other: Information of counterintelligence interest to the intelligence community or other agencies will be reported in accordance with established procedures utilizing normal reporting vehicles such as oral reports, Agent Reports, Spot Reports or Summaries of Information as appropriate. Information reports will be classified according to their content. Such reports will indicate when and to whom the information was passed and what action the command has taken or plans to take. Subject blocks, special warning notices and Privacy Act caveats, etc., will be those utilized in established investigative activity procedures. (AR 381-20 and USAINTA Reg 381-100).

(3) (U) When fragmentary information of counterintelligence interest is initially surfaced, the DSSA will attempt to determine whether or not the information is credible prior to reporting it to the supported Commander. Preliminary checks may be made only to the extent authorized in para 3-6, USAINTA Reg 380-100. Should this prove to be insufficient to establish the credibility of the information, the DSSA will then refer the matter to group headquarters for coordination with USAINTA. Credible information concerning a member of the supported command should be used to support a formal Request for Investigation to USAINTA.

(4) (U) The supported commander or his designated representative will be orally briefed on all items of threat information concerning his command, or be provided written reports as appropriate. Examples of the types of threat information include satellite overflights, Soviet bloc

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

country commercial overflights, communications intercept capabilities/ vulnerabilities from air, ground or water, personnel security vulnerabilities and others as listed below. Depending upon the source of the information and its previous distribution within the intelligence community, the information may be passed laterally or to higher echelons in accordance with established reporting requirements. All information gleaned from the operation will be briefly summarized in the Quarterly Progress Report.

g. (U) A list of EEI will be developed by the DSSA in order to focus specialized coverage on the specific requirements of the local situation and the supported commander. Examples of EEI are attached at APPENDIX B. It should be noted that the EEI contain items of specific interest to the supported commander and other items that pertain to lead material for use by the US Army intelligence community. A copy of the developed EEI list will be attached to the initial Quarterly Progress Report.

h. (U) A Quarterly Status Report in the format contained at APPENDIX C will be submitted to Group Headquarters no later than 10 working days following each calendar quarter. The first report will be due after the completion of the first full quarter of operation after initiation. The report should reflect the developments and progress of the operation, problems encountered, information obtained during the reporting period, future actions contemplated and lessons learned or recommendations as appropriate.

8. (U) Reducing Vulnerabilities: Once a security weakness or hazard has been identified, the DSSA then has the responsibility to make sound recommendations for corrective actions to be taken by the supported commander to reduce or eliminate them. In making these recommendations, the DSSA must use good judgement based upon his background and experience, cost verses absolute security, knowledge of similar instances, common sense, and an intimate knowledge of those technical and/or specialized security services and/or investigations available to the supported commander from other USAINTA elements. Each corrective action must be viable, made on its own merit, be practical and be within the capability of the supported command. USAINTA Security Support Bulletins contain excellent examples of "quick-fix" solutions. In those rare instances when corrective actions cannot be accomplished due to cost restrictions or limited resources available to the command, the commander must be made aware of, and accept the possible security risk(s) involved.

9. (U) It is visualized that situations, incidents or conditions may be uncovered which could have serious deleterious effect on the security

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

posture of the installation and could not be resolved through the techniques of the DSCCP. In these cases, the matter should be expeditiously referred to Group Headquarters where it will be brought to USAINTA's attention for resolution, considering ICIPs, SCOPIs, Special Operations, or other more sophisticated methods.

10. (U) The application of the DSCCP to a supported installation is a special effort and will probably require the services of the DSSA on a near full time basis with additional manhours of support furnished by FO and Group Headquarters. Consequently, FO Commanders and RO SAICs should proceed with caution in offering this service to commanders to prevent over-extending their resources. Nevertheless, the DSSA approach of the DSCCP is sound and could well be applied to other installations in the area of operations but to a much lesser degree than in the DSCCP. This should be done as a routine matter and no formal approval is required. Thus, one MI Special Agent could become the DSSA to several installations of lower priority.

11. (U) This pamphlet provides policy and guidance for 902d MI Group personnel in the conduct of all-source, multi-discipline counterintelligence support within the area of responsibility of the 902d MI Group. It complements existing US Army Regulations, USAINTA Regulations and USAINTA policy and guidance. Nothing in this pamphlet shall be construed to contravene or to be in conflict with existing US Army or USAINTA policy. In the event that possible conflicts may arise, the provisions of existing US Army and/or USAINTA policy will apply. Any questions pertaining to possible conflict of the provisions of this pamphlet with existing policy will be addressed to this headquarters, ATTN: MIIA-GPB-AC, for further staffing with appropriate USAINTA staff elements. Comments and recommendations are encouraged and should be submitted on DA Form 2028 (Recommended Changes to Publications) to this headquarters for consideration and staffing.

HASSEL L. PARKER
Colonel, MI
Commanding

3 Incl
Appendix A - References
Appendix B - EEI
Appendix C - Quarterly Report

DISTRIBUTION:
B plus
10-S3, 902d MI Group
1-MIIA-SO
1-DARCOM LNO
1-USASA LNO
1-FORSCOM LNO
1-Cdr, 525th MI Group
1-MIIA-ADM
2-MIIA-CI
1-MIIA-IN
1-USACC LNO
1-HSC LNO
1-TRADOC LNO
1-Cdr, 901st MI Det

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

Page 2364 of 3957

UNCLASSIFIED

APPENDIX A TO 902D MI GROUP PAMPHLET 381-3

REFERENCES

1. Army Regulations:

a. AR 18-7, Army Information and Data Systems, Data Processing Installation Management, Procedures, and Standards.

b. AR 190-13, the Army Physical Security Program

c. AR 340-21, Office Management, The Army Privacy Program.

d. AR 380-5, Security, Department of the Army Supplement to DOD 5200.1-R (DODISPR).

e. (C) AR 380-10, Department of the Army Policy for Disclosure of Military Information to Foreign Governments (U).

f. AR 380-13, Security, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations.

g. AR 380-150, Access to and Dissemination of Restricted Data.

h. (C) AR 381-3, Signals Intelligence (SIGINT) (U).

i. AR 381-11, Military Intelligence, Threat Analysis.

j. AR 381-12, Subversion and Espionage Directed Against US Army and Deliberate Security Violations (Short Title: SAEDA).

k. (C) AR 381-12-1, Processing of SAEDA Incidents (U).

l. (C) AR 381-14, Counterintelligence - Technical Surveillance Countermeasures (U).

m. (C) AR 381-15, Military Intelligence, Domestic Exploitation Program (U)

n. AR 381-20, Military Intelligence, US Army Counterintelligence (CI) Activities.

o. (C) AR 381-141, Military Intelligence, Provisions for Administration, Supervision, Control and use of Intelligence Contingency Funds (ICF) (U)

UNCLASSIFIED

Page 2365 of 3957

UNCLASSIFIED

p. (C) AR 530-1, Operational Security (U).

q. (C) AR 530-2, Communications Security (U).

r. (C) AR 530-3, Electronics Security (U).

s. (C) AR 530-4, Control of Compromising Emanations (U).

t. AR 604-5, Clearance of Personnel for Access to Classified Defense Information and Material.

u. AR 604-10, Military Personnel Security Program.

2. DOD Publications:

a. DOD 5200.1-R, Information Security Program Regulation.

b. (SI) DOD 5200.1F (M-2) Special Security Manual

c. DOD 5200.28-M, ADP Security Manual

d. DOD 5220-22-M, Industrial Security Manual for Safeguarding Classified Information.

e. DIAM 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities.

3. Field Manuals:

a. FM 19-30, Physical Security.

b. FM 30-17, Counterintelligence Operations.

4. ACSI, DA Publications.

a. OACSI Sensitive Installation and Unit List (SIUL).

b. AARGRAMs (as applicable).

5. USAINTA Publications.

a. USAINTA Reg 10-2, Organization and Functions Manual.

b. (C) USAINTA Reg 381-1, ICF (U)

c. USAINTA Reg 381-100, Counterintelligence Activities and Procedures.

d. (S) USAINTA Security Support Bulletins (U).

UNCLASSIFIED

UNCLASSIFIED

e. (S) USAINTA Security Support Program Manual "THREAT" (U)

f. (C) USAINTA Security Support Program Manual "Operations" (U)

g. USAINTA Security Support Program Computer Security Manual.

h. USAINTA Daily Operational Reports (as applicable).

i. USAINTA Supplement to AR 380-5.

6. 902d MI Group Publications:

a. (S) 902d MI Group Pamphlet 380-2, Security, SATRAN Reports (U).

b. 902d MI Group Daily Operational Reports (as applicable).

UNCLASSIFIED

~~CONFIDENTIAL~~

APPENDIX B TO 902D MI GROUP PAMPHLET 381-3

ESSENTIAL ELEMENTS OF INFORMATION (EEI)

1. (U) GENERAL: In devising EEI applicable to the supported installation, each one of the multi-discipline threats must be examined in conjunction with the mission and situation of the particular target. The actual or potential vulnerabilities thereby conceived become EEI affecting the supported installation. Since each installation has its own specific situation, it is imperative that the DSSA work very closely with a representative of the supported installation in order to arrive at an EEI listing tailored to the specific needs of the command. The references listed at APPENDIX A provide background information and guidance in devising EEI. Many of the areas covered by these references, which heretofore have been of little concern to the Special Agent, are now essential elements of knowledge to the DSSA if he is to successfully accomplish his mission under the DSCCP concept. This is particularly necessary in the areas of SIGINT, PHOTINT, OPSEC and Computer Security. Listed below are sample EEI for each category. These EEI are basic and are only a partial listing provided as an aid in developing a list peculiar to the supported command. Some of the items may not be germane to every DSSA but are included as nuclei for possible development of new or related ideas. The final EEI list prepared by the DSSA should include the source or sources that can provide the required information.

2. (U) HUMINT: The following elements are those normally attributed to collection or exploitation by human intelligence sources. The information will usually be obtained by various HUMINT sources, personal observation by the DSSA and liaison contacts:

a. HOIS subscriptions or regular acquisition of local and post newspapers and periodicals. Sources: LNO contacts and USAINTA.

b. Deliberate compromise of classified information or unauthorized release of military information to representatives of foreign governments (ARs 380-5, 380-10, 381-12 and 381-12-1)

c. Public information releases and local newspaper articles revealing unclassified but useful (to HOIS) information regarding the command.

d. Theft, suspected theft, or unauthorized reproduction of classified documents and or material.

e. Reported or suspected blackmail or coercion of individuals employed within the supported command.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

(U) CONFIDENTIAL

f. Actual or attempted physical breaches of restricted area perimeter security, external or internal.

g. Early detection of persons whose activities and/or character weaknesses may render them vulnerable to hostile intelligence exploitation. Suitability factors may include:

(1) Excessive indebtedness or recurring financial difficulties.

(2) Unexplained affluence.

(3) Conduct rendering the individual vulnerable to pressure, such as homosexual, criminal or immoral acts.

(4) Excessive use of alcoholic beverages or improper use of drugs or narcotics.

(5) Mental or emotional instability or history thereof.

(6) Those who attempt to commit suicide.

(7) Drastic changes in behavior to indicate possible unexplained pressures being brought to bear.

h. Personnel who regularly and voluntarily work during non-duty hours when unobserved access to classified data is possible.

i. Sudden unexplained or inadequately explained absences from work.

j. Membership in, or association with members of organizations constituting a local threat against the US Army as defined in AR 380-13.

k. Unsolicited correspondence from individuals, organizations or addressees known to be a threat to the US Army.

l. Allegations or denunciations of espionage or sabotage on the part of sensitive installation personnel.

3. (U) PHOTINT: This pertains to intelligence obtained by means of photography, mainly through HOIS satellites or HOIS commercial aircraft. Also included must be threats posed by hand-held cameras operated from low-flying private aircraft and ground-level photography conducted from areas outside the perimeter of the installation. Photography from seaborne platforms should be considered at installations located near international waters. Sources of information for this type of data are documentary sources such as SATRAN messages, schedules of tests, operations and troop movements, as well as results of liaison contacts and personal observations. Some sample EEI are as follows:

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

Page 2369 of 3957

(U) CONFIDENTIAL

a. Following activities during periods of scheduled overflights by HOIS satellites and commercial aircraft:

(1) Large and significant training exercises.

(2) Testing of equipment and/or techniques in the open.

(3) Uncamouflaged new or sensitive equipment.

(4) Other significant movements and activities.

(5) Concentration of transportation equipment, i.e., transports, etc.

b. Build up of major item stockpiles in the open.

c. Gradual build up of facilities at a test site.

d. Repeated violation of air restricted zones by commercial/private planes.

e. Appearance of private aircraft during classified, or significant tests/demonstrations.

f. Placing, operating or testing of new, significant or classified equipment in areas exposed to the public.

g. Sudden appearance of camera-carrying "tourists" in the vicinity, coinciding with the scheduling of new, unusual and/or classified activity.

h. Unobstructed windows and apertures in areas where classified matters are handled, permitting observation and photography from uncontrolled areas.

i. Foreign vessels, particularly from East Bloc Countries, appearing off-coast of installations near international waters.

4. (U) SIGINT: Signal intelligence is derived from the intercept and analysis of communications, COMINT, and from communications electromagnetic radiations, ELINT. HOIS SIGINT collection against US facilities is accomplished from air-borne, sea-borne, and land-based platforms. HOIS capabilities in this field are described in the USAINTA Threat Manual and additional information as to specific threat to the supported installation may be found in reports of SVAs and SAVEs and/or requested from USAINTA. The field of SIGINT is a very complex and specialized one. Adequate protection of a command/installation from HOIS SIGINT collection requires

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

[redacted]

the application of Signal Security (SIGSEC) which includes Communications Security (COMSEC), and Electronic Security (ELSEC). COMSEC measures are applied to telecommunications systems and has four components; crypto security, physical security, transmission security and emmission security. ELSEC pertains to protective measures applied to electromagnetic radiation of non-communications equipment and systems to prevent the interception, analysis or exploitation of those radiations by foreign intelligence. The DSSA must become sufficiently familiar with the above subjects in order to recognize vulnerabilities, and know when to recommend a request for technical assistance. References 1h, 1, p, q, r, s, and 5d and e in APPENDIX A will provide additional information. Furthermore, the DSSA must work closely with the staff element having responsiblity for SIGSEC of the supported installation. The EEI selected will be the type that can be fulfilled by human sources, preferably located in communication/electronics work areas. Some EEI common to SIGINT are located in para 1c, Appendix to AR 530-1. Other sample EEI follow:

a. Conducting tests on new or sensitive radars and other non-communication emmitters within range of land based, air-borne or sea-borne HOIS ELINT platforms.

b. Installing and operating electrically operated, information-processing equipment which handles classified information without the application of compromising emanations control measures.

c. Poor telephone security to include:

(1) Discussion of classified matters over Autovon and commercial telephone systems.

(2) Discussions of upcoming events which can provide tipoffs to classified activities.

(3) Use of double talk in reference to classified messages.

(4) Reading/quoting verbatim portions of classified matters.

5. (U) OTHER EEI: The following items are of interest to the US Army intelligence community and will be forwarded to this headquarters by Agent Report format for appropriate action. A statement in Agents Notes will indicate if and how the information has been reported through other appropriate channels. As the information will be passed to USAINTA for possible exploitation bt the Special Operations Detachment or the Director of Operations as appropriate, the Agent Reports will be classified CONFIDENTIAL-NO FOREIGN DISSEM. Normally this information is not passed to the local commander other than to insure that other proper reporting

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

procedures are being followed by the command.

a. Identification and extent of foreign contacts of military and DOD civilian personnel, with emphasis on Soviet bloc countries.

b. Intended foreign travel of military or DOD civilian personnel to Soviet bloc countries or attendance at social or official functions at which Soviet bloc countries are present.

c. Foreign business or professional connections and the extent thereof of military and DOD civilian personnel and their families, with emphasis on Soviet bloc countries.

d. Solicitation by foreign national or organizations of personal or official information through official or unofficial channels.

e. Invitations by non-US Government organizations or individuals to members of the supported command to Participate in conferences or symposia or to submit papers for publications in professional journals on activities related to their government employment.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

APPENDIX C TO 902D MI GROUP PAMPHLET 381-3

DSCCP QUARTERLY PROGRESS REPORT

1. (U) IDENTIFY: (Name of 902d MI Group Field Element providing support).

2. (U) SUPPORTED COMMAND: (The activity(ies) receiving the support and the major command(s) involved.)

3. ( ) TARGET ANALYSIS: (In the initial report summarize the results of target analyses conducted for all activities, installations, or separate elements designated and included in the program, by order of priority of support. Subordinate elements large enough to be designated sub-targets will be listed in subparagraphs. In subsequent reports, indicate only changes as they occur.)

4. ( ) QUARTERLY BRIEFING OF SUPPORTED COMMAND

a. Circumstances: In brief narrative form, cite date(s), identities of all persons present, and subjects discussed and results of the briefing(s).

b. Recapitulation of Operational Progress During the Period: In as many subparagraphs as may be required, cite significant developments as pertain to development of the program, improvements in target coverage, and any operational readjustments made during the period. In citing specific items of interest, identify each by making reference to the appropriate reports made during the reporting period which contained details of the topic discussed with the commanders, if applicable.

c. Significant Counterintelligence Information Developed: In as many subparagraphs as may be required, cite identities of personalities, incidents, or groups discussed with reference to the report previously submitted.

5. ( ) INFORMATION SUBMITTED:

a. To the local commander and actions implemented or taken as a result:

Subject	Type Information Developed	Action Taken	Date of Action

b. To the intelligence community;

Subject	Type Information Developed	To whom reported

6. ( ) COMMENTS, REMARKS AND RECOMMENDATIONS:

In this paragraph, indicate any general remarks or indications of special

879

Page 2373 of 3957

interest shown by the supported command that are not covered in above paragraphs. These remarks should reflect the commander's assessment of the viability of the program, whether it is meeting the objectives and achievements as he sees them, and any problems and/or recommendations. Also indicated the extent with which the commander or his representative has cooperated with the FO/RO and/or this group and any pertinent remarks which could serve to improve the DSCCP support to the command. Where problem areas have been encountered, findings and recommended solutions will be provided. Lessons learned should be included to assist in the planning and implementation of other operations. A statement will be entered as to whether any information concerning non-affiliated DOD civilians or organizations was reported (AR 380-13). If affirmative, reference specific report or attach copy. Utilize subparagraphs to explain or amplify information or data reported.

NOTE: Classify each paragraph according to its content. Because of the distribution of this report, care must be taken to insure that the contents of the report do not reveal SI/SAO access material. An example of this would be to include the Statement "three items of PHOTINT information, reference messages_____,_____, and_____, were received and passed to the supported command. Appropriate actions were taken", without revealing the SI/SAO information contained within the reference messages.

880

C2

(U) ~~CONFIDENTIAL~~

2 January 1979

MEMORANDUM FOR DIRECTOR, COUNTERINTELLIGENCE

SUBJECT: Lentil Monkey (U) ICIP (U)

1. Attached at TAB A is Operation Plan for ICIP, Lentil Monkey (U), located at the Defense Language Institute (DLI), Presidio of Monterey, CA.

2. Attached at TAB B are the Quarterly Summaries on Lentil Monkey (U) for FY 78.

3. Attached at TAB C is an FBI report on an individual who [redacted] in 1977 being considered for employment at DLI.

4. In December 1978, discussion with SOD personnel concerning this ICIP revealed that subject ICIP would be terminated in early 1979. As you know, Bob Wright has an action before "higher authority" regarding a change in the definition of surveillance. My concern has been whether or not ICIP violates the definition used in the E.O. The DOD IG appears to be satisfied that it does not. With the termination of Lentil Monkey the question from my concern becomes academic. According to SOD, Lentil Monkey (U) will be replaced with another plan that will be administered by the 902d MIG and will eliminate the area of concern.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

~~CONFIDENTIAL~~

88

OPERATION PLAN LENTIL MONKEY (U) 25 January 1978

INTERNAL COUNTERINTELLIGENCE PROGRAM (ICIP)

1. (U) Mission, Background, Objectives, & Base of Operations

a. Mission. To provide counterintelligence support, security support and operations security support to the Defense Language Institute (DLI), located at the Presidio of Monterey, CA.

b. Background. Ref b designated the Secretary of the Army as Executive Agent for the Defense Language Program and tasked the Department of the Army to control the program. Military Intelligence received the above stated mission. The Commandant, DLI requested by ref j, the implementation of an Aggressive Counterintelligence Program. This program is now known as an Internal Counterintelligence Program (ICIP). A target vulnerability analysis, conducted by the 115th MI Group in March 1968, indicated the request was fully justified. Additionally, information contained in ref h continues to support this determination.

c. Objectives.

(1) To attempt to identify as early as possible specific hostile intelligence collection operations or threats to the DLI to allow neutralization or exploitation of offensive counterintelligence operations of such hostile threats and/or operations.

(2) To identify those activities, practices and/or personnel within DLI that pose potential or existent security threats and to neutralize threats so identified. Specific target areas are identified by priority in Annex B.

d. Base of DLI Operations.

(1) Project Case Officer (PCO): A day office is located at the US Navy Post Graduate School in proximity to, but, physically separated from the Presidio of Monterey.

(2) Project Liaison Officer (PLO): Presidio of Monterey.

2. (U) Personnel:

a. Project Case Officer.

b. Project Liaison Officer.

Classified by CDR, USAINSCOM
EXEMPT FROM [illegible] OF EXECUTIVE ORDER 11652
SCHEDULE OF [illegible] EXEMPTION CATEGORY 2
DECLASSIFY ON 31 December 2008

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

882

CONFIDENTIAL

OPERATION PLAN LENTIL MONKEY (U)

c. Sources: To be recruited as available from members of the student body, staff and faculty of DLI.

d. Control Personnel: See Annex C, (Knowledgeability List).

3. (C) Cover and Documentation:

a. b1

b. b1

c. b1

d. b1

4. (U) Execution:

a. Concept of Operations:

(1) The ICIP operation will be implemented by the coordinated utilization of overt liaison contacts, conventional sources and confidential sources. Priority of source recruitment will be in accordance with the target priorities established in Annex B and based on expressed or demonstrated needs of the DLI Commandant. The PLO will constantly spot, assess and recruit potential Confidential Sources for utilization in priority target areas.

(2) Each individual and source involved in the conduct or control of this ICIP will be briefed on and comply with current policies and constraints pertaining to counterintelligence operations and other activities as they concern persons and organizations not affiliated with Department of Defense (references a, c, i). Upon recruitment (or earlier if deemed appropriate), each Confidential Source will be briefed on these constraints and will sign a certificate to this effect. A copy of the certificate will be included in the source data forwarded to higher Headquarters.

OPERATION PLAN LENTIL MONKEY (U)

(3) The scope of this operation will not be expanded to cover off-post targets not affiliated with the Department of Defense without prior approval in compliance with reference c.

(4) Activities and duties of the PCO and PLO are contained in reference f. The PLO, in exceptional cases, based on the nature of the DLI environment, may serve as a PCO for selected Confidential Sources.

b. Essential Elements of Information (EEI): Annex D.

c. Target Area: Annex B.

d. Implementation by Phases:

(1) Overt phase is on-going as approved and validated by DA ACSI Letter dated 14 July 1976, subject: Internal Counterintelligence Program (ICIP) (U). The overt phase is a primary responsibility of the PLO.

(2) The objectives of the overt phase are:

(a) Spotting and assessing potential Confidential Sources.

(b) Establishment and maintenance of a professional and cooperative relationship with the DLI Commandant and his staff, with emphasis on the DLI Security Officer and other personnel in key positions involving priority targets.

(c) Further apprising the DLI Commandant of the ICIP, its objectives, capabilities and limitations.

(d) Establishment and maintenance of a liaison link through the DLI Security Officer with the DLI Commandant to facilitate the passage of perishable and critical information.

(e) Accomplishment of selected local investigative requirements relative to both overt and other sources.

(f) Development and maintenance of liaison contacts with local and Federal law enforcement, security, and investigative personnel.

(3) Covert Phase.

(a) The covert phase is initiated upon the recruitment of a Confidential Source and will continue for the duration of the utilization of such source, or until the operation is terminated.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2378 of 3957

OPERATION PLAN LENTIL MONKEY (U)

(b) The objectives of the covert phase, which are the responsibility of the PCO's are:

(1) Development and timely reporting of credible information relating to the detection, neutralization or exploitation of factors or individuals who pose a direct threat to the security of DLI and the United States.

(2) Training and exploitation of in-place Confidential Sources who have placement and access within the selected priority target areas, and who are capable of developing and reporting information not available through overt means.

e. Security Considerations: All personnel will comply with the administrative and operational security procedures set forth in reference f.

f. Technical Requirements: Utilization of technical equipment is not anticipated. If, during the course of the operation, such a requirement develops, supplementary correspondence will be initiated.

5. (C) Communications:

a. b1

b. b1

c. b1

d. b1

6. (C) Training:

a. b1

OPERATION PLAN LENTIL MONKEY (U)

b. b1

7. (C) Finances and Logistics:

a. b1

b. b1

8. (U) Termination:

a. Termination With and Without Prejudice: Sources recruited for these operations will be terminated when their use to the operation ceases, they show indications of insecure practices which could compromise the operation, they are no longer amenable to control, or the operation is terminated. Circumstances under which termination is effected will determine whether termination is with or without prejudice. Security debriefing and severance statements will be obtained at the time of termination when practicable.

b. Commitments: The only commitments to be made to Sources will be assurance of protection of their identity and of reimbursement of expenses incurred at the direction of the PCO or PLO.

c. Knowledgeability: Knowledgeability of Confidential Sources will be limited to names of the PCO and PLO; vehicles and license plates; meeting sites; training, EEI and other modus operandi acquired by a Source in the course of his utilization in an operation. Knowledgeability of Conventional Sources, witting, or unwitting, will generally be less than that of Confidential Sources; however, they will be met and debriefed whenever practical, with the same operational techniques and procedures utilized with Confidential Sources.

9. (U) Coordination and Liaison:

Coordination of this operation has been effected with the Commandant, DII,

886
886

CONFIDENTIAL

Page 2380 of 3957

and appropriate staff officers. Liaison will continue to be conducted with these officials. Liaison has also been established and maintained with appropriate local and Federal law enforcement and investigative agencies.

10. (U) Reports:

a. Source administration and operational reports will be submitted in accordance with USAINTA Regulation 381-100 & 1 and FM 30-17A. The following reports are required.

(1) Quarterly Status Report (See example in USAINTA Regulation 381-100-1, Appendix A)

(2) Lead Development Report (See example in FM 30-17A, Appendix D)

(3) Contact Report (See example in FM 30-17A, Appendix D)

(4) Agent Report (See example in USAINTA Regulation 381-100, Appendix A)

b. Quarterly status reports will be submitted so as to arrive at Special Operations Detachment, HQ, USAINSCOM, NLT three working days after the end of the reporting period.

ANNEX: A - References

B - Target List and Priorities

C - Knowledgeability List

D - Essential Elements of Information

E - Finance and Logistics

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

887
887

ANNEX A: References

a. Executive Order 11905, United States Foreign Intelligence Activities (U), 18 Feb 76.

b. DOD Directive 5160-41, dated 5 Oct 68, Subject: Defense Language Program.

c. AR 380-13, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations (U), 30 Sep 74.

d. AR 381-141, Provisions for Administration, Supervision, Control and Use of Intelligence Contingency Funds (U), 7 Jul 76.

e. DA Letter, ACSI-CIPR, dated 8 Oct 69, Subject: Counterintelligence Support of Defense Language Institute (U).

f. USAINTC Regulation 381-100-1, Counterintelligence Special Operations (U), dated 8 Jun 74.

g. USAINTC Regulation 381-1, Provisions for Administration, Supervision, Control and Use of Intelligence Contingency Funds (U), 24 Aug 74.

h. USAINTA Report, A Security Incident Review, Defense Language Institute (U), dated Jan 1977.

i. Letter, ICDO-OP, dated 12 Apr 74, Subject: Umbrella OPLAN (U).

j. Letter, CDT, DLIWC, dated 11 Sep 67, Subject: Request for Aggressive Counterintelligence Support (U), with 1st Indorsement, DLI, dated 14 Sep 67.

k. Letter, MIIA-GPA-CO, dated 6 Jan 77, Subject: Administration of Internal Counterintelligence Program (U).

887

888

Page 2382 of 3957

ANNEX B: Target Areas (U)

1(U)~~(C)~~ Priority I targets linclude the following DLI Language Departments:

a. Russian

b. Czech

c. Polish

d. Hungarian

e. Romanian

f. Bulgarian

g. Serbo-Croatian

h. Chinese - Cantonese

i. Chinese - Mandarin

j. Albanian

2(U)~~(C)~~ Priority II targets include the following DLI Language Departments:

a. Arabic

b. French

c. German

d. Italian

e. Indonesian

f. Korean

g. Persian

h. Portugese

i. Spanish

j. Thai

k. Turkish

l. Vietnamese

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

889
889

~~CONFIDENTIAL~~

Page 2383 of 3957

ANNEX B: Target Areas (U)

3. (U) ~~(C)~~ Priority III targets include the following Non-Academic Directorates:

a. Directorate of Support

b. Directorate of Training

c. Directorate of Evaluation

d. Directorate of Training Development

e. ~~Nonresident~~ Training

f. Troop Command

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

890
890

CONFIDENTIAL

Page 2384 of 3957

ANNEX C: Knowledgeability List (U)

SPECIFIC KNOWLEDGEABILITY ROSTER (26 August 1977)*

ICIP LENTIL MONKEY (U)

NAME	POSITION	DATE OF ACCESS
LTC Russell E. Cooley	Commander	Jul 1977
LTC Joseph E. Hawkins	Executive Officer	Nov 1976
MAJ Leonard A. Kostelnik	S2/3	Jul 1977
MAJ Carl L. Biemiller	Chief Operations Branch	Aug 1977
SSG Richard L. McCauley	Operations Branch	Feb 1977
Jeremy H. Hughes	PLO	Apr 1974
Ronald M. Olson	PCO	Feb 1976
John Carstens	PCO	Aug 1974
LTC Arthur D. McQueen	Special Assistant	Sep 1974

* All Personnel Listed Are Assigned to the 93D MI BN (Prov)

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

891
891

CONFIDENTIAL

Page 2385 of 3957

~~SECRET~~

GENERAL KNOWLEDGEABILITY ROSTER (1 AUG 7)

ICIP LENTIL MONKEY (U)

NAME	POSITION	DATE OF ACCESS
COL Samuel L. Stapleton	Commandant, Defense Language Institute (DLI)	Sep 1975
COL R. Jaanson	Deputy Commandant, DLI	Jul 1977
LTC R. P. Kelly	XO, DLI	Sep 1977
LTC P. R. Burger, Jr.	Director, Support, DLI	Sep 1975
LTC Waldo Webb	Security Officer, DLI	Nov 1977
James R. Green	Security Officer, DLI	Jan 1974
MAJ William A. Sensenderfer	Chief, OPSEC Team, 93d MI Bn (Prov)	Jul 1977
CPT Van B. Lowry, Jr.	Adjutant, 93d MI Bn (Prov)	Sep 1975
CPT Brendon A. Xiques	CDR, Ft Ord Field Office	Aug 1975
Jesse Boone	S/A Ft Ord FO	Jan 1975
Max Dolan	S/A Ft Ord FO	Jan 1975
b1 Per FBI		Jul 1974
b1 Per FBI		Sep 1976
MG H. R. Aaron	ACSI, DA	Jul 1977
MAJ (FNU) Morgan	ACSI, DA Staff Officer	Jul 1977
CPT Edward F. Alves	S-4, 93d MI Bn (Prov)	Jul 1977
CPT Ashton Grimes	CDR, TSCM Team	Jul 1977
CPT John F. Roe	Action Officer, S7-S 93d MI Bn (Prov)	Jul 1977
CPT Fred A. Kinnan	TEMPEST Officer, 93d MI Bn (Prov)	Jul 1977

DECLASSIFIED SECRET
ON 20 MAR 1998
BY USAINSCOM FOI/PA
Auth Para 4-102, DOD 5200.1R

~~SECRET~~ 892

~~CONFIDENTIAL~~

Page 2386 of 3957

ANNEX D: Essential Elements of Information

(U) Consistent with the stated mission and objectives of JCIP LENTIL MONKEY, the following Essential Elements of Information (EEI) are established. These EEI apply to all military and DOD civilian personnel assigned to or associated with DLI activities to include students, permanent party, staff and faculty, and visitors:

1. Identification and extent of foreign contacts and business or professional connections, particularly those with communist bloc countries.

2. Foreign travel, intended or completed, to communist bloc countries; recurring trips to Mexico and Canada.

3. Attendance at social and official functions at which communist bloc country personnel are present.

4. Solicitation by foreign nationals or organizations of official or personal information through either official or non-official channels.

5. Identification of personnel corresponding or associating with communist bloc embassies or receiving unsolicited correspondence from individuals, organizations or addresses known to be a threat to the US Army.

6. Identification of personnel whose activities and character weaknesses render them potentially vulnerable to pressure, blackmail, coercion, and exploitation by foreign intelligence. Such information includes:

a. Excessive indebtedness or recurring financial difficulties.

b. Unexplained affluence inconsistent with income.

c. Commitment or solicitation to commit immoral or illegal acts in CONUS or in foreign countries where such acts could be considered illegal.

d. Drastic changes in or acts of personal behavior to indicate possible unexplained pressures being brought to bear.

e. Excessive use of alcoholic beverages or improper use or abuse of drugs or narcotics.

f. Mental or emotional instability or illness of sufficient seriousness to affect materially the individual's duty performance.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

CONFIDENTIAL

Page 2387 of 3957

7. Identification of violations of established installation and/or personnel security policy and procedures.

8. Identification of individuals displaying unusual interest in anothers personal and military background and future assignment; attempting to identify individuals on orders to classified and foreign command and general staff assignments; photographing apparently selected individuals.

9. Allegations or denunciations of espionage or sabotage activities.

10. Sudden unexplained or inadequately explained absences from work.

11. Identification of unofficial visitors to DLI.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

894

~~CONFIDENTIAL~~

Page 2388 of 3957

Page 2389 of 3957

[redacted]

LENTIL MONKEY - ICIP - DLI

895

TYPE RPT	1ST QUARTER	2nd QUARTER	3rd QUARTER	4th QUARTER	TOTALS	
CONTACT	32	41	34	43	150	
ORAL	48	49	42	55	194	
AGENT	109	112	118	65	404	749
MANHOURS EXPENDED	1,320	1448	1301	1142	5,211	

[redacted]

Page 2389 of 3957

(U)

(C) LENTIL MONKEY: (QSR, 1st QTR FY 78)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Seventeen.

c. Information Obtained or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained:

(1) During the quarter, sources continued to report contacts between Russian Language Department (RLD) instructors and friends and relatives in the USSR. In addition to written correspondence, packages containing clothing, books and other articles have been sent to individuals in the USSR: sometimes through third parties. One RLD instructor has received both standard and military dictionaries from a friend in the USSR, to include a copy of the Warsaw Pact Military Terminology. An RLD instructor has sent over $4,000, in increments over a period of several years, to friends and relatives in the USSR. The instructor refused to reveal the method/system used to transmit the money that he had borrowed while in the USSR in order to emigrate to the US. An RLD instructor who visited the USSR during the quarter was questioned while there by an individual who identified himself as a Soviet Army officer. The instructor was asked for the names of DLI personnel, students' branches of service, and the purpose of their language studies. The instructor reported that she had refused to answer the questions.

(2) A Polish Language Department (PLD) instructor obtained a visa from the Polish Embassy in London while on leave in July 1977 and proceeded to visit Poland. The instructor failed to comply with DLI regulations in that he did not report his intent to visit a Communist Bloc country and receive the required briefing from the DLI Security Officer. This instructor has taken past trips to Poland, but had always complied with DLI regulations. A PLD instructor who has been employed at DLI since 1955 is reportedly planning to retire in the near future and move to Poland. He stated he would be able to live better in Poland because of lower living costs. This same instructor had visited Poland last May, and had photographed DLI students from the Polish and Serbo-Croatin Language Departments during a class picnic in November 1977. A PLD instructor who last visited Poland in June 1977, was visited by friends, a man and woman, from Poland during late September, early October. The instructor took his guests to the Ft Ord Officers' Club on 1 October 1977.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2390 of 3957

(3) A female instructor of the Serbo-Croatin Language Department (SCLD) has developed a close association with a US Army Captain, and former DLI student, now attending the Yugoslavian Staff College. Since his departure from DLI in June 1977, the instructor has corresponded with the Captain and has sent packages to him for delivery to her relatives in Yugoslavia. She plans to visit the captain during her programmed visit/TDY to Yugoslavia in April 1978. The captain is allegedly gathering data for her that can be used by the SCLD. The instructor, a former Yugoslav citizen, is now a permanent resident of the US, and her husband is a US Army enlisted man stationed at Ft Ord.

(4) An instructor of the Hungarian Language Department (HLD) required his students to complete, in English, a Hungarian visa application as homework assignment. When filled in, the application provides considerable biographic data. The application was printed in four languages, Hungarian, German, French and English.

e. Operational Status:

(1) Seventeen confidential sources were active during the quarter. Four sources were terminated, three due to graduation and one due to unexpected reassignment, and three new sources were recruited. Four other individuals, including one instructor, are currently under assessment as potential confidential sources. In addition to the confidential source coverage, twelve conventional sources also provided coverage at DLI.

(2) During the reporting period, information obtained from all sources, including that acquired from overt liaison activities with other services, resulted in the production of two Summaries of Information, 32 Contact Reports, 48 oral reports to the DLI Commandant, eight Source Lead Development Reports (SLDR), and 109 Agent Reports. A total of 1,320 manhours were expended during the 1st Quarter.

(3) On 20 December 1977, the Project Liaison Officer (PLO) provided the Quarterly Progress Briefing to COL Samuel L. Stapleton, Commandant, DLI, with LTC Richard P. Kelly, XO, DLI and LTC Waldo R. Webb, Security Officer, DLI, also present. COL Stapleton directed that significant information in the briefing also be furnished the Deputy DLI Commandant, COL R. Jansson, USAF. This was accomplished on 21 December 1977.

(4) As a result of the Quarterly Briefing and items presented to the Commandant and his staff as developed by the ICIP during the quarter, the DLI Security Officer denied permission for an ASA enlisted student to reside in the home of an RLD instructor. The instructor has had extensive contacts with individuals in the USSR, reportedly attempted to obtain the release of family members from the USSR, and has had alleged contacts with the Soviet Consulate. The DLI Commandant has tasked the Security Officer to determine what restrictions could be placed on foreign visitors to DLI,

897 REGRADED UNCLASSIFIED ON SEP -5 1997 BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD 5200.1-R

and what actions can be taken against the PLD instructor who visited Poland without complying with DLI regulations. Further, the Security Officer was tasked to follow-up on the visa application homework assigned by an instructor of the HLD. Such assignments appear out-of-line and without academic basis.

(5) Special Operations Detachment, USAINSCOM, is closely monitoring the reports concerning the relationship between the SCLD instructor and US Army Captain. Should substantive information develop as a result of this relationship, necessary investigative or other appropriate action will be initiated.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

893

Page 2392 of 3957

2

(C) LENTIL MONKEY: (QSR, 2d QTR FY 78)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Seventeen

c. Information Obtained or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained:

(1) A Russian Language Department (RLD) instructor revealed that her mother, who resides in the USSR, had been recently questioned by KGB officials when she unsuccessfully attempted to have a manuscript smuggled out of the USSR by an American tourist for delivery to her daughter. The manuscript was allegedly the instructor's translation of some of the works of an ancient Greek philosopher. The tourist, a male student (not further identified), was apprehended and the package confiscated by airport officials. An RLD instructor revealed that while a resident of the USSR he had been approached by the KGB to be an informer. At the time, 1974, the instructor was teaching English language to Soviet Jews. Through the advice of an acquaintance, he allegedly told everyone he knew about the KGB approach and was never bothered by them again. The acquaintance was b6 a former NSA employee who defected to the Soviet Union in 1960. The RLD instructor has been attempting for some time to foster a language teaching method at DLI that he developed while in the USSR at the Pavlov Institute on Physiology. The method has a physiological-psychological basis. Three RLD instructors received unsolicited offers to purchase Soviet publications from an alleged Communist controlled bookstore in New York City.

(2) During a visit to Czechoslovakia this past Christmas season, a Czech Language Department (CLD) instructor mentioned to students that while there she was surveilled by unidentified person(s) on two separate occasions. The instructor had not reported this fact to the DLI Security Officer upon her return as required by DLI regulations. During a DLI sponsored trip to the Stanford University Library, students were approached by an unidentified man and invited to attend a Czech sponsored social function in the local area. An official invitation was later received by the CLD chairman.

(3) A Chinese Mandarin Language Department (CMLD) instructor visited the Peoples Republic of China (PRC) during January 1978, without complying with DLI regulations concerning reporting of such trips. This is the instructor's second visit to the PRC; she had complied with appropriate regulations prior to her first visit.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

899

(4) According to an unsubstantiated statement of a former Egyptian citizen, an instructor in the Arabic Language Department was reportedly a fund raiser for "El Fatah" and avid supporter of the Palestine Liberation Organization when he resided in Egypt.

(5) Through several instructors in the Hungarian Language Department (HLD), the president of a local Hungarian club requested a student volunteer to present a speech in Hungarian at a forthcoming club ceremony. A USAF enlisted student expressed willingness to present the requested speech.

e. Operational Status:

(1) Seventeen confidential sources were active during the quarter. Four sources were terminated and four new sources recruited. Five individuals are currently under assessment as potential confidential sources. In addition to confidential source coverage, ten conventional sources provided coverage at DLI.

(2) During the reporting period, information obtained from all sources, including that acquired from overt liaison activities, resulted in production of five Summaries of Information, 41 Contact Reports, 49 oral reports to the DLI Commandant and or designated representatives, five Source Lead Development Reports, and 112 Agent Reports. A total of 1448 manhours were expended on the ICIP during the 2d Quarter.

(3) On 13 March 1978, the required quarterly briefing was presented to COL Samuel L. Stapleton, Commandant, DLI. LTC Waldo R. Webb, DLI Security Officer, also attended the briefing. At the Commandant's request, on 20 March 1978, the Deputy Commandant and Executive Officer were also briefed on the progress of the ICIP.

(4) As a result of the quarterly briefing and items reported to the DLI Commandant and his staff as developed by the ICIP during the quarter, the Commandant directed that letters, requiring written replys of explanation, be sent to the DLI instructors who travelled to Communist bloc countries and did not comply with established DLI policy. He further directed the DLI Information Officer to contact the student discussed in para d(5) above, and advise him of applicable DOD, USAF and DLI regulations regarding military personnel participation in off post political rallies and activities. Such appearances, speeches or other participation by DLI staff, faculty and student personnel must be cleared through the Public Affairs Office. The DLI Security Officer was directed to determine what action can be taken concerning instructors whose actions or backgrounds indicate they may be possible security risks (reference para d(1) wherein an RLD instructor revealed contacts with the KGB and a known US defector while residing in the USSR. SOD, USAINSCOM, has been and will continue to closely monitor the instructor's teaching methods and activities.).

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2394 of 3957

[redacted]

(2)

(S) LENTIL MONKEY: (QSR, 3d QTR FY 78)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Fifteen

c. Information Obtained or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained:

(1) A Russian Language Department (RLD) supervisor entertained a Soviet citizen as his house guest for a period of over a month. The Soviet citizen, an engineer, was in Monterey awaiting settlement of his uncle's will. He returned to Moscow in mid-April following partial settlement, and has arranged with the RLD supervisor to have remaining funds sent to him through banks in the USSR and Western Europe. An RLD instructor has been selected by the US Coast Guard in Monterey to serve as a Russian Language interpreter when needed in cases involving Russian ships or personnel.

(2) An instructor in the Arabic Language Department (ALD) is reportedly subjecting his students to Palestinian Liberation Organization propaganda.

(3) An instructor in the Polish Language Department (PLD) required students to fill out a questionnaire covering such subjects as the students' military specialty; prior language training; life goals, leisure time activities; and how he/she plans to take advantage of language proficiency in future personal career.

(4) An instructor in the German Language Department (GLD) presented lectures to various GLD classes concerning his recently completed trip to East Berlin and East Germany. The instructor failed to comply with DLI regulations concerning prior reporting of trips to Communist bloc countries.

e. Operational Status:

(1) Fifteen confidential sources were active during the quarter. Five sources were terminated and three new sources recruited. Seven individuals are currently under assessment as potential confidential sources. In addition to confidential source coverage, ten conventional sources provided coverage at DLI.

(2) During the reporting period, information obtained from all sources, including that acquired from overt liaison activities, resulted in production of seven Summaries of Information, 34 Contact Reports, 42 oral reports to the DLI Commandant and/or designated representatives, eight Source Lead Development Reports, and 118 Agent Reports. A total of 1301 manhours were expended on the ICIP during the 3d quarter.

[redacted] Cdr USCCOM [redacted] 31 Dec 08

901

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

(3) On 22 June 1978, the required quarterly briefing was presented to COL Samuel L. Stapleton, Commandant, DLI. LTC Richard P. Kelly, DLI Executive Officer, and LTC Waldo R. Webb, DLI Security Officer, also attended the briefing.

(4) As a result of the quarterly briefing and items reported to the DLI Commandant and staff as developed by the ICIP during the quarter, the Commandant directed that DLI visitor control procedures be strengthened through greater coordination between the Security and Information Offices. Procedures for the direct, expeditious reporting of the arrival of visitors and monitoring of their activities at DLI are being established. The Commandant directed that a letter of reprimand be sent to the GLD instructor who visited East Berlin and East Germany without complying with appropriate DLI regulations. The Commandant directed the Security Officer to ascertain the details concerning the PLD instructor's requirement for students to complete a questionnaire soliciting biographic, professional and personal information on the students. The Commandant commented that appropriate attention must be paid to the ALD since any attempts to sabotage Arabic language teaching efforts would have serious effect on various US Aid Agreements with Arabic speaking countries. He does not wish to see the improvement in morale and efficiency of the ALD that has occurred over the past few years negated by outside interference by either pro or anti-Arab elements.

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted]

(C) LENTIL MONKEY: (QSR, 4th QTR FY 78)

a. Location: Defense Language Institute (DLI), Presidio of Monterey, CA.

b. Confidential Source Utilization: Eighteen

c. Information Obtained or Reported on Non-affiliated Civilians: None.

d. Useful Information Obtained:

(1) Unauthorized visitors to the Polish, Serbo-Croatian and Arabic Language Departments were reported during the quarter. The visitor to the Arabic Language Department (ALD), a newspaperman of unknown citizenship, allegedly plans to write an article about DLI and solicited information from the Public Affairs/Visitor Support Division (PAVSD) after he had already visited ALD.

(2) A student in the German Language Department (GLD) attending DLI in civilian cover status was questioned by a substitute instructor regarding his status, type job, assignment upon graduation, and whether he knew, and/or would be working with a former civilian GLD student now in Germany. To determine if a trend exists or is developing, attempts will be made to ascertain if any special attention or undue curiosity is shown to "civilian" personnel attending language training by the DLI instructors.

e. Operational Status:

(1) Eighteen confidential sources were active during the quarter. Two sources were terminated and eight new sources recruited. Four individuals are currently under assessment as potential confidential sources. In addition to confidential source coverage, ten conventional sources provided coverage at DLI.

(2) During the reporting period, information obtained from all sources, including that acquired from overt liaison activities, resulted in production of three Summaries of Information, 43 Contact Reports, 55 oral reports to the DLI Commandant and/or designated representatives, six Source Lead Development Reports, and 65 Agent Reports. A total of 1142 manhours were expended on the ICIP during the 4th quarter.

(3) On 20 September 1978, the required quarterly briefing was presented to LTC Waldo R. Webb, Security Officer, DLI. A comprehensive briefing on the operation will be presented to the newly assigned (22 Sep 78) DLI Commandant in the near future.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2397 of 3957

(4) Based on information reported to the DLI Commandant and staff during the quarter the following actions were initiated:

(a) During their initial security briefing, it is emphasized to all incoming student personnel that neither DLI language instructors nor their relatives have security clearances. This action was based on information that relatives of insturctors, citizens of Communist bloc countries, have attended social functions sponsored by language departments and met and conversed with students.

(b) The Security Officer and Chief, PAVSD are working together to implement and enforce effective visitor control procedures. Personnel of the ALD, see para d(1), were admonished for permitting a visitor access to that department without first coordinating with the PAVSD.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Page 2398 of 3957

DEPARTMENT OF THE ARMY
HEADQUARTERS
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FORT GEORGE G. MEADE, MARYLAND 20755

IASO-SA

SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operations (U) 78

HQDA (DAMI-DOS/Miss Brannan)
WASH DC 20310

1. (U) Submitted herewith is the status report for the 1st Quarter, FY 78, for ICIP Operation LENTIL MONKEY (U). During the reporting period, the operation produced two Summaries of Information, eight Source Lead Development Reports, 32 Contact Reports, and 109 Agent Reports.

2. (U) LENTIL MONKEY (U), supporting the Defense Language Institute, Foreign Language Center, Presidio of Monterey, CA, is the only CONUS ICIP being conducted.

3. (U) At Inclosure 2 is an updated OPLAN for LENTIL MONKEY (U). There are no significant changes to the operational concept and objectives reflected in the original OPLAN, dated 22 September 1971. The primary intent of the revision is to update terminology and references, refine Essential Elements of Information, and incorporate appropriate provisions of AR 380-13, EO 11905 and EO 12036.

2 Incl
as

WILLIAM I. JENNINGS
Special Assistant (OPS)

CDR USAINSCOM

2
31 DEC 08

REGRADED UNCLASSIFIED
ON 15 SEP 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

905

[redacted]

DEPARTMENT OF THE ARMY
HEADQUARTERS
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FORT GEORGE G. MEADE, MARYLAND 20755

2 [illegible]

IASO-SA

SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-DOS/Miss Brannan)
WASH DC 20310

(U)

1. (U) Submitted herewith is the status report, 2d Quarter, FY 78, for ICIP Operation LENTIL MONKEY (U). During the reporting period, the operation produced five Summaries of Information, five Source Lead Development Reports, 41 Contact Reports, and 112 Agent Reports.

(2)

2. (U) LENTIL MONKEY (U), supporting the Defense Language Institute, Foreign Language Center, Presidio of Monterey, CA, is the only CONUS ICIP being conducted.

1 Incl
as

WILLIAM I. JENNINGS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON SEP - 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

[redacted] CDR USAINSCOM [redacted]
[redacted] 2
[redacted] 31 Dec 08 [redacted]

906

DEPARTMENT OF THE ARMY
HEADQUARTERS
US ARMY INTELLIGENCE AND SECURITY COMMAND
FORT GEORGE G. MEADE, MARYLAND 20755

IASO-SA

OCT 3 0 1978

SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-CIC/Miss Brannan)
WASH DC 20310

(U)

1. [redacted] Submitted herewith is the status report, 4th Quarter, FY 78, for ICIP Operation LENTIL MONKEY (U). During the reporting period the operation produced three Summaries of Information, six Source Lead Development Reports, 43 Contact Reports and 65 Agent Reports.

(U)

2. [redacted] LENTIL MONKEY (U), supporting the Defense Language Institute, Foreign Language Center, Presidio of Monterey, CA, is the only CONUS ICIP being conducted.

1 Incl
as

WILLIAM T. JENNINGS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified ... Cdr USAINSCOM
EXEMPT ... CATION
SOURCE ...
EXEMPT ...
DECLASSIFY ... 31 DEC 08

907

~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
HEADQUARTERS
US ARMY INTELLIGENCE AND SECURITY COMMAND
FORT GEORGE G. MEADE, MARYLAND 20755

JUL 24 1978

IASO-SA

SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operations (U)

HQDA (DAMI-~~DOS~~ CIC/Miss Brannan)
WASH DC 20310

1. (U) Submitted herewith is the status report, 3d Quarter, FY 78, for ICIP Operation LENTIL MONKEY (U). During the reporting period, the operation produced seven Summaries of Information, eight Source Lead Development Reports, 34 Contact Reports and 118 Agent Reports.

2. (U) LENTIL MONKEY (U), supporting the Defense Language Institute, Foreign Language Center, Presidio of Monterey, CA, is the only CONUS ICIP being conducted.

1 Incl
as

WILLIAM I. JENNINGS
Special Assistant (OPS)

REGRADED UNCLASSIFIED
ON SEP 5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Classified by Cdr. INSCOM
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 3
DECLASSIFY ON 31 Dec 08

~~CONFIDENTIAL~~

OFFICE OF THE DIRECTOR

~~SECRET~~
~~CONFIDENTIAL~~

UNITED STATES DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

WASHINGTON, D.C. 20535

b1 Per FBI (S)

BY LIAISON

Date: May 11, 1978

To: Assistant Chief of Staff for Intelligence
Department of the Army
INSCOM LNO (IAINTA-SO-L)
Room 1J073, Forrestal Building
1000 Independence Avenue, Southwest
Washington, D.C.

From: William H. Webster, Director

Subject: b1 Per FBI (S)

b1 Per FBI (c)

b1 Per FBI (c)

b1 Per FBI (c)

~~CONFIDENTIAL~~
Classified by 7006
Exempt from GDS, Categories 2 and 3
Date of Declassification Indefinite

~~SECRET~~
~~CONFIDENTIAL~~ 909

REGRADED ~~SECRET~~
ON 20 MAR 1998
BY USAINSCOM FOI/PO
Auth Para 4-102 DOD 5200.1R

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

USC 552 (b)(1) per FBI

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 910

IAGPA-CSF Form 6-R
1 Sep 93

CONFIDENTIAL

Assistant Chief of Staff for Intelligence
Department of the Army

b1 Per FBI (C)

b1 Per FBI (C)

You will be kept advised of all pertinent developments. (U)

911

CONFIDENTIAL

- 3 -

OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
3 MARCH 2021 IA-45978-21

FOREIGN INFLUENCE

(U) Iranian Influence Efforts Primarily use Online Tools to Target US Audiences, Remain Easily Detectable for Now

(U//FOUO) **Scope:** This *Intelligence In Focus* (*IIF*) is a companion piece to the I&A *IIF*, "Iranian Efforts to Manipulate US Media Narratives," released on 24 February 2021, providing baseline assessments of Iran's attempts to conduct malign influence operations against US audiences.

(U//FOUO) ***We assess that Iran likely will continue to rely primarily on proxy news websites and affiliated social media accounts to attempt sustained influence against US audiences, while we expect intermittent, issue-specific influence attempts via other means (e.g., e-mails).*** We base this assessment on Iran's actions since at least 2008 to build and maintain vast malign influence networks anchored by proxy websites, as well as Iran's attempts to find new avenues to re-launch established malign influence networks after suspension. Tehran employs a network of proxy social media accounts and news websites that typically launder Iranian state media stories (stripped of attribution), plagiarize articles from Western wire services, and occasionally pay US persons to write articles to appear more legitimate to US audiences.

- *(U)* The American Herald Tribune (AHT)—an Iranian Government proxy website established in 2015 that purported to be a genuine media outlet—was seized by the US Government on 4 November 2020 for attempting to covertly influence United States policy and public opinion, according to a DOJ press release. However, AHT by at least 16 November 2020 resurfaced on a Canada-based domain, according to AHT's website. AHT is also known to pay unwitting US persons to contribute to its disinformation campaigns, according to the same website.
- *(U)* The International Union of Virtual Media (IUVM) since at least August 2018 has maintained a network of proxy accounts and websites posing as news sources that attempted to insert Iranian Government narratives into Western target audiences and to denigrate the United States, Western governments, and other regional adversaries, according to reports from a research institute and a social media analysis firm. Since IUVM started, US social media outlets have repeatedly removed its accounts from their platforms for being engaged in pro-Iran information operations and deceiving users; most recently, the FBI in October 2020 seized IUVM's domains, according to the same reports and a DOJ press release. Despite these setbacks, however, IUVM created new accounts and returned to operations, according to these same reports.

(U) Prepared by the Cyber Mission Center. Coordinated with the DHS Intelligence Enterprise (CETC, CIMC, FOD, and ICE).
For questions, contact DHS-SPS-RFI@hq.dhs.gov.

Page 2406 of 3957

- *(U)* Iranian state media-linked Liberty Front Press, created in 2013, claimed to be an independent media organization that published US political news, including content from other proxies such as IUVM and US-based media sites, according to reports from a media outlet, a cybersecurity firm, and a research institute. Liberty Front Press and its network of affiliated proxy news websites published content directly from other sources, and any original content contained poorly written English, according to the same cybersecurity firm report. In August 2018, US social media platforms deactivated accounts associated with Liberty Front Press because of its connection to Iranian state media, according to media reporting. The Liberty Front Press website was officially seized by the FBI in October 2020, according to a DOJ affidavit. The FBI identified over 1,000 domains, e-mail accounts, and social media accounts associated with Liberty Front Press as part of its investigation, according to the same affidavit.

(U//FOUO) ***For at least the next year, we assess that these Iranian-run news websites and affiliated social media accounts targeting US audiences likely will remain easily detectable by the US Government and US social media companies due to Iran's use of thinly masked and often unsubtle promotion of pro-Iranian content.*** We base this assessment on Iran's promotion of pro-Iranian messaging behind a veneer of supposedly otherwise focused pages and the ease at which these pages have previously been identified and removed from US social media platforms and registered domains. While Iranian websites have remained easily detectable to date, if these deceptive outlets improved their obfuscation techniques and replaced obvious pro-Iranian content with divisive anti-US content, these outlets could blend into the information environment and be more difficult to attribute. Thus, it is important for the US Government and social media companies to maintain a close working relationship to continue to detect and uncover Iranian covert influence efforts as they develop and grow in complexity.

- *(U)* In August 2018, a cybersecurity firm made the first major attribution of Iranian proxy accounts attempting to promote political narratives in line with Iranian interests, which directly led to the suspension and removal of over 900 accounts, pages, and groups from US social media platforms, some accounts dating back as early as 2015, according to reports from a cybersecurity firm and social media companies.

- *(U)* In October 2019, a social media company removed several Iran-based pages attempting to hide behind a façade of otherwise focused pages, while pushing pro-Iranian messaging, including a page supposedly supporting Black Lives Matter[USPER], according to a research institute.

- *(U)* In October 2020, a US social media company removed an Iran-based page attempting to conceal its identity and activity, while pushing false claims and unsubstantiated US election-related threats as part of an influence operation, according to a report from the same social media company.

- *(U)* In October 2020, a social media company acted on information provided by the FBI to take down over a hundred accounts appearing to originate from Iran and attempting unsuccessfully to disrupt the public conversation of the first 2020 US presidential debate, according to a report from the same social media company.

Source, Reference, and Dissemination Information

Source Summary Statement	*(U//FOUO)* This product is based on reports from two research institutes, a cybersecurity firm, a social media analysis firm, US social media companies, and press releases from US Government agencies. *(U//FOUO)* We assess that Iran likely will continue to primarily rely on proxy news websites and affiliated social media accounts to attempt sustained influence against US audiences, while we expect intermittent, issue-specific influence attempts via other means (e.g., e-mails). We have **moderate confidence** in our assessment based on reports from sources with a history of credible reporting and corroboration of reporting among a wide range of sources including the US Government and the social media platforms themselves. Our confidence would increase if we saw continued evidence of US detection and disruption of Iranian information operations, and we would re-evaluate this assessment if we discovered Iranian online influence that had previously been undetected for a prolonged period. *(U//FOUO)* For at least the next year, we assess that these Iranian-run news websites and affiliated social media accounts targeting US audiences likely will remain easily detectable by the US Government and US social media companies due to Iran's use of thinly masked and often unsubtle promotion of pro-Iranian content. We have **moderate confidence** in our assessment based on reports from sources with a history of credible reporting and the corroboration of reporting among a wide range of sources. Our confidence would increase if we saw further evidence of attempts of Iranian obfuscation across multiple platforms and resonating in the US information environment.
Definitions	*(U//FOUO)* **Disinformation:** A foreign government's deliberate use of false or misleading information intentionally directed at another government's decisionmakers and decision-making processes to mislead the target, force it to waste resources, or influence a decision in favor of a foreign government's interests. Disinformation always depends on falsehoods and is sometimes relayed clandestinely for the target to "discover." *(U//FOUO)* **Influence Activities:** The use of covert and overt tools to achieve a foreign government's objectives, sometimes in support of broader influence operations. Activities may be carried out by an array of actors, independently or in coordination. *(U//FOUO)* **Influence Operations:** Broad use of influence activities conducted by various state and nonstate actors, sometimes to achieve specific goals under a larger influence campaign objective.
Dissemination	*(U)* Senior DHS leadership, federal officials, governors, lieutenant governors, secretaries of state, homeland security advisors, fusion center directors and their staff.
Civil Rights and Civil Liberties	*(U//FOUO)* US persons linking, citing, quoting, or voicing the same arguments raised by these influence activities likely are engaging in First Amendment-protected activity, unless they are acting at the discretion or control of a foreign threat actor. Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect foreign influence or malign activity absent information specifically attributing the content to malign foreign actors. This information should be considered in the context of all applicable legal and policy authorities to use open source information while protecting privacy, civil rights, and civil liberties.

CISA Guidelines for Countering Foreign Influence	*(U)* CISA defines foreign influence as malign actions taken by foreign governments to spread disinformation designed to manipulate the public, sow discord and ill will, discredit the electoral process, disrupt markets, and undermine the interests of the American people. Recognize the risk: understand how foreign actors try to affect behavior. Question the source: check who produced the content and question their intent. Investigate the issue: search for other reliable sources before sharing. Think before you link: ask yourself why you're sharing, and let your emotions cool. Talk to your circle: talk to your social circle about the risks of spreading disinformation.
Warning Notices & Handling Caveats	*(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. *(U)* This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. Should you require the minimized US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@hq.dhs.gov. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.

Actions to take today to mitigate Volt Typhoon activity:

- **Apply patches for internet-facing systems**. Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.
- **Implement phishing-resistant MFA**.
- **Ensure logging is turned on for application, access, and security logs** and store logs in a central system.

CISA, NSA, FBI and the following partners are releasing this advisory to warn critical infrastructure organizations about this assessment, which is based on observations from the U.S. authoring agencies' incident response activities at critical infrastructure organizations compromised by the PRC state-sponsored cyber group known as Volt Typhoon (also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus):

- U.S. Department of Energy (DOE)
- U.S. Environmental Protection Agency (EPA)
- U.S. Transportation Security Administration (TSA)
- Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS), a part of the Communications Security Establishment (CSE)
- United Kingdom National Cyber Security Centre (NCSC-UK)
- New Zealand National Cyber Security Centre (NCSC-NZ)

The U.S. authoring agencies have confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—primarily in Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors—in the continental and non-continental United States and its territories, including Guam. Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions. The U.S. authoring agencies are concerned about the potential for these actors to use their network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts. CCCS assesses that the direct threat to Canada's critical infrastructure from PRC state-sponsored actors is likely lower than that to U.S. infrastructure, but should U.S. infrastructure be disrupted, Canada would likely be affected as well, due to cross-border integration. ASD's ACSC and NCSC-NZ assess Australian and New Zealand critical infrastructure, respectively, could be vulnerable to similar activity from PRC state-sponsored actors.

As the authoring agencies have previously highlighted, the use of living off the land (LOTL) techniques is a hallmark of Volt Typhoon actors' malicious cyber activity when targeting critical infrastructure. The group also relies on valid accounts and leverage strong operational security, which combined, allows for long-term undiscovered persistence. In fact, the U.S. authoring agencies have recently observed indications of Volt Typhoon actors maintaining access and footholds within some victim IT environments for at least five years. Volt Typhoon actors conduct extensive pre-exploitation reconnaissance to learn about the target organization and its environment; tailor their tactics, techniques, and procedures (TTPs) to the victim's environment; and dedicate ongoing resources to maintaining persistence and understanding the target environment over time, even after initial compromise.

The authoring agencies urge critical infrastructure organizations to apply the mitigations in this advisory and to hunt for similar malicious activity using the guidance herein provided, along with the recommendations found in joint guide Identifying and Mitigating Living Off the Land Techniques. These mitigations are primarily intended for IT and OT administrators in critical infrastructure organizations. Following the mitigations for prevention of or in response to an incident will help disrupt Volt Typhoon's accesses and reduce the threat to critical infrastructure entities.

If activity is identified, the authoring agencies strongly recommend that critical infrastructure organizations apply the incident response recommendations in this advisory and report the incident to the relevant agency (see Contact Information section).

For additional information, see joint advisory People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection and U.S. Department of Justice (DOJ) press release U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure. For more information on PRC state-sponsored malicious cyber activity, see CISA's China Cyber Threat Overview and Advisories webpage.

For a downloadable copy of indicators of compromise (IOCs), see:

- MAR-10448362-1.v1 (JSON, 60 KB)

TABLE OF CONTENTS

Summary 2
Table of Contents 4
Technical Details 6
Overview of Activity 6
Observed TTPs 9
Reconnaissance 9
Resource Development 9
Initial Access 9
Execution 9
Persistence 10
Defense Evasion 10
Credential Access 10
Discovery 11
Lateral Movement 13
Collection and Exfiltration 14
Command and Control 15
Detection/Hunt Recommendations 16
Apply Living off the Land Detection Best Practices 16
Review Application, Security, and System Event Logs 16
Monitor and Review OT System Logs 19
Use gait to Detect Possible Network Proxy Activities 20
Review Logins for Impossible Travel 20
Review Standard Directories for Unusual Files 20
Incident Response 20
Mitigations 23
IT Network Administrators and Defenders 23
Harden the Attack Surface 23
Secure Credentials 24
Secure Accounts 24
Secure Remote Access Services 25
Secure Sensitive Data 26

Implement Network Segmentation....26
Secure Cloud Assets....26
Be Prepared....27
OT Administrators and Defenders....28
Contact Information....29
Validate Security Controls....30
References....30
Resources....30
Disclaimer....30
Acknowledgements....31
Version History....31
Appendix A: Volt Typhoon Observed Commands / LOTL Activity....32
Appendix B: Indicators of Compromise....36
Appendix C: MITRE ATT&CK Tactics and Techniques....37

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 14. See Appendix C: MITRE ATT&CK Tactics and Techniques section for tables of the Volt Typhoon cyber threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Overview of Activity

In May 2023, the authoring agencies—working with industry partners—disclosed information about activity attributed to Volt Typhoon (see joint advisory People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection). Since then, CISA, NSA, and FBI have determined that this activity is part of a broader campaign in which Volt Typhoon actors have successfully infiltrated the networks of critical infrastructure organizations in the continental and non-continental United States and its territories, including Guam.

The U.S. authoring agencies have primarily observed compromises linked to Volt Typhoon in Communications, Energy, Transportation Systems, and Water and Wastewater Systems sector organizations' IT networks. Some victims are smaller organizations with limited cybersecurity capabilities that provide critical services to larger organizations or key geographic locations.

Volt Typhoon actors tailor their TTPs to the victim environment; however, the U.S. authoring agencies have observed the actors typically following the same pattern of behavior across identified intrusions. Their choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable the disruption of OT functions across multiple critical infrastructure sectors (see Figure 1).

1. **Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's network architecture and operational protocols.** This reconnaissance includes identifying network topologies, security measures, typical user behaviors, and key network and IT staff. The intelligence gathered by Volt Typhoon actors is likely leveraged to enhance their operational security. For example, in some instances, Volt Typhoon actors may have abstained from using compromised credentials outside of normal working hours to avoid triggering security alerts on abnormal account activities.
2. **Volt Typhoon typically gains initial access to the IT network by exploiting known or zero-day vulnerabilities in public-facing network** appliances (e.g., routers, virtual private networks [VPNs], and firewalls) and then connects to the victim's network via VPN for follow-on activities.
3. **Volt Typhoon aims to obtain administrator credentials within the network, often by exploiting privilege escalation vulnerabilities in the operating system or network services.** In some cases, Volt Typhoon has obtained credentials insecurely stored on a public-facing network appliance.

4. **Volt Typhoon uses valid administrator credentials to move laterally to the domain controller (DC) and other devices** via remote access services such as Remote Desktop Protocol (RDP).
5. **Volt Typhoon conducts discovery in the victim's network, leveraging LOTL binaries for stealth**. A key tactic includes using PowerShell to perform targeted queries on Windows event logs, focusing on specific users and periods. These queries facilitate the discreet extraction of security event logs into `.dat` files, allowing Volt Typhoon actors to gather critical information while minimizing detection. This strategy, blending in-depth pre-compromise reconnaissance with meticulous post-exploitation intelligence collection, underscores their sophisticated and strategic approach to cyber operations.
6. **Volt Typhoon achieves full domain compromise by extracting the Active Directory database (`NTDS.dit`) from the DC.** Volt Typhoon frequently employs the Volume Shadow Copy Service (VSS) using command-line utilities such as `vssadmin` to access `NTDS.dit`. The `NTDS.dit` file is a centralized repository that contains critical Active Directory data, including user accounts, passwords (in hashed form), and other sensitive data, which can be leveraged for further exploitation. This method entails the creation of a shadow copy—a point-in-time snapshot—of the volume hosting the `NTDS.dit` file. By leveraging this snapshot, Volt Typhoon actors effectively bypass the file locking mechanisms inherent in a live Windows environment, which typically prevent direct access to the `NTDS.dit` file while the domain controller is operational.
7. **Volt Typhoon likely uses offline password cracking techniques to decipher these hashes.** This process involves extracting the hashes from the `NTDS.dit` file and then applying various password cracking methods, such as brute force attacks, dictionary attacks, or more sophisticated techniques like rainbow tables to uncover the plaintext passwords. The successful decryption of these passwords allows Volt Typhoon actors to obtain elevated access and further infiltrate and manipulate the network.
8. **Volt Typhoon uses elevated credentials for strategic network infiltration and additional discovery, often focusing on gaining capabilities to access OT assets.** Volt Typhoon actors have been observed testing access to domain-joint OT assets using default OT vendor credentials, and in certain instances, they have possessed the capability to access OT systems whose credentials were compromised via `NTDS.dit` theft. This access enables potential disruptions, such as manipulating heating, ventilation, and air conditioning (HVAC) systems in server rooms or disrupting critical energy and water controls, leading to significant infrastructure failures (in some cases, Volt Typhoon actors had the capability to access camera surveillance systems at critical infrastructure facilities). In one confirmed compromise, Volt Typhoon actors moved laterally to a control system and were positioned to move to a second control system.

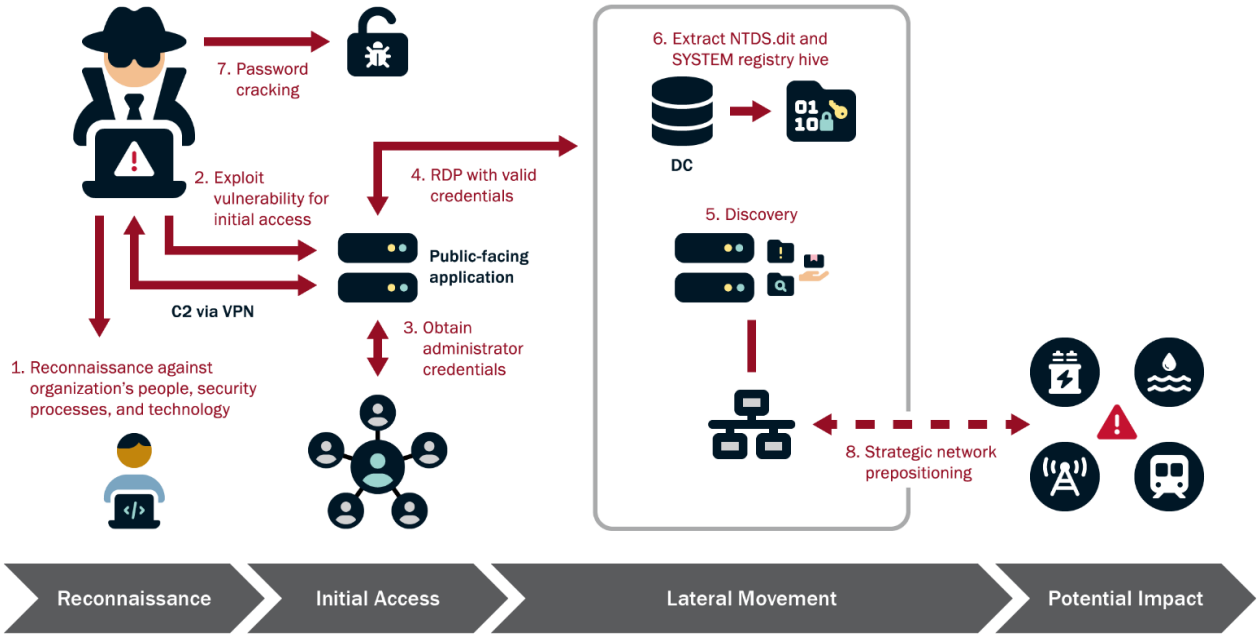


Figure 1: Typical Volt Typhoon Activity

After successfully gaining access to legitimate accounts, Volt Typhoon actors exhibit minimal activity within the compromised environment (except discovery as noted above), suggesting their objective is to maintain persistence rather than immediate exploitation. This assessment is supported by observed patterns where Volt Typhoon methodically re-targets the same organizations over extended periods, often spanning several years, to continuously validate and potentially enhance their unauthorized accesses. Evidence of their meticulous approach is seen in instances where they repeatedly exfiltrate domain credentials, ensuring access to current and valid accounts. For example, in one compromise, Volt Typhoon likely extracted `NTDS.dit` from three domain controllers in a four-year period. In another compromise, Volt Typhoon actors extracted `NTDS.dit` two times from a victim in a nine-month period.

Industry reporting—identifying that Volt Typhoon actors are silent on the network following credential dumping and perform discovery to learn about the environment, but do not exfiltrate data—is consistent with the U.S. authoring agencies' observations. This indicates their aim is to achieve and maintain persistence on the network. In one confirmed compromise, an industry partner observed Volt Typhoon actors dumping credentials at regular intervals.

In addition to leveraging stolen account credentials, the actors use LOTL techniques and avoid leaving malware artifacts on systems that would cause alerts. Their strong focus on stealth and operational security allows them to maintain long-term, undiscovered persistence. Further, Volt Typhoon's operational security is enhanced by targeted log deletion to conceal their actions within the compromised environment.

See the below sections for Volt Typhoon TTPs observed by the U.S. authoring agencies from multiple confirmed Volt Typhoon compromises.

Observed TTPs

Reconnaissance

Volt Typhoon actors conduct extensive pre-compromise reconnaissance [TA0043] to learn about the target organization [T1591], its network [T1590], and its staff [T1589]. This includes web searches [T1593]—including victim-owned sites [T1594]—for victim host [T1592], identity, and network information, especially for information on key network and IT administrators. According to industry reporting, Volt Typhoon actors use FOFA[1], Shodan, and Censys for querying or searching for exposed infrastructure. In some instances, the U.S. authoring agencies have observed Volt Typhoon actors targeting the personal emails of key network and IT staff [T1589.002] post compromise.

Resource Development

Historically, Volt Typhoon actors use multi-hop proxies for command and control (C2) infrastructure [T1090.003]. The proxy is typically composed of virtual private servers (VPSs) [T1583.003] or small office/home office (SOHO) routers. Recently, Volt Typhoon actors used Cisco and NETGEAR end-of-life SOHO routers implanted with KV Botnet malware to support their operations [T1584.005]. (See DOJ press release U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure for more information).

Initial Access

To obtain initial access [TA0001], Volt Typhoon actors commonly exploit vulnerabilities in networking appliances such as those from Fortinet, Ivanti Connect Secure (formerly Pulse Secure), NETGEAR, Citrix, and Cisco [T1190]. They often use publicly available exploit code for known vulnerabilities [T1588.005] but are also adept at discovering and exploiting zero-day vulnerabilities [T1587.004].

- In one confirmed compromise, Volt Typhoon actors likely obtained initial access by exploiting CVE-2022-42475 in a network perimeter FortiGate 300D firewall that was not patched. There is evidence of a buffer overflow attack identified within the Secure Sockets Layer (SSL)-VPN crash logs.

Once initial access is achieved, Volt Typhoon actors typically shift to establishing persistent access [TA0003]. They often use VPN sessions to securely connect to victim environments [T1133], enabling discreet follow-on intrusion activities. This tactic not only provides a stable foothold in the network but also allows them to blend in with regular traffic, significantly reducing their chances of detection.

Execution

Volt Typhoon actors rarely use malware for post-compromise execution. Instead, once Volt Typhoon actors gain access to target environments, they use hands-on-keyboard activity via the command-line [T1059] and other native tools and processes on systems [T1218] (often referred to as "LOLBins"), known as LOTL, to maintain and expand access to the victim networks. According to industry reporting, some "commands appear to be exploratory or experimental, as the operators [i.e., malicious actors] adjust and repeat them multiple times."[2]

For more details on LOTL activity, see the Credential Access and Discovery sections and Appendix A: Volt Typhoon LOTL Activity.

Similar to LOTL, Volt Typhoon actors also use legitimate but outdated versions of network admin tools. For example, in one confirmed compromise, actors downloaded [T1105] an outdated version of `comsvcs.dll` on the DC in a non-standard folder. `comsvcs.dll` is a legitimate Microsoft Dynamic Link Library (DLL) file normally found in the `System32` folder. The actors used this DLL with `MiniDump` and the process ID of the Local Security Authority Subsystem Service (LSASS) to dump the LSASS process memory [T1003.001] and obtain credentials (LSASS process memory space contains hashes for the current user's operating system (OS) credentials).

The actors also use legitimate non-native network admin and forensic tools. For example, Volt Typhoon actors have been observed using Magnet RAM Capture (MRC) version 1.20 on domain controllers. MRC is a free imaging tool that captures the physical memory of a computer, and Volt Typhoon actors likely used it to analyze in-memory data for sensitive information (such as credentials) and in-transit data not typically accessible on disk. Volt Typhoon actors have also been observed implanting Fast Reverse Proxy (FRP) for command and control.[3] (See the Command and Control section).

Persistence

Volt Typhoon primarily relies on valid credentials for persistence [T1078].

Defense Evasion

Volt Typhoon has strong operational security. Their actors primarily use LOTL for defense evasion [TA0005], which allows them to camouflage their malicious activity with typical system and network behavior, potentially circumventing simplistic endpoint security capabilities. For more information, see joint guide Identifying and Mitigating Living off the Land Techniques.

Volt Typhoon actors also obfuscate their malware. In one confirmed compromise, Volt Typhoon obfuscated FRP client files (`BrightmetricAgent.exe` and `SMSvcService.exe`) and the command-line port scanning utility ScanLine by packing the files with Ultimate Packer for Executables (UPX) [T1027.002]. FRP client applications support encryption, compression, and easy token authentication and work across multiple protocols—including transmission control protocol (TCP), user datagram protocol (UDP), hypertext transfer protocol (HTTP), and hypertext transfer protocol secure (HTTPS). The FRP client applications use the Kuai connection protocol (KCP) for error-checked and anonymous data stream delivery over UDP, with packet-level encryption support. See Appendix C and CISA Malware Analysis Report (MAR)-10448362-1.v1 for more information.

In addition to LOTL and obfuscation techniques, Volt Typhoon actors have been observed selectively clearing Windows Event Logs [T1070.001], system logs, and other technical artifacts to remove evidence [T1070.009] of their intrusion activity and masquerading file names [T1036.005].

Credential Access

Volt Typhoon actors first obtain credentials from public-facing appliances after gaining initial access by exploiting privilege escalation vulnerabilities [T1068] in the operating system or network services.

In some cases, they have obtained credentials insecurely stored on the appliance [T1552]. In one instance, where Volt Typhoon likely exploited CVE-2022-42475 in an unpatched Fortinet device, Volt Typhoon actors compromised a domain admin account stored inappropriately on the device.

Volt Typhoon also consistently obtains valid credentials by extracting the Active Directory database file (`NTDS.dit`)—in some cases multiple times from the same victim over long periods [T1003.003]. `NTDS.dit` contains usernames, hashed passwords, and group memberships for all domain accounts, essentially allowing for full domain compromise if the hashes can be cracked offline.

To obtain `NTDS.dit`, the U.S. authoring agencies have observed Volt Typhoon:

1. Move laterally [TA0008] to the domain controller via an interactive RDP session using a compromised account with domain administrator privileges [T1021.001];
2. Execute the Windows-native `vssadmin` [T1006] command to create a volume shadow copy;
3. Use Windows Management Instrumentation Console (WMIC) commands [T1047] to execute `ntdsutil` (a LOTL utility) to copy `NTDS.dit` and `SYSTEM` registry hive from the volume shadow copy; and
4. Exfiltrate [TA0010] `NTDS.dit` and `SYSTEM` registry hive to crack passwords offline) [T1110.002]. (For more details, including specific commands used, see Appendix A: Volt Typhoon LOTL Activity.)
   Note: A volume shadow copy contains a copy of all the files and folders that exist on the specified volume. Each volume shadow copy created on a DC includes its `NTDS.dit` and the `SYSTEM` registry hive, which provides keys to decrypt the `NTDS.dit` file.

Volt Typhoon actors have also been observed interacting with a PuTTY application by enumerating existing stored sessions [T1012]. Given this interaction and the exposure of cleartext-stored proxy passwords used in remote administration, Volt Typhoon actors potentially had access to PuTTY profiles that allow access to critical systems (see the Lateral Movement section).

According to industry reporting, Volt Typhoon actors attempted to dump credentials through LSASS (see Appendix B for commands used).[2]

The U.S. authoring agencies have observed Volt Typhoon actors leveraging Mimikatz to harvest credentials, and industry partners have observed Volt Typhoon leveraging Impacket.[2]

- Mimikatz is a credential dumping tool and Volt Typhoon actors use it to obtain credentials. In one confirmed compromise, the Volt Typhoon used RDP to connect to a server and run Mimikatz after leveraging a compromised administrator account to deploy it.
- Impacket is an open source Python toolkit for programmatically constructing and manipulating network protocols. It contains tools for Kerberos manipulation, Windows credential dumping, packet sniffing, and relay attacks—as well as remote service execution.

Discovery

Volt Typhoon actors have been observed using commercial tools, LOTL utilities, and appliances already present on the system for system information [T1082], network service [T1046], group [T1069] and user [T1033] discovery.

Volt Typhoon uses at least the following LOTL tools and commands for system information, network service, group, and user discovery techniques:

- cmd
- certutil
- dnscmd
- ldifde
- makecab
- net user/group/use
- netsh
- nltest
- netstat
- ntdsutil
- ping
- PowerShell
- quser
- reg query/reg save
- systeminfo
- tasklist
- wevtutil
- whoami
- wmic
- xcopy

Some observed specific examples of discovery include:

- Capturing successful logon events [T1654].
  - Specifically, in one incident, analysis of the PowerShell console history of a domain controller indicated that security event logs were directed to a file named `user.dat`, as evidenced by the executed command `Get-EventLog security -instanceid 4624 -after [year-month-date] | fl * | Out-File 'C:\users\public\documents\user.dat'`. This indicates the group's specific interest in capturing successful logon events (event ID `4624`) to analyze user authentication patterns within the network. Additionally, file system analysis, specifically of the Master File Table (MFT), uncovered evidence of a separate file, `systeminfo.dat`, which was created in `C:\Users\Public\Documents` but subsequently deleted [T1070.004]. The presence of these activities suggests a methodical approach by Volt Typhoon actors in collecting and then possibly removing traces of sensitive log information from the compromised system.
- Executing `tasklist /v` to gather a detailed process listing [T1057], followed by executing `taskkill /f /im rdpservice.exe` (the function of this executable is not known).
- Executing `net user` and `quser` for user account information [T1087.001].
- Creating and accessing a file named `rult3uil.log` on a domain controller in `C:\Windows\System32\`. The `rult3uil.log` file contained user activities on a compromised system, showcasing a combination of window title information [T1010] and focus shifts, keypresses, and command executions across Google Chrome and Windows PowerShell, with corresponding timestamps.
- Employing `ping` with various IP addresses to check network connectivity [T1016.001] and `net start` to list running services [T1007].

See Appendix A for additional LOTL examples.

In one confirmed compromise, Volt Typhoon actors attempted to use Advanced IP Scanner, which was on the network for admin use, to scan the network.

Volt Typhoon actors have been observed strategically targeting network administrator web browser data—focusing on both browsing history and stored credentials [T1555.003]—to facilitate targeting of personal email addresses (see the Reconnaissance section) for further discovery and possible network modifications that may impact the threat actor's persistence within victim networks.

In one confirmed compromise:

- Volt Typhoon actors obtained the history file from the `User Data` directory of a network administrator user's Chrome browser. To obtain the history file, Volt Typhoon actors first executed an RDP session to the user's workstation where they initially attempted, and failed, to obtain the `C$ File Name: users\{redacted}\appdata\local\Google\Chrome\UserData\default\History` file, as evidenced by the accompanying `1016` (reopen failed) SMB error listed in the application event log. The threat actors then disconnected the RDP session to the workstation and accessed the file `C:\Users\{redacted}\Downloads\History.zip`. This file presumably contained data from the `User Data` directory of the user's Chrome browser, which the actors likely saved in the Downloads directory for exfiltration [T1074]. Shortly after accessing the `history.zip` file, the actors terminated RDP sessions.
- About four months later, Volt Typhoon actors accessed the same user's Chrome data `C$ File Name: Users\{redacted}\AppData\Local\Google\Chrome\User Data\Local State` and `$ File Name: Users\{redacted}\AppData\Local\Google\Chrome\User Data\Default\Login Data` via SMB. The Local State file contains the Advanced Encryption Standard (AES) encryption key [T1552.004] used to encrypt the passwords stored in the Chrome browser, which would enable the actors to obtain plaintext passwords stored in the Login Data file in the Chrome browser.

In another confirmed compromise, Volt Typhoon actors accessed directories containing Chrome and Edge user data on multiple systems. Directory interaction was observed over the network to paths such as `C:\Users\{redacted}\AppData\Local\Google\Chrome\User Data\` and `C:\Users\{redacted}\AppData\Local\Microsoft\Edge\User Data\`. They also enumerated several directories, including directories containing vulnerability testing and cyber related content and facilities data, such as construction drawings [T1083].

Lateral Movement

For lateral movement, Volt Typhoon actors have been observed predominantly employing RDP with compromised valid administrator credentials. **Note:** With a full on-premises Microsoft Active Directory identity compromise (see the Credential Access section), the group may be capable of using other methods such as Pass the Hash or Pass the Ticket for lateral movement [T1550].

In one confirmed compromise of a Water and Wastewater Systems Sector entity, after obtaining initial access, Volt Typhoon actors connected to the network via a VPN with administrator credentials they obtained and opened an RDP session with the same credentials to move laterally. Over a nine-month period, they moved laterally to a file server, a domain controller, an Oracle Management Server (OMS), and a VMware vCenter server. The actors obtained domain credentials from the domain controller and performed discovery, collection, and exfiltration on the file server (see the Discovery and Collection and Exfiltration sections).

Volt Typhoon's movement to the vCenter server was likely strategic for pre-positioning to OT assets. The vCenter server was adjacent to OT assets, and Volt Typhoon actors were observed interacting

with the PuTTY application on the server by enumerating existing stored sessions. With this information, Volt Typhoon potentially had access to a range of critical PuTTY profiles, including those for water treatment plants, water wells, an electrical substation, OT systems, and network security devices. This would enable them to access these critical systems [T1563]. See Figure 2.

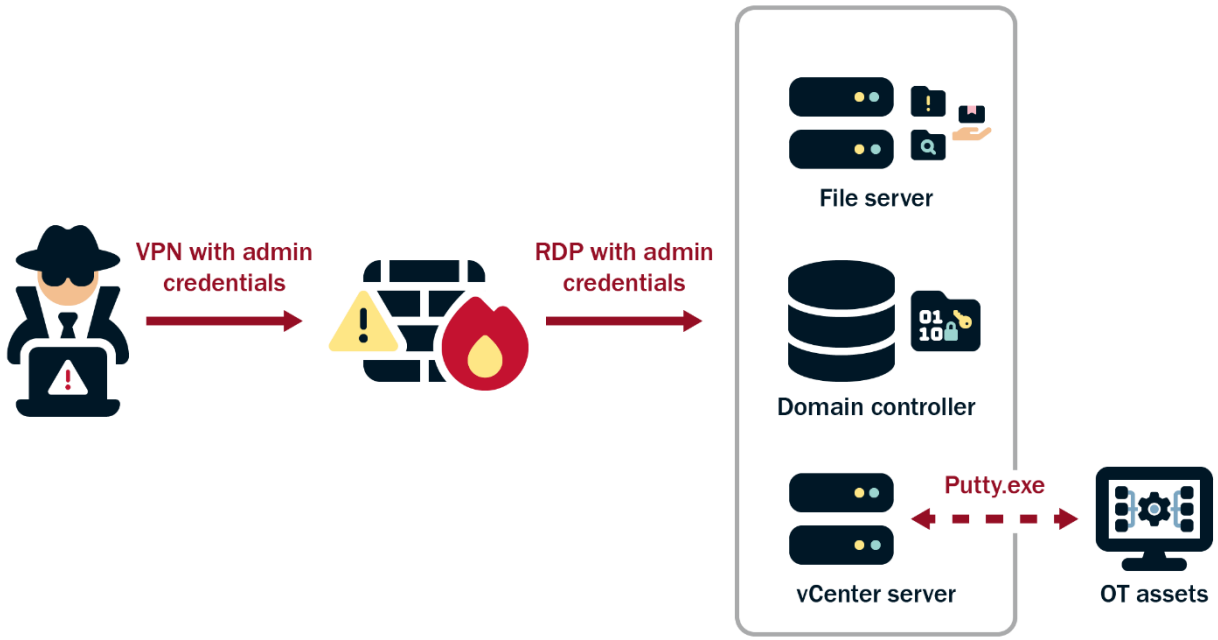


Figure 2: Volt Typhoon Lateral Movement Path File Server, DC, and OT-Adjacent Assets

Additionally, Volt Typhoon actors have been observed using PSExec to execute remote processes, including the automated acceptance of the end-user license agreement (EULA) through an administrative account, signified by the `accepteula` command flag.

Volt Typhoon actors may have attempted to move laterally to a cloud environment in one victim's network but direct attribution to the Volt Typhoon group was inconclusive. During the period of the their known network presence, there were anomalous login attempts to an Azure tenant [T1021.007] potentially using credentials [T1078.004] previously compromised from theft of `NTDS.dit`. These attempts, coupled with misconfigured virtual machines with open RDP ports, suggested a potential for cloud-based lateral movement. However, subsequent investigations, including password changes and multifactor authentication (MFA) implementations, revealed authentication failures from non-associated IP addresses, with no definitive link to Volt Typhoon.

Collection and Exfiltration

The U.S. authoring agencies assess Volt Typhoon primarily collects information that would facilitate follow-on actions with physical impacts. For example, in one confirmed compromise, they collected [TA0009] sensitive information obtained from a file server in multiple zipped files [T1560] and likely exfiltrated [TA0010] the files via Server Message Block (SMB) [T1048] (see Figure 3). Collected

information included diagrams and documentation related to OT equipment, including supervisory control and data acquisition (SCADA) systems, relays, and switchgear. This data is crucial for understanding and potentially impacting critical infrastructure systems, indicating a focus on gathering intelligence that could be leveraged in actions targeting physical assets and systems.

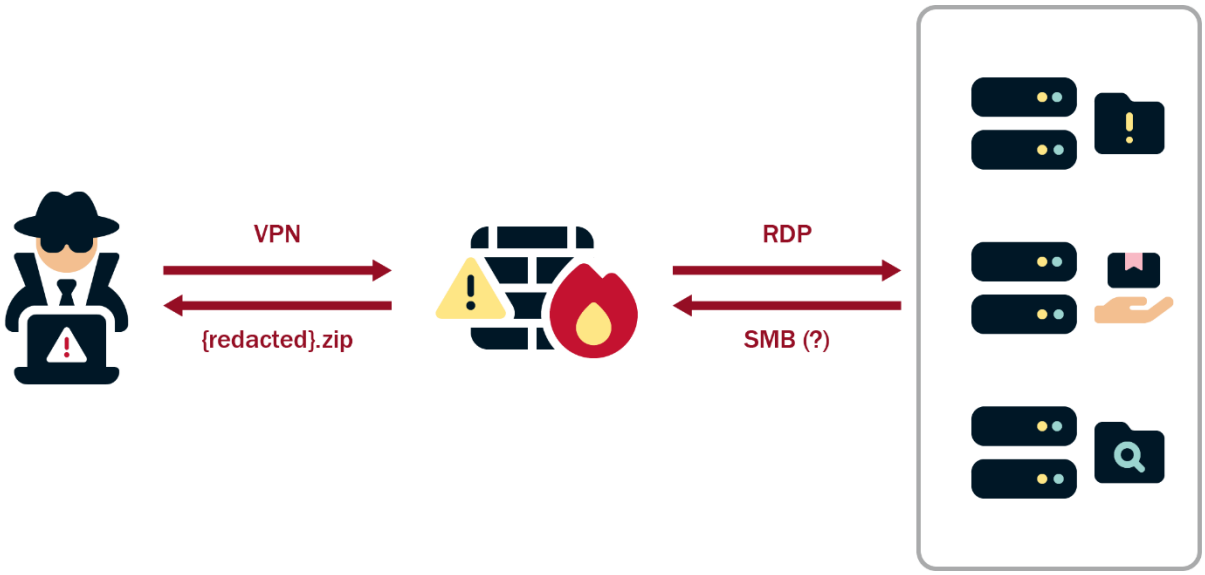


Figure 3: Volt Typhoon Attack Path for Exfiltration of Data from File Server

In another compromise, Volt Typhoon actors leveraged WMIC to create and use temporary directories (`C:\Users\Public\pro`, `C:\Windows\Temp\tmp`, `C:\Windows\Temp\tmp\Active Directory` and `C:\Windows\Temp\tmp\registry`) to stage the extracted `ntds.dit` and `SYSTEM` registry hives from `ntdsutil` execution volume shadow copies (see the Credential Access section) obtained from two DCs. They then compressed and archived the extracted `ntds.dit` and accompanying registry files by executing `ronf.exe`, which was likely a renamed version of the archive utility `rar.exe`) [T1560.001].

Command and Control

Volt Typhoon actors have been observed leveraging compromised SOHO routers and virtual private servers (VPS) to proxy C2 traffic. For more information, see DOJ press release U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure).

They have also been observed setting up FRP clients [T1090] on a victim's corporate infrastructure to establish covert communications channels [T1573] for command and control. In one instance, Volt Typhoon actors implanted the FRP client with filename `SMSvcService.exe` on a Shortel Enterprise Contact Center (ECC) server and a second FRP client with filename `Brightmetricagent.exe` on another server. These clients, when executed via PowerShell [T1059.001], open reverse proxies

between the compromised system and Volt Typhoon C2 servers. `Brightmetricagent.exe` has additional capabilities. The FRP client can locate servers behind a network firewall or obscured through Network Address Translation (NAT) [T1016]. It also contains multiplexer libraries that can bi-directionally stream data over NAT networks and contains a command-line interface (CLI) library that can leverage command shells such as PowerShell, Windows Management Instrumentation (WMI), and Z Shell (zsh) [T1059.004]. See Appendix C and MAR-10448362-1.v1 for more information.

In the same compromise, Volt Typhoon actors exploited a Paessler Router Traffic Grapher (PRTG) server as an intermediary for their FRP operations. To facilitate this, they used the `netsh` command, a legitimate Windows command, to create a PortProxy registry modification [T1112] on the PRTG server [T1090.001]. This key alteration redirected specific port traffic to Volt Typhoon's proxy infrastructure, effectively converting the PRTG's server into a proxy for their C2 traffic [T1584.004] (see Appendix B for details).

DETECTION/HUNT RECOMMENDATIONS

Apply Living off the Land Detection Best Practices

Apply the prioritized detection and hardening best practice recommendations provided in joint guide Identifying and Mitigating Living off the Land Techniques. Many organizations lack security and network management best practices (such as established baselines) that support detection of malicious LOTL activity—this makes it difficult for network defenders to discern legitimate behavior from malicious behavior and conduct behavior analytics, anomaly detection, and proactive hunting. Conventional IOCs associated with the malicious activity are generally lacking, complicating network defenders' efforts to identify, track, and categorize this sort of malicious behavior. This advisory provides guidance for a multifaceted cybersecurity strategy that enables behavior analytics, anomaly detection, and proactive hunting, which are part of a comprehensive approach to mitigating cyber threats that employ LOTL techniques.

Review Application, Security, and System Event Logs

Routinely review application, security, and system event logs, focusing on Windows Extensible Storage Engine Technology (ESENT) Application Logs. Due to Volt Typhoon's ability for long-term undetected persistence, network defenders should assume significant dwell time and review specific application event log IDs, which remain on endpoints for longer periods compared to security event logs and other ephemeral artifacts. Focus on Windows ESENT logs because certain ESENT Application Log event IDs (`216`, `325`, `326`, and `327`) may indicate actors copying `NTDS.dit`.

See Table 1 for examples of ESENT and other key log indicators that should be investigated. Please note that incidents may not always have exact matches listed in the Event Detail column due to variations in event logging and TTPs.

Table 1: Key Log Indicators for Detecting Volt Typhoon Activity

Event ID (Log)	Event Detail	Description
216 (Windows ESENT Application Log)	A database location change was detected from 'C:\Windows\NTDS\ntds.dit' to '\\?\GLOBALROOT\Device\{redacted}VolumeShadowCopy1\Windows\NTDS\ntds.dit'	A change in the `NTDS.dit` database location is detected. This could suggest an initial step in NTDS credential dumping where the database is being prepared for extraction.
325 (Windows ESENT Application Log)	The database engine created a new database (2, C:\Windows\Temp\tmp\Active Directory\ntds.dit).	Indicates creation of a new `NTDS.dit` file in a non-standard directory. Often a sign of data staging for exfiltration. Monitor for unusual database operations in temp directories.
637 (Windows ESENT Application Log)	C:\Windows\Temp\tmp\Active Directory\ntds.jfm-++- (0) New flush map file “C:\Windows\Temp\tmp\Active Directory\ntds.jfm” will be created to enable persisted lost flush detection.	A new flush map file is being created for `NTDS.dit`. This may suggest ongoing operations related to NTDS credential dumping, potentially capturing uncommitted changes to the `NTDS.dit` file.
326 (Windows ESENT Application Log)	NTDS-++-12460,D,100-++--++-1-++- C:\$SNAP_{redacted}_VOLUMEC$\Windows\NTDS\ntds.dit-++-0-++- [1] The database engine attached a database. Began mounting of C:\Windows\NTDS\ntds.dit file created from volume shadow copy process	Represents the mounting of an `NTDS.dit` file from a volume shadow copy. This is a critical step in NTDS credential dumping, indicating active manipulation of a domain controller’s data.

Event ID (Log)	Event Detail	Description
327 (Windows ESENT Application Log)	C:\Windows\Temp\tmp\Active Directory\ntds.dit-++-1-++- [1] The database engine detached a database (2, C:\Windows\Temp\tmp\Active Directory\ntds.dit). Completion of mounting of ntds.dit file to C:\Windows\Temp\tmp\Active Director	The detachment of a database, particularly in a temp directory, could indicate the completion of a credential dumping process, potentially as part of exfiltration preparations.
21 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session logon succeeded: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Successful authentication to a Remote Desktop Services session.
22 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Shell start notification received: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Successful start of a new Remote Desktop session. This may imply lateral movement or unauthorized remote access, especially if the user or session is unexpected.
23 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session logoff succeeded: User: {redacted}\{redacted} Session ID: {redacted}	Successful logoff of Remote Desktop session.
24 (Windows Terminal Services Local	Remote Desktop Services: Session has been disconnected: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Remote Desktop session disconnected by user or due to network connectivity issues.

Event ID (Log)	Event Detail	Description
Session Manager Operational Log)		
25 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session reconnection succeeded: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Successful reconnection to a Remote Desktop Services session. This may imply lateral movement or unauthorized remote access, especially if the user or session is unexpected.
1017 (Windows System Log)	Handle scavenged. Share Name: C$ File Name: users\{redacted}\downloads\History.zip Durable: 1 Resilient or Persistent: 0 Guidance: The server closed a handle that was previously reserved for a client after 60 seconds.	Indicates the server closed a handle for a client. While common in network operations, unusual patterns or locations (like `History.zip` in a user's downloads) may suggest data collection from a local system.
1102 (Windows Security Log)	All	All Event ID `1102` entries should be investigated as logs are generally not cleared and this is a known Volt Typhoon tactic to cover their tracks.

Monitor and Review OT System Logs

- Review access logs for communication paths between IT and OT networks, looking for anomalous accesses or protocols.
- Measure the baseline of normal operations and network traffic for the industrial control system (ICS) and assess traffic anomalies for malicious activity.
- Configure intrusion detection systems (IDS) to create alarms for any ICS network traffic outside normal operations.
- Track and monitor audit trails on critical areas of ICS.

- Set up security incident and event monitoring (SIEM) to monitor, analyze, and correlate event logs from across the ICS network to identify intrusion attempts.

Review CISA's Recommended Cybersecurity Practices for Industrial Control Systems and the joint advisory, NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems, for further OT system detection and mitigation guidance.

Use gait to Detect Possible Network Proxy Activities

Use gait[4] to detect network proxy activities. Developed by Sandia National Labs, gait is a publicly available Zeek[5] extension. The gait extension can help enrich Zeek's network connection monitoring and SSL logs by including additional metadata in the logs. Specifically, gait captures unique TCP options and timing data such as a TCP, transport layer security (TLS), and Secure Shell (SSH) layer inferred round trip times (RTT), aiding in the identification of the software used by both endpoints and intermediaries.

While the gait extension for Zeek is an effective tool for enriching network monitoring logs with detailed metadata, it is not specifically designed to detect Volt Typhoon actor activities. The extension's capabilities extend to general anomaly detection in network traffic, including—but not limited to—proxying activities. Therefore, while gait can be helpful in identifying tactics similar to those used by Volt Typhoon, such as proxy networks and FRP clients for C2 communication, not all proxying activities detected by using this additional metadata are necessarily indicative of Volt Typhoon presence. It serves as a valuable augmentation to current security stacks for a broader spectrum of threat detection.

For more information, see Sandia National Lab's gait GitHub page sandialabs/gait: Zeek Extension to Collect Metadata for Profiling of Endpoints and Proxies.

Review Logins for Impossible Travel

Examine VPN or other account logon times, frequency, duration, and locations. Logons from two geographically distant locations within a short timeframe from a single user may indicate an account is being used maliciously. Logons of unusual frequency or duration may indicate a threat actor attempting to access a system repeatedly or maintain prolonged sessions for the purpose of data extraction.

Review Standard Directories for Unusual Files

Review directories, such as `C:\windows\temp\` and `C:\users\public\`, for unexpected or unusual files. Monitor these temporary file storage directories for files typically located in standard system paths, such as the `System32` directory. For example, Volt Typhoon has been observed downloading `comsvcs.dll` to a non-standard folder (this file is normally found in the `System32` folder).

INCIDENT RESPONSE

If compromise, or potential compromise, is detected, **organizations should assume full domain compromise** because of Volt Typhoon's known behavioral pattern of extracting the `NTDS.dit` from

the DCs. Organizations should immediately implement the following immediate, defensive countermeasures:

1. **Sever the enterprise network from the internet. Note:** this step requires the agency to understand its internal and external connections. When making the decision to sever internet access, knowledge of connections must be combined with care to avoid disrupting critical functions.
   a. If you cannot sever from the internet, **shutdown all non-essential traffic between the affected enterprise network and the internet**.
2. **Reset credentials of privileged and non-privileged accounts within the trust boundary of each compromised account**.
   a. Reset passwords for all domain users and all local accounts, such as `Guest`, `HelpAssistant`, `DefaultAccount`, `System`, `Administrator`, and `kbrtgt`. The `kbrtgt` account is responsible for handling Kerberos ticket requests as well as encrypting and signing them. The `kbrtgt` account should be reset twice because the account has a two-password history. The first account reset for the `kbrtgt` needs to be allowed to replicate prior to the second reset to avoid any issues. See CISA's Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise for more information. Although tailored to FCEB agencies compromised in the 2020 SolarWinds Orion supply chain compromise, the steps are applicable to organizations with Windows AD compromise.
      i) Review access policies to temporarily revoke privileges/access for affected accounts/devices. If it is necessary to not alert the attacker (e.g., for intelligence purposes), then privileges can be reduced for affected accounts/devices to "contain" them.
   b. Reset the relevant account credentials or access keys if the investigation finds the threat actor's access is limited to non-elevated permissions.
      i) Monitor related accounts, especially administrative accounts, for any further signs of unauthorized access.
3. Audit all network appliance and edge device configurations with indicators of malicious activity for signs of unauthorized or malicious configuration changes. Organizations should ensure they audit the current network device running configuration and any local configurations that could be loaded at boot time. If configuration changes are identified:
   a. Change all credentials being used to manage network devices, to include keys and strings used to secure network device functions (SNMP strings/user credentials, IPsec/IKE preshared keys, routing secrets, TACACS/RADIUS secrets, RSA keys/certificates, etc.).
   b. Update all firmware and software to the latest version.
4. **Report the compromise to an authoring agency** (see the Contact Information section).
5. For organizations with cloud or hybrid environments, **apply best practices for identity and credential access management.**
   a. Verify that all accounts with privileged role assignments are cloud native, not synced from Active Directory.

b. Audit conditional access policies to ensure Global Administrators and other highly privileged service principals and accounts are not exempted.
c. Audit privileged role assignments to ensure adherence to the principle of least privilege when assigning privileged roles.
d. Leverage just-in-time and just-enough access mechanisms when administrators need to elevate to a privileged role.
e. In hybrid environments, ensure federated systems (such as AD FS) are configured and monitored properly.
f. Audit Enterprise Applications for recently added applications and examine the API permissions assigned to each.

6. **Reconnect to the internet. Note:** The decision to reconnect to the internet depends on senior leadership's confidence in the actions taken. It is possible—depending on the environment—that new information discovered during pre-eviction and eviction steps could add additional eviction tasks.
7. **Minimize and control use of remote access tools and protocols** by applying best practices from joint Guide to Securing Remote Access Software and joint Cybersecurity Information Sheet: Keeping PowerShell: Security Measures to Use and Embrace.
8. **Consider sharing technical information with an authoring agency and/or a sector-specific information sharing and analysis center.**

For more information on incident response and remediation, see:

- Joint advisory Technical Approaches to Uncovering and Remediating Malicious Activity. This advisory provides incident response best practices.
- CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to U.S. Federal Civilian Executive Branch (FCEB) agencies, the playbooks are applicable to all organizations. The incident response playbook provides procedures to identify, coordinate, remediate, recover, and track successful mitigations from incidents.
- Joint Water and Wastewater Sector - Incident Response Guide. This joint guide provides incident response best practices and information on federal resources for Water and Wastewater Systems Sector organizations.

MITIGATIONS

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of Volt Typhoon activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

These mitigations are intended for IT administrators in critical infrastructure organizations. The authoring agencies recommend that software manufactures incorporate secure by design and default principles and tactics into their software development practices to strengthen the security posture for their customers.

For information on secure by design practices that may protect customers against common Volt Typhoon techniques, see joint guide Identifying and Mitigating Living off the Land Techniques and joint Secure by Design Alert Security Design Improvements for SOHO Device Manufacturers.

For more information on secure by design, see CISA's Secure by Design webpage and joint guide.

IT Network Administrators and Defenders

Harden the Attack Surface

- **Apply patches for internet-facing systems within a risk-informed span of time** [CPG 1E]. Prioritize patching critical assets, known exploited vulnerabilities, and vulnerabilities in appliances known to be frequently exploited by Volt Typhoon (e.g., Fortinet, Ivanti, NETGEAR, Citrix, and Cisco devices).
- **Apply vendor-provided or industry standard hardening guidance** to strengthen software and system configurations. **Note:** As part of CISA's Secure by Design campaign, CISA urges software manufacturers to prioritize secure by default configurations to eliminate the need for customer implementation of hardening guidelines.
- **Maintain and regularly update an inventory of all organizational IT assets** [CPG 1A].
- **Use third party assessments to validate current system and network security compliance** via security architecture reviews, penetration tests, bug bounties, attack surface management services, incident simulations, or table-top exercises (both announced and unannounced) [CPG 1F].
- **Limit internet exposure of systems when not necessary**. An organization's primary attack surface is the combination of the exposure of all its internet-facing systems. Decrease the attack surface by not exposing systems or management interfaces to the internet when not necessary.

Secure Credentials

- **Do not store credentials on edge appliances/devices.** Ensure edge devices do not contain accounts that could provide domain admin access.
- **Do not store plaintext credentials on any system** [CPG 2L]. Credentials should be stored securely—such as with a credential/password manager or vault, or other privileged account management solutions—so they can only be accessed by authenticated and authorized users.
- **Change default passwords** [CPG 2A] and ensure they meet the policy requirements for complexity.
- Implement and enforce an organizational system-enforced policy that:
  - **Requires passwords for all IT password-protected assets to be at least 15 characters;**
  - **Does not allow users to reuse passwords for accounts, applications, services**, etc., [CPG 2C]; and
  - **Does not allow service accounts/machine accounts to reuse passwords** from member user accounts.
- **Configure Group Policy settings to prevent web browsers from saving passwords** and disable autofill functions.
- **Disable the storage of clear text passwords in LSASS memory**.

Secure Accounts

- **Implement phishing-resistant MFA** for access to assets [CPG 2H].
- **Separate user and privileged accounts**.
  - User accounts should never have administrator or super-user privileges [CPG 2E].
  - Administrators should never use administrator accounts for actions and activities not associated with the administrator role (e.g., checking email, web browsing).
- **Enforce the principle of least privilege**.
  - **Ensure administrator accounts only have the minimum permissions** necessary to complete their tasks.
  - **Review account permissions for default/accounts for edge appliances/devices and remove domain administrator privileges,** if identified.
  - **Significantly limit the number of users with elevated privileges**. Implement continuous monitoring for changes in group membership, especially in privileged groups, to detect and respond to unauthorized modifications.
  - **Remove accounts from high-privilege groups like Enterprise Admins and Schema Admins**. Temporarily reinstate these privileges only when necessary and under strict auditing to reduce the risk of privilege abuse.
  - **Transition to Group Managed Service Accounts (gMSAs)** where suitable for enhanced management and security of service account credentials. gMSAs provide automated password management and simplified Service Principal Name (SPN) management, enhancing security over traditional service accounts. See Microsoft's Group Managed Service Accounts Overview.

- **Enforce strict policies via Group Policy and User Rights Assignments** to limit high-privilege service accounts.
- **Consider using a privileged access management (PAM) solution** to manage access to privileged accounts and resources [CPG 2L]. PAM solutions can also log and alert usage to detect any unusual activity.
- **Complement the PAM solution with role-based access control (RBAC)** for tailored access based on job requirements. This ensures that elevated access is granted only when required and for a limited duration, minimizing the window of opportunity for abuse or exploitation of privileged credentials.
- **Implement an Active Directory tiering model to segregate administrative accounts** based on their access level and associated risk. This approach reduces the potential impact of a compromised account. See Microsoft's PAM environment tier model.
- **Harden administrative workstations** to only permit administrative activities from workstations appropriately hardened based on the administrative tier. See Microsoft's Why are privileged access devices important - Privileged access.
- **Disable all user accounts and access to organizational resources of employees on the day of their departure** [CPG 2G]
- **Regularly audit all user, admin, and service accounts** and remove or disable unused or unneeded accounts as applicable.
- **Regularly roll NTLM hashes of accounts that support token-based authentication.**
- Improve management of hybrid (cloud and on-premises) identity federation by:
  - **Using cloud only administrators that are asynchronous with on-premises environments** and ensuring on-premises administrators are asynchronous to the cloud.
  - **Using CISA's SCuBAGear tool to discover cloud misconfigurations in Microsoft cloud tenants**. SCuBA gear is automation script for comparing Federal Civilian Executive Branch (FCEB) agency tenant configurations against CISA M365 baseline recommendations. SCuBAGear is part of CISA's Secure Cloud Business Applications (SCuBA) project, which provides guidance for FCEB agencies, securing their cloud business application environments and protecting federal information created, accessed, shared, and stored in those environments. Although tailored to FCEB agencies, the project provides security guidance applicable to all organizations with cloud environments. For more information on SCuBAGear see CISA's Secure Cloud Business Applications (SCuBA) Project.
  - **Using endpoint detection and response capabilities to actively** defend on-premises federation servers.

Secure Remote Access Services

- **Limit the use of RDP and other remote desktop services**. If RDP is necessary, apply best practices, including auditing the network for systems using RDP, closing unused RDP ports, and logging RDP login attempts.

- **Disable Server Message Block (SMB) protocol version 1 and upgrade to version 3 (SMBv3)** after mitigating existing dependencies (on existing systems or applications), as they may break when disabled.
- **Harden SMBv3** by implementing guidance included in joint #StopRansomware Guide (see page 8 of the guide).
- **Apply mitigations from the joint Guide to Securing Remote Access Software**.

Secure Sensitive Data

- **Securely store sensitive data** (including operational technology documentation, network diagrams, etc.), ensuring that only authenticated and authorized users can access the data.

Implement Network Segmentation

- **Ensure that sensitive accounts use their administrator credentials only on hardened, secure computers**. This practice can reduce lateral movement exposure within networks.
- **Conduct comprehensive trust assessments to identify business-critical trusts and apply necessary controls** to prevent unauthorized cross-forest/domain traversal.
- **Harden federated authentication by enabling Secure Identifier (SID) Filtering and Selective Authentication on AD trust relationships** to further restrict unauthorized access across domain boundaries.
- **Implement network segmentation to isolate federation servers** from other systems and limit allowed traffic to systems and protocols that require access in accordance with Zero Trust principles.

Secure Cloud Assets

- **Harden cloud assets** in accordance with vendor-provided or industry standard hardening guidance.
  - Organizations with Microsoft cloud infrastructure, see CISA's Microsoft 365 Security Configuration Baseline Guides, which provide minimum viable secure configuration baselines for Microsoft Defender for Office 365, Azure Active Directory (now known as Microsoft Entra ID), Exchange Online, OneDrive for Business, Power BI, Power Platform, SharePoint Online, and Teams. For additional guidance, see the Australian Signals Directorate's Blueprint for Secure Cloud.
  - Organizations with Google cloud infrastructure, see CISA's Google Workspace Security Configuration Baseline Guides, which provide minimum viable secure configuration baselines for Groups for Business, GMAIL, Google Calendar, Google Chat, Google Common Controls, Google Classroom, Google Drive and Docs, Google Meet, and Google Sites.
- **Revoke unnecessary public access to cloud environment.** This involves reviewing and restricting public endpoints and ensuring that services like storage accounts, databases, and virtual machines are not publicly accessible unless absolutely necessary. Disable legacy authentication protocols across all cloud services and platforms. Legacy protocols frequently lack support for advanced security mechanisms such as multifactor authentication, rendering

them susceptible to compromises. Instead, enforce the use of modern authentication protocols that support stronger security features like MFA, token-based authentication, and adaptive authentication measures.
    - **Enforce this practice through the use of Conditional Access Policies**. These policies can initially be run in `report-only` mode to identify potential impacts and plan mitigations before fully enforcing them. This approach allows organizations to systematically control access to their cloud resources, significantly reducing the risk of unauthorized access and potential compromise.
- **Regularly monitor and audit privileged cloud-based accounts**, including service accounts, which are frequently abused to enable broad cloud resource access and persistence.

Be Prepared

- **Ensure logging is turned on for application, access, and security logs** (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, and VPNs) [CPG 2T]. Given Volt Typhoon's use of LOTL techniques and their significant dwell time, application event logs may be a valuable resource to hunt for Volt Typhoon activity because these logs typically remain on endpoints for relatively long periods of time.
    - For OT assets where logs are non-standard or not available, **collect network traffic and communications between those assets and other assets**.
    - Implement file integrity monitoring (FIM) tools to detect unauthorized changes.
- **Store logs in a central system**, such as a security information and event management (SIEM) tool or central database.
    - **Ensure the logs can only be accessed or modified by authorized and authenticated users** [CPG 2U].
    - **Store logs for a period informed by risk or pertinent regulatory guidelines**.
    - **Tune log alerting to reduce noise while ensuring there are alerts for high-risk activities**. (For information on alert tuning, see joint guide Identifying and Mitigating Living Off the Land Techniques.)
- **Establish and continuously maintain a baseline of installed tools and software, account behavior, and network traffic**. This way, network defenders can identify potential outliers, which may indicate malicious activity. **Note:** For information on establishing a baseline, see joint guide Identifying and Mitigating Living off the Land Techniques.
- **Document a list of threats and cyber actor TTPs relevant to your organization** (e.g., based on industry or sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats [CPG 3A].
- **Implement periodic training for all employees and contractors that covers basic security concepts** (such as phishing, business email compromise, basic operational security, password security, etc.), as well as fostering an internal culture of security and cyber awareness [CPG 2I].
    - **Tailor the training to network IT personnel/administrators and other key staff based on relevant organizational cyber threats and TTPs**, such as Volt Typhoon. For example, communicate that Volt Typhoon actors are known to target personal email

accounts of IT staff, and encourage staff to protect their personal email accounts by using strong passwords and implementing MFA.
    - In addition to basic cybersecurity training, **ensure personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training** on at least an annual basis [CPG 2J].
    - **Educate users about the risks associated with storing unprotected passwords**.

OT Administrators and Defenders

- **Change default passwords** [CPG 2A] and ensure they meet the policy requirements for complexity. If the asset's password cannot be changed, implement compensating controls for the device; for example, segment the device into separate enclaves and implement increased monitoring and logging.
- **Require that passwords for all OT password-protected assets be at least 15 characters**, when technically feasible. In instances where minimum passwords lengths are not technically feasible (for example, assets in remote locations), apply compensating controls, record the controls, and log all login attempts. [CPG 2B].
- **Enforce strict access policies for accessing OT networks**. Develop strict operating procedures for OT operators that details secure configuration and usage.
- **Segment OT assets from IT environments** by [CPG 2F]:
    - **Denying all connections to the OT network by default** unless explicitly allowed (e.g., by IP address and port) for specific system functionality.
    - **Requiring necessary communications paths between IT and OT networks to pass through an intermediary**, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone (DMZ), which is closely monitored, captures network logs, and only allows connections from approved assets.
- **Closely monitor all connections into OT networks for misuse, anomalous activity, or OT protocols**.
- **Monitor for unauthorized controller change attempts**. Implement integrity checks of controller process logic against a known good baseline. Ensure process controllers are prevented from remaining in remote program mode while in operation if possible.
- **Lock or limit set points in control processes to reduce the consequences of unauthorized controller access**.
- **Be prepared** by:
    - **Determining your critical operational processes' reliance on key IT infrastructure**:
        - Maintain and regularly update an inventory of all organizational OT assets.
        - Understand and evaluate cyber risk on "as-operated" OT assets.
        - Create an accurate "as-operated" OT network map and identify OT and IT network inter-dependencies.
    - **Identifying a resilience plan that addresses how to operate if you lose access to or control of the IT and/or OT environment**.
        - Plan for how to continue operations if a control system is malfunctioning, inoperative, or actively acting contrary to the safe and reliable operation of the process.

        - Develop workarounds or manual controls to ensure ICS networks can be isolated if the connection to a compromised IT environment creates risk to the safe and reliable operation of OT processes.
    - **Create and regularly exercise an incident response plan**.
        - Regularly test manual controls so that critical functions can be kept running if OT networks need to be taken offline.
    - **Implement regular data backup procedures** on OT networks.
        - Regularly test backup procedures.
- **Follow risk-informed guidance** in the joint advisory NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems, the NSA advisory Stop Malicious Cyber Activity Against Connected Operational Technology.

CONTACT INFORMATION

US organizations: To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact:

- CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870 or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.
- Water and Wastewater Systems Sector organizations, contact the EPA Water Infrastructure and Cyber Resilience Division at watercyberta@epa.gov to voluntarily provide situational awareness.
- Entities required to report incidents to DOE should follow established reporting requirements, as appropriate. For other energy sector inquiries, contact EnergySRMA@hq.doe.gov.
- For transportation entities regulated by TSA, report to CISA Central in accordance with the requirements found in applicable Security Directives, Security Programs, or TSA Order.

Australian organizations: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations: Report incidents by emailing CCCS at contact@cyber.gc.ca.

New Zealand organizations: Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom organizations: Report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring agencies recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 5 through Table 17).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring agencies recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

REFERENCES

[1] fofa

[2] Microsoft: Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

[3] GitHub - fatedier/frp: A fast reverse proxy to help you expose a local server behind a NAT or firewall to the internet

[4] GitHub - sandialabs/gait: Zeek Extension to Collect Metadata for Profiling of Endpoints and Proxies

[5] The Zeek Network Security Monitor

RESOURCES

Microsoft: Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

Secureworks: Chinese Cyberespionage Group BRONZE SILHOUETTE Targets U.S. Government and Defense Organizations

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities,

products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

ACKNOWLEDGEMENTS

Fortinet and Microsoft contributed to this advisory.

VERSION HISTORY

February 7, 2024: Initial Version.

APPENDIX A: VOLT TYPHOON OBSERVED COMMANDS / LOTL ACTIVITY

See Table 2 and Table 3 for Volt Typhoon commands and PowerShell scripts observed by the U.S. authoring agencies during incident response activities. For additional commands used by Volt Typhoon, see joint advisory People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.

Table 2: Volt Typhoon Observed Commands in PowerShell Console History

Command/Script	Description/Use
Get-EventLog security -instanceid 4624 -after {redacted date} | fl * | Out-File 'C:\users\public\documents\user.dat'	PowerShell command extracts security log entries with the Event ID `4624` after a specified date. The output is formatted (`fl *`) and saved to `user.dat`. Potentially used to analyze logon patterns and identify potential targets for lateral movement.
Get-EventLog security -instanceid 4624 | Where-Object {$_.message.contains('{redacted user account}')} | select -First 1 | fl *	PowerShell command extracts security log entries with the Event ID `4624` and filters them to include only those containing a specific user account, selecting the first instance of such an event.
wminc process get name,processid	Appears to be an attempt to use the wmic command but with a misspelling (`wminc` instead of `wmic`). This command, as it stands, would not execute successfully and would return an error in a typical Windows environment. This could indicate a mistake made during manual input.
wmic process get name,processid	WMI command lists all running processes with process names and process IDs. Potentially used to find process IDs needed for other operations, like memory dumping.
tasklist /v	Command displays detailed information about currently running processes, including the name, PID, session number, and memory usage.

Command/Script	Description/Use
taskkill /f /im rdpservice.exe	Command forcibly terminates the process `rdpservice.exe`. Potentially used as a cleanup activity post-exploitation.
ping -n 1 {redacted IP address}	Command sends one ICMP echo request to a specified IP address.
ping -n 1 -w 1 {redacted IP address}	Command sends one ICMP echo request to a specified IP address with a timeout (`-w`) of 1 millisecond.
net user	Lists all user accounts on the local machine or domain, useful for quickly viewing existing user accounts.
quser query user	Displays information about user sessions on a system, aiding in identifying active users or sessions.
net start	Lists all active services.
cmd	Opens a new instance of the command prompt.
cd [Redacted Path]	Changes the current directory to a specified path, typically for navigating file systems.
Remove-Item .\Thumbs.db	PowerShell command to delete the `Thumbs.db` file, possibly for cleanup or removing traces.
move .\Thumbs.db ttt.dat	Relocates and renames the file `Thumbs.db` in the current directory to `ttt.dat` within the same directory.
del .\Thumbs.db /f /s /q	Force deletes `Thumbs.db` files from the current directory and all subdirectories, part of cleanup operations to erase traces.
del ??	Deletes files with two-character names, potentially a targeted cleanup command.

Command/Script	Description/Use
del /?	Displays help information for the `del` command.
exit	Terminates the command prompt session.
ipconfig	Retrieves network configuration details, helpful for discovery and mapping the victim's network.
net time /dom	Queries or sets the network time for a domain, potentially used for reconnaissance or to manipulate system time.
netstta -ano	Intended as `netstat -ano`; a mistyped command indicating a potential operational error.
netstat -ano	Lists active network connections and processes, helpful for identifying communication channels and potential targets.
type .\Notes.txt	Displays the contents of `Notes.txt`, possibly used for extracting specific information or intelligence gathering.
logoff	Logs off the current user session.

Table 3: Volt Typhoon Observed PowerShell Scripts

Script name and location	Contents	Description/Use
C:\{redacted}\ logins.ps1	# Find DC list from Active Directory $DCs = Get-ADDomainController -Filter * # Define time for report (default is 1 day) $startDate = (get-date).AddDays(-1)	The script is designed for user logon discovery in a Windows Active Directory environment. It retrieves a list of DCs and then queries security logs on these DCs for successful logon events (Event ID **4624**) within the last day. The script differentiates

Script name and location	Contents	Description/Use

	# Store successful logon events from security logs with the specified dates and workstation/IP in an array
	foreach ($DC in $DCs){
	$slogonevents = Get-Eventlog -LogName Security -ComputerName $DC.Hostname -after $startDate \| where {$_.eventID -eq 4624 }}
	
	# Crawl through events; print all logon history with type, date/time, status, account name, computer and IP address if user logged on remotely
	
	foreach ($e in $slogonevents){
	# Logon Successful Events
	# Local (Logon Type 2)
	if (($e.EventID -eq 4624) -and ($e.ReplacementStrings[8] -eq 2)){
	write-host "Type: Local Logon`tDate: "$e.TimeGenerated "`tStatus: Success`tUser: "$e.ReplacementStrings[5] "`tWorkstation: "$e.ReplacementStrings[11]
	}
	# Remote (Logon Type 10)
	if (($e.EventID -eq 4624) -and ($e.ReplacementStrings[8] -eq 10)){
	write-host "Type: Remote Logon`tDate: "$e.TimeGenerated "`tStatus: Success`tUser: "$e.ReplacementStrings[5] "`tWorkstation: "$e.ReplacementStrings[11] "`tIP Address: "$e.ReplacementStrings[18]
	}}
		between local (Logon Type 2) and remote (Logon Type 10) logon events. For each event, it extracts and displays details including the logon type, date/time of logon, status, account name, and the workstation or IP address used for the logon. Volt Typhoon may be leveraging this script to monitor user logon activities across the network, potentially to identify patterns, gather credentials, or track the movement of users and administrators within the network.

APPENDIX B: INDICATORS OF COMPROMISE

See Table 4 for Volt Typhoon IOCs obtained by the U.S. authoring agencies during incident response activities.

Table 4: Volt Typhoon Malicious Files and Associated Hashes

Note: See MAR-10448362-1.v1 for more information on this malware.

File Name	Description	MD5	Hashes (SHA256)
BrightmetricAgent.exe	The file is an FRP that could be used to reveal servers situated behind a network firewall or obscured through Network Address Translation (NAT).	fd41134e8ead1c18ccad27c62a260aa6	edc0c63065e88ec96197c8d7a40662a15a812a9583dc6c82b18ecd7e43b13b70
SMSvcService.exe	The file is a Windows executable "FRPC" designed to open a reverse proxy between the compromised system and the threat actor(s) C2 server.	b1de37bf229890ac181bdef1ad8ee0c2	99b80c5ac352081a64129772ed5e1543d94cad708ba2adc46dc4ab7a0bd563f1

APPENDIX C: MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 5 through Table 17 for all referenced threat actor tactics and techniques in this advisory.

Table 5: Volt Typhoon actors ATT&CK Techniques for Enterprise – Reconnaissance

Reconnaissance		
Technique Title	**ID**	**Use**
Gather Victim Host Information	T1592	Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including victim-owned sites, for victim host, identity, and network information, especially for information on key network and IT administrators.
Gather Victim Identity Information	T1589	Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's staff.
Gather Victim Identity Information: Email Addresses	T1589.002	Volt Typhoon targets the personal emails of key network and IT staff.
Gather Victim Network Information	T1590	Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's network.
Gather Victim Org Information	T1591	Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization.
Search Open Websites/Domains	T1593	Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including victim-owned sites, for victim host, identity, and network information, especially for information on key network and IT administrators.
Search Victim-Owned Websites	T1594	Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including victim-owned sites, for victim host, identity, and network information, especially for information on key network and IT administrators.

Table 6: Volt Typhoon actors ATT&CK Techniques for Enterprise – Resource Development

Resource Development		
Technique Title	**ID**	**Use**
Acquire Infrastructure: Botnet	T1583.003	Volt Typhoon uses multi-hop proxies for command-and-control infrastructure. The proxy is typically composed of Virtual Private Servers (VPSs) or small office/home office (SOHO) routers.
Compromise Infrastructure: Botnet	T1584.005	Volt Typhoon used Cisco and NETGEAR end-of-life SOHO routers implanted with KV Botnet malware to support their operations.
Compromise Infrastructure: Server	T1584.004	Volt Typhoon has redirected specific port traffic to their proxy infrastructure, effectively converting the PRTG's Detection Guidance server into a proxy for their C2 traffic.
Develop Capabilities: Exploits	T1587.004	Volt Typhoon uses publicly available exploit code, but is also adept at discovering and exploiting vulnerabilities as zero days.
Obtain Capabilities: Exploits	T1588.005	Volt Typhoon uses publicly available exploit code, but is also adept at discovering and exploiting vulnerabilities as zero days.

Table 7: Volt Typhoon actors ATT&CK Techniques for Enterprise – Initial Access

Initial Access		
Technique Title	**ID**	**Use**
Exploit Public-Facing Application	T1190	Volt Typhoon commonly exploits vulnerabilities in networking appliances such as Fortinet, Ivanti (formerly Pulse Secure), NETGEAR, Citrix, and Cisco.
External Remote Services	T1133	Volt Typhoon often uses VPN sessions to securely connect to victim environments, enabling discreet follow-on intrusion activities.

Table 8: Volt Typhoon actors ATT&CK Techniques for Enterprise – Execution

Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter	T1059	Volt Typhoon uses hands-on-keyboard execution for their malicious activity via the command-line.
Command and Scripting Interpreter: PowerShell	T1059.001	Volt Typhoon has executed clients via PowerShell.
Command and Scripting Interpreter: Unix Shell	T1059.004	Volt Typhoon has used `Brightmetricagent.exe`, which contains multiplexer libraries that can bi-directionally stream data over through NAT networks and contains a command-line interface (CLI) library that can leverage command shells such as PowerShell, Windows Management, Instrumentation (WMI), and Z Shell (zsh).
Windows Management Instrumentation	T1047	Volt Typhoon has used Windows Management Instrumentation Console (WMIC) commands.

Table 9: Volt Typhoon actors ATT&CK Techniques for Enterprise – Persistence

Persistence		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	Volt Typhoon primarily relies on valid credentials for persistence.

Table 10: Volt Typhoon actors ATT&CK Techniques for Enterprise – Privilege Escalation

Privilege Escalation		
Technique Title	**ID**	**Use**
Exploitation for Privilege Escalation	T1068	Volt Typhoon first obtains credentials from public-facing appliances after gaining initial access by exploiting privilege

		escalation vulnerabilities in the operating system or network services.

Table 11: Volt Typhoon actors ATT&CK Techniques for Enterprise – Defense Evasion

Defense Evasion		
Technique Title	**ID**	**Use**
Direct Volume Access	T1006	Volt Typhoon has executed the Windows-native `vssadmin` command to create a volume shadow copy.
Indicator Removal: Clear Persistence	T1070.009	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.
Indicator Removal: Clear Windows Event Logs	T1070.001	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.
Indicator Removal: File Deletion	T1070.004	Volt Typhoon created `systeminfo.dat` in `C:\Users\Public\Documents`, but subsequently deleted it.
Masquerading: Match Legitimate Name or Location	T1036.005	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.
Modify Registry	T1112	Volt Typhoon has used the `netsh` command, a legitimate Windows command, to create a PortProxy registry modification on the PRTG server.
Obfuscated Files or Information: Software Packing	T1027.002	Volt Typhoon has obfuscated FRP client files (`BrightmetricAgent.exe` and `SMSvcService.exe`) and the command-line port scanning utility ScanLine by packing the files with Ultimate Packer for Executables (UPX).
System Binary Proxy Execution	T1218	Volt Typhoon uses hands-on-keyboard activity via the command-line and use other native tools and processes on systems (often referred to as “LOLBins”), known as LOTL, to maintain and expand access to the victim networks.

Table 12: Volt Typhoon actors ATT&CK Techniques for Enterprise – Credential Access

Credential Access		
Technique Title	**ID**	**Use**
Brute Force: Password Cracking	T1110.002	Volt Typhoon has exfiltrated `NTDS.dit` and `SYSTEM` registry hive to crack passwords offline.
Credentials from Password Stores	T1555	Volt Typhoon has installed browsers saved passwords history, credit card details, and cookies.
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	Volt Typhoon has strategically targeted network administrator web browser data, focusing on both browsing history and stored credentials.
OS Credential Dumping: LSASS Memory	T1003.001	Volt Typhoon used a DLL with `MiniDump` and the process ID of Local Security Authority Subsystem Service (LSASS) to dump the LSASS process memory and obtain credentials.
OS Credential Dumping: NTDS	T1003.003	Volt Typhoon appears to prioritize obtaining valid credentials by extracting the Active Directory database file (`NTDS.dit`).
Unsecured Credentials	T1552	Volt Typhoon has obtained credentials insecurely stored on an appliance.
Unsecured Credentials: Private Keys	T1552.004	Volt Typhoon has accessed a Local State file that contains the Advanced Encryption Standard (AES) encryption key used to encrypt the passwords stored in the Chrome browser, which enables the actors to obtain plaintext passwords stored in the Login Data file in the Chrome browser.

Table 13: Volt Typhoon actors ATT&CK Techniques for Enterprise – Discovery

Discovery		
Technique Title	**ID**	**Use**
Account Discovery: Local Account	T1087.001	Volt Typhoon executed `net user` and `quser` for user account information.

Application Window Discovery	T1010	Volt Typhoon created and accessed a file named `rult3uil.log` on a Domain Controller in `C:\Windows\System32\`. The `rult3uil.log` file contained user activities on a compromised system, showcasing a combination of window title information and focus shifts, keypresses, and command executions across Google Chrome and Windows PowerShell, with corresponding timestamps.
Browser Information Discovery	T1217	Volt Typhoon has installed browsers saved passwords history, credit card details, and cookies.
File and Directory Discovery	T1083	Volt Typhoon enumerated several directories, including directories containing vulnerability testing and cyber related content and facilities data, such as construction drawings.
Log Enumeration	T1654	Volt Typhoon has captured successful logon events.
Network Service Discovery	T1046	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.
Peripheral Device Discovery	T1120	Volt Typhoon has obtained the victim's system screen dimension and display devices information.
Permission Groups Discovery	T1069	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.
Process Discovery	T1057	Volt Typhoon executed `tasklist /v` to gather a detailed process listing.
Query Registry	T1012	Volt Typhoon has interacted with a PuTTY application by enumerating existing stored sessions.
Software Discovery	T1518	Volt Typhoon has obtained the victim's list of applications installed on the victim's system.
System Information Discovery	T1082	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.

System Location Discovery	T1614	Volt Typhoon has obtained the victim's system current locale.
System Network Configuration Discovery: Internet Connection Discovery	T1016.001	Volt Typhoon employs `ping` with various IP addresses to check network connectivity and `net start` to list running services.
System Owner/User Discovery	T1033	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.
System Service Discovery	T1007	Volt Typhoon employs `ping` with various IP addresses to check network connectivity and `net start` to list running services.
System Time Discovery	T1124	Volt Typhoon has obtained the victim's system timezone.

Table 14: Volt Typhoon actors ATT&CK Techniques for Enterprise – Lateral Movement

Lateral Movement		
Technique Title	**ID**	**Use**
Remote Service Session Hijacking	T1563	Volt Typhoon potentially had access to a range of critical PuTTY profiles, including those for water treatment plants, water wells, an electrical substation, operational technology systems, and network security devices. This would enable them to access these critical systems.
Remote Services: Cloud Services	T1021.007	During the period of Volt Typhoon's known network presence, there were anomalous login attempts to an Azure tenant potentially using credentials previously compromised from theft of `NTDS.dit`.
Remote Services: Remote Desktop Protocol	T1021.001	Volt Typhoon has moved laterally to the Domain Controller via an interactive RDP session using a compromised account with domain administrator privileges.

Use Alternate Authentication Material	T1550	Volt Typhoon may be capable of using other methods such as Pass the Hash or Pass the Ticket for lateral movement.
Valid Accounts: Cloud Accounts	T1078.004	During the period of Volt Typhoon's known network presence, there were anomalous login attempts to an Azure tenant potentially using credentials previously compromised from theft of `NTDS.dit`.

Table 15: Volt Typhoon actors ATT&CK Techniques for Enterprise – Collection

Collection		
Technique Title	**ID**	**Use**
Archive Collected Data	T1560	Volt Typhoon collected sensitive information obtained from a file server in multiple zipped files.
Archive Collected Data: Archive via Utility	T1560.001	Volt Typhoon has compressed and archived the extracted `ntds.dit` and accompanying registry files (by executing `ronf.exe`, which was likely a renamed version of `rar.exe`).
Data Staged	T1074	Volt Typhoon accessed the file `C:\Users\{redacted}\Downloads\History.zip`, which presumably contained data from the User Data directory of the user's Chrome browser, which the actors likely saved in the Downloads directory for exfiltration.
Screen Capture	T1113	Volt Typhoon has obtained a screenshot of the victim's system using two libraries (`gdi32.dll` and `gdiplus.dll`)

Table 16: Volt Typhoon actors ATT&CK Techniques for Enterprise – Command and Control

Command and Control		
Technique Title	**ID**	**Use**
Encrypted Channel	T1573	Volt Typhoon has setup FRP clients on a victim's corporate infrastructure to establish covert communications channels for command and control.

Ingress Tool Transfer	T1105	Volt Typhoon uses legitimate, but outdated versions of network admin tools. For example, in one confirmed compromise, actors downloaded an outdated version of `comsvcs.dll`, on the DC in a non-standard folder.
Proxy	T1090	Volt Typhoon has setup FRP clients on a victim's corporate infrastructure to establish covert communications channels for command and control.
Proxy: Internal Proxy	T1090.001	Volt Typhoon has used the `netsh` command, a legitimate Windows command, to create a PortProxy registry modification on the PRTG server.
Proxy: Multi-hop Proxy	T1090.003	Volt Typhoon uses multi-hop proxies for command-and-control infrastructure.

Table 17: Volt Typhoon actors ATT&CK Techniques for Enterprise – Exfiltration

Exfiltration		
Technique Title	**ID**	**Use**
Exfiltration Over Alternative Protocol	T1048	Volt Typhoon exfiltrated files via Server Message Block (SMB).

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A MEME'S ROLE IN INFORMATION DISORDER CAMPAIGNS: DESIGNING AN EXPERIMENT THAT DRAWS CORRELATIONS BETWEEN AGE, EDUCATION LEVEL AND GENDER, AND PARTICIPANT WILLINGNESS TO INTERACT WITH FALSE INFORMATION

by

Katherine A. Cisewski

June 2021

Thesis Advisor:	Anthony Canan
Co-Advisor:	Steven J. Iatrou
Second Reader:	Glenn R. Cook

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
A MEME'S ROLE IN INFORMATION DISORDER CAMPAIGNS: DESIGNING AN EXPERIMENT THAT DRAWS CORRELATIONS BETWEEN AGE, EDUCATION LEVEL AND GENDER, AND PARTICIPANT WILLINGNESS TO INTERACT WITH FALSE INFORMATION

5. FUNDING NUMBERS

6. AUTHOR(S) Katherine A. Cisewski

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The use of social media has been growing every year since its inception. With that, individuals, organizations, businesses, and nations have created clever ways to spread messages to large audiences; however, in the last decade, those same entities have begun utilizing social media to spread false narratives that fit their agenda. Using Tweets and memes, non-state and state actors have successfully influenced elections, incited riots, and increased membership. Current academic research does not describe who is most susceptible to this new type of information disorder. For that reason, the experiment detailed in this thesis was designed to aid information environment researchers in identifying groups that are most susceptible to information disorder; when conducted, it will reveal correlations between the acceptance and propagation of false information spread through Tweets and memes and the age group, gender, and education level of those most likely to interact with the false information. Once complete, defensive and offensive measures can be put in place by individuals, organizations, businesses, and nations to defend or attack the most at-risk groups.

14. SUBJECT TERMS
human-machine interaction, information warfare, information sciences

15. NUMBER OF PAGES
109

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Page 2457 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2458 of 3957

Approved for public release. Distribution is unlimited.

A MEME'S ROLE IN INFORMATION DISORDER CAMPAIGNS: DESIGNING AN EXPERIMENT THAT DRAWS CORRELATIONS BETWEEN AGE, EDUCATION LEVEL AND GENDER, AND PARTICIPANT WILLINGNESS TO INTERACT WITH FALSE INFORMATION

Katherine A. Cisewski
Captain, United States Marine Corps
BS, Texas A & M University, 2015

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

and

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: Anthony Canan
Advisor

Steven J. Iatrou
Co-Advisor

Glenn R. Cook
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

Glenn R. Cook
Academic Associate, Graduate School of Defense Management

Page 2459 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2460 of 3957

ABSTRACT

The use of social media has been growing every year since its inception. With that, individuals, organizations, businesses, and nations have created clever ways to spread messages to large audiences; however, in the last decade, those same entities have begun utilizing social media to spread false narratives that fit their agenda. Using Tweets and memes, non-state and state actors have successfully influenced elections, incited riots, and increased membership. Current academic research does not describe who is most susceptible to this new type of information disorder. For that reason, the experiment detailed in this thesis was designed to aid information environment researchers in identifying groups that are most susceptible to information disorder; when conducted, it will reveal correlations between the acceptance and propagation of false information spread through Tweets and memes and the age group, gender, and education level of those most likely to interact with the false information. Once complete, defensive and offensive measures can be put in place by individuals, organizations, businesses, and nations to defend or attack the most at-risk groups.

Page 2461 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. SOCIAL MEDIA, THE NEWS, AND MARKETING: WHAT COULD GO WRONG? 1
- B. KEY INFORMATION DISSEMINATION TOOLS: TWEETS AND IMAGE MACRO MEMES 2
- C. WHAT MAKES MEMETIC RESEARCH IMPORTANT? 4
- D. PROBLEM STATEMENT 7
- E. PURPOSE STATEMENT 7
- F. RESEARCH DESIGN 8

II. BACKGROUND 11
- A. THE RISE OF SOCIAL MEDIA 11
  - 1. Social Media as a Community 12
  - 2. Social Media and Activism 12
  - 3. Social Media and Political Appointees 13
  - 4. Social Media and Marketing 13
- B. WHAT MAKES A MEME, A MEME? 14
- C. WHAT IS INFORMATION DISORDER? 18
- D. A MEME'S ROLE IN INFORMATION DISORDER CAMPAIGNS 22
- E. TWITTER'S ROLE IN INFORMATION DISORDER 24

III. RELATED WORK 27
- A. RESEARCH ON INFORMATION DISORDER WITH MEMES 27
  - 1. Political Memes and Fake News Discourses on Instagram 27
  - 2. Inferring Social Influence and Meme Interaction with Hawkes Processes 27
  - 3. The Evolution of Political Memes: Detecting and Characterizing Internet Memes with Multi-Modal Deep Learning 28
- B. RESEARCH ON INFORMATION DISORDER USING TWITTER 28
  - 1. Coronavirus Goes Viral: Quantifying the COVID-19 Misinformation Epidemic on Twitter 29
  - 2. The Spread of True and False News Online 29
- C. INFLUENCE EFFECTIVENESS OF INFORMATION DISORDER 30
  - 1. Does Russian Propaganda Work? 30

Page 2463 of 3957

2. Understanding What Makes Terrorist Groups' Propaganda Effective: An Integrative Complexity Analysis of ISIL and Al Qaeda 31
D. CATEGORIZATION AND DECISION MAKING 31
1. Interference Effects of Categorization on Decision Making 32
2. An Evidential Dynamical Model to Predict the Interference Effect of Categorization on Decision Making Results 32

IV. METHODOLOGY 35
A. HYPOTHESES 35
B. EXPERIMENTAL DESIGN OVERVIEW 36
C. TWEETS AND MEMES USED 39
1. Tweets Used in the Experimental Design 39
2. Memetics Used in Experimental Design 53
D. QUALTRICS 67
1. Steps to Create the Experiment Designed in this Thesis 68
2. Testing the Survey 78
E. LIMITATIONS 78

V. FUTURE WORK, IMPLICATIONS, CONCLUSION 79
A. FUTURE WORK 79
B. IMPLICATIONS 79
C. CONCLUSION 80

LIST OF REFERENCES 81

INITIAL DISTRIBUTION LIST 91

Page 2464 of 3957

LIST OF FIGURES

Figure 1. A breakdown of a Tweet. Adapted from Twitter (2021). 3

Figure 2. Image macro meme....4

Figure 3. Slim Jim and BarkBox image macro memes. Source: Slimjim (2021) and BarkBox (2021).....5

Figure 4. 2016 Election meme created and propagated by foreign state actors. Source: *National Post* Staff (2017).....18

Figure 5. Components of information disorder. Source: Wardle and Derakhshan (2017).....20

Figure 6. Experiment flow chart.....37

Figure 7. Tweet number one. Adapted from *The New York Times* (2021). 40

Figure 8. Tweet number two. Adapted from *The New York Times* (2021). 41

Figure 9. Tweet number three. Adapted from *The New York Times* (2021). 42

Figure 10. Tweet number four. Adapted from *The New York Times* (2021). 43

Figure 11. Tweet number five. Adapted from *The New York Times* (2021). 44

Figure 12. Tweet number six. Adapted from *The New York Times* (2021). 45

Figure 13. Tweet number seven. Adapted from *The New York Times* (2021). 46

Figure 14. Tweet number eight. Adapted from *The New York Times* (2021). 47

Figure 15. Tweet number nine. Adapted from *The New York Times* (2021). 48

Figure 16. Tweet number ten. Adapted from *The New York Times* (2021). 49

Figure 17. Tweet number eleven. Adapted from *The New York Times* (2021).....50

Figure 18. Tweet number twelve. Adapted from *The New York Times* (2021). 51

Figure 19. Tweet number thirteen. Adapted from The *New York Times* (2021).....52

Figure 20. Tweet number fourteen. Adapted from *The New York Times* (2021).....53

Figure 21. Meme number one. Adapted from Bremmer (2020). 54

Page 2465 of 3957

Figure 22. Meme number two. Adapted from Lynas (2020). 55
Figure 23. Meme number three. Adapted from Lynas (2020). 56
Figure 24. Meme number four. Adapted from Lynas (2020).....57
Figure 25. Meme number five. Adapted from Lewis (2020). 58
Figure 26. Meme number six. Adapted from Pinsker (2021), Beals (2020), Bazelon (2020), & Clarke (2020). 59
Figure 27. Meme number seven. Adapted from Lee (2020), & Naishadham et al. (2020). 60
Figure 28. Meme number eight. Adapted from Pitofsky (2021).....61
Figure 29. Meme number nine. Adapted from Lynas (2020). 62
Figure 30. Meme number ten. Adapted from CDC (2021). 63
Figure 31. Meme number eleven. Adapted from Pitofsky (2020). 64
Figure 32. Meme number twelve. Adapted from Klepper et al. (2021).....65
Figure 33. Meme number thirteen. Adapted from Lynas (2020). 66
Figure 34. Meme number fourteen. Adapted from Lewis (2020). 67
Figure 35. Question one example.....68
Figure 36. Question two example.....69
Figure 37. Question three example.....69
Figure 38. Question four example.....70
Figure 39. Question five example 71
Figure 40. No initial categorization block example 72
Figure 41. Initial categorization block example.....73
Figure 42. Complete Qualtrics image library.....74
Figure 43. End of survey acknowledgement.....75
Figure 44. First set of the survey flow.....76

Page 2466 of 3957

Figure 45. Second set of the survey flow 77

Figure 46. Preview of the survey.....78

Page 2467 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Variables collected during the experiment 36

Page 2469 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Throughout the writing process, Dr. Canan was committed to helping me succeed, despite my tendency toward procrastination. Thank you for believing in a thesis all about memes, Mustafa! Without you, these pages would not exist.

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2472 of 3957

I. INTRODUCTION

A. SOCIAL MEDIA, THE NEWS, AND MARKETING: WHAT COULD GO WRONG?

According to a 2019 study by the Pew Research Center, 55% of U.S. adults get their news from social media (Suciu, 2019). This figure is up 8% since 2018 and has likely increased more due to the 2020 global pandemic (Suciu, 2019). Currently, Facebook accounts for 52% of said news, while Twitter is at 17% and Instagram is 14% (Suciu, 2019). In addition to news, many social media users are seeking product discovery (Gorman, 2021). According to Global Web Index, a leading marketing firm for targeted advertisements, 42% of individuals use social media for brand/merchandise research and roughly "24% of global internet users have clicked on a sponsored post or ad on social media" during any given month (Gorman, 2021, sec. "Who clicks on social media ads?"). Although many people assume that articles are the main source of news, and digital marketing advertisements for product sales, short text blurbs, like Tweets (Figure 1), and quick scroll images, like image macro memes (Figure 2), are becoming a mainstream and rapid source for current events and brand awareness (Boulter & Bolaji, 2020; Mottola, 2020). Occasionally, the worlds of social media advertising and news will collide, utilizing algorithms (discussed in Chapter II) to target certain audiences for bipartisan or social justice topics (Weise, 2018). Unfortunately, this type of intersection creates a massive vulnerability to American citizens, opening them up to influence campaigns run by external groups.

While social media does a great job of disseminating word rapidly and to a number of audiences, this form of mass distribution opens doors for a new type of information operation. Russia, a nation on the forefront of this movement, has been infiltrating social media for many years (Wardle & Derakhshan, 2017). Notably, as described in a Senate Intelligence Committee report, the 2016 election was fraught with memes and Twitter accounts propagating false information aimed at dividing our nation (2019). Much of this misinformation took the form of targeted advertisements, like the one beginning with "African-Americans have to choose between old Hillary Clinton and rich Donald Trump,"

Page 2473 of 3957

that was directly displayed to Facebook users identifying as Hispanic, Asian American, or African-American (Weise, 2018, para. 8). Furthermore, after seemingly failed influence attempts, China agreed to work with Russia in current and future information operations against the Western nations, who they claim to have distorted the narrative around the current global pandemic (Weitz, 2020). With that in mind, it is safe to say that foreign actors have successfully attempted to influence the thoughts and actions of American citizens, and they will only improve at it. These tools (i.e., Tweets, memes, and targeted advertisements) are assisting our peer-adversaries in completing their mission, making it vitally important that we understand who is most susceptible to online delivered information weapons.

B. KEY INFORMATION DISSEMINATION TOOLS: TWEETS AND IMAGE MACRO MEMES

Using no more than 280 characters at a time, Twitter (2021a), an online social media platform, allows users to instantly express their thoughts and feelings to the world at large, describing themselves as serving public conversations. The organization believes "you should be able to speak your mind and find credible information easily" (Twitter, 2021c, sec. "Healthy conversations"). The Twittersphere is not exclusive to individual users; companies and organizations may use the platform to promote new products, share news articles, or show support for current change initiatives. Figure 1, containing a real Tweet from *The New York Times* Twitter page, is annotated to pinpoint specific aspects of Tweets that, as detailed in a later chapter, were altered during creation of the false Tweets in the experimental design of this thesis.

Page 2474 of 3957

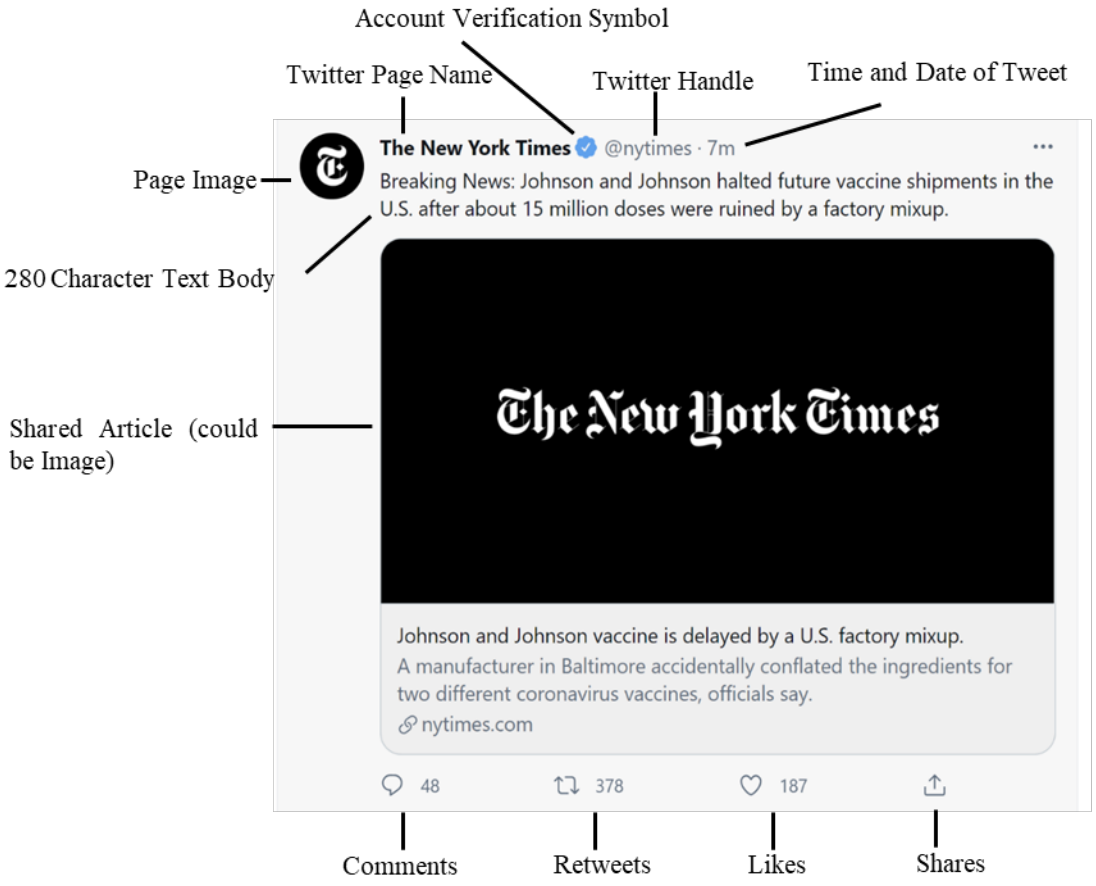


Figure 1. A breakdown of a Tweet. Adapted from Twitter (2021).

Image macro memes, like Figure 2, are likely what comes to mind when the word "meme" is used in conversation or writing; they contain text on top of a widely distributed photograph (Mina, 2019). For that reason, image macro memes are what will be used for this experimental design. However, these digital objects consist of more than images with text, encompassing videos, performances, and selfies as well (Mina, 2019). Image macro memes appear on all social media platforms, including Twitter, Facebook, Instagram, Tik Tok, Reddit, etc., and may be shared by any user in a matter of seconds.

Page 2475 of 3957

Figure 2. Image macro meme

C. WHAT MAKES MEMETIC RESEARCH IMPORTANT?

Whether a social media user is on Twitter, Facebook, Instagram, or another popular application, they are bound to see memes daily. These memes, even if the viewer does not realize it, are being created with specific goals in mind; through humor and irony (Burroughs, 2020), memes serve as marketing strategies, evident by Fashion Nova's Instagram takeover (Raaf, 2018), political campaign ads and propaganda (Burroughs, 2020), extremist recruitment (Zitser, 2021), or foreign influence tools (Wardle & Derakhshan, 2017). Because this information dissemination tactic has evolved from simple humorous and ironic images into manipulation techniques, it is paramount that society gain a better understanding of how they propagate.

With undeniable benefits to marketing on social media, it is not surprising that 96% of small businesses use it for their marketing strategy (Shepherd, 2021). In fact, social media marketing use drives an increase in customer loyalty, leading consumers to spend

40% more money once engaged with the business via a follow, like share, etc. (Shepherd, 2021). Because the preponderance of social media users are on the applications to laugh, memes as a marketing tool are growing in popularity (Sprout Social, 2018). Brands ranging from Slim Jim to BarkBox are currently utilizing image macro memes (Barker, 2021) like the ones displayed in Figure 3. Slim Jim, whose official Instagram page is covered in image macro memes, has amassed a following of 1.3 million people (slimjim, 2021). With such a large following, Slim Jim holds a lot of influence; if they chose to start posting politically driven memetics vice meat stick centric ones, there is no telling what impact they would have. Luckily, however, most companies leave the controversial memes to individual users, extremist groups, or foreign state actors, who may or may not have a following near that of Slim Jim.

Figure 3. Slim Jim and BarkBox image macro memes. Source: Slimjim (2021) and BarkBox (2021).

According to the *Washington Post*, the 2016 political primaries were "the most-memed election in U.S. history" (Heiskanen, 2017, p. 1). However, one can make a case that the 2020 election took the crown; upon a quick Google search, millions of articles appear characterizing an abundance of memes from the most recent presidential election.

Page 2477 of 3957

For example, *Inside Hook* published a piece entitled "Election Week 2020, As Told in Memes," while *Cosmopolitan* wrote "These 2020 U.S. Presidential Election Memes Will Keep You Laughing Until Inauguration Day" (Isaac, 2020; Mahan, 2020). Prior to the 2020 election, copious amounts of politically driven memetics tended to point out candidate hypocrisy or critique policy positions (Heiskanen, 2017). Due to the lack of literature surrounding the most recent election, it is difficult to say whether the 2020 memes were focused on the same central points. However, upon review of the two articles mentioned above, the 2020 election may have encompassed a wider breadth of topics, like the removal of Donald Trump from office (Isaac, 2020). Interestingly, politically driven memes like the ones mentioned propagate quicker within groups of the same political ideology, making it difficult to tell whether they influence voter action (Heiskanen, 2017). Despite the uncertainty behind the influential factor of memetics, many extremist groups and foreign actors still use them to gain group members or push narratives that benefit them (Graff, 2018).

According to the CEO of the Center for Countering Digital Hate (CCDH), a not-for-profit organization aimed at "disrupting the architecture of online hate and misinformation" (CCDH, 2021, sec. "About"), "Instagram is actively pulling its predominantly young users down an extremist rabbit hole" (Zitser, 2021, para. 5). At the forefront of these extremist groups is the neo-Nazis (Zitser, 2021). HOPE Not Hate, a United Kingdom based group focused on defeating extremism (HOPE not hate, 2021), names Instagram as the "platform of choice" for radicalizing the young generation into neo-Nazi supporters (Zitser, 2021, para. 7). According to a researcher at HOPE Not Hate, memes are the easiest way to spread these ideologies, allowing propagators to hide extremism under humor and irony (Zitser, 2021). Once a user interacts with extremist posts on Instagram, the algorithm pushes like-information to the "explore" page on the users individual account, only increasing the content they encounter (Warren, 2021). According to the social media site itself, "interest" is the number one driving factor for feed posts, pushing items believed to be "liked" by the user to the top of their screen (Warren, 2021). This means that, while one individual may see cookie decorating and cake baking, another user will view neo-Nazi and racially charged hate.

If extremist groups are using memetics to boost membership, it should come as no surprise that foreign actors, specifically Russia and China, are using them to spread propaganda and pit our nation against itself (Gaff, 2018; Kao & Li, 2020). In fact, an attempt at destabilization through predominantly politically driven misinformation memetics has become commonplace (Weitz, 2020). Things like political candidates, second amendment rights, and even the COVID-19 pandemic are drivers for foreign influence operations (Weitz, 2020; Wyrich, 2017). For example, in Hong Kong, a number of students rapidly spread COVID-19 memes with hashtags that placed blame on China and its people, hoping to continue longstanding anti-Chinese movements in the area (McMinn, 2020). As discussed, however, the effectiveness of memes at dividing a nation is unknown (Heiskanen, 2021); this thesis and experimental design will address this gap in the literature.

D. PROBLEM STATEMENT

Memes have taken center stage in discussions about marketing, politics, extremist recruitment, foreign state actors, and even the COVID-19 pandemic (Burroughs, 2020). The memes, which include a combination of perceptual cues/elements (Figure 2), traditionally manifest themselves as images, texts, videos, performative pieces, and selfies (Mina, 2019). However, despite their immense popularity in social media and online environments, the field remains understudied. This omnipresence of memetics gives rise to an important question: How do memes affect the acceptance and propagation of false information? If it is determined that including memes in perceptual stimuli can give rise to systemic variation by age, gender, and education level when propagating false information, they can be used as leverage in all the methods listed above, especially influence operation targeting endeavors.

E. PURPOSE STATEMENT

The purpose of this thesis is to design an experiment that explores how memes affect the acceptance and propagation of the false information within various ages, education levels, and gender groups, when compared to text blurbs (Tweets) alone. In order to achieve that, an experiment was designed through the Naval Postgraduate School via the

Page 2479 of 3957

online experimental platform Qualitrics, which, when performed, may be delivered via Mechanical Turk (MTURK). The independent variables are the age, education level, and gender, which are provided by the experiment participants. The dependent variable is the participant willingness to interact with the presented Tweets and memes and their reason for doing so. The manipulated variable is the presentation of Tweets and image macro memes that contain false information.

F. RESEARCH DESIGN

After completing an in-depth literature review, this thesis utilizes experimental design to address the purpose and problem statements. It expounds upon how the experiment was built, including the reasoning for every single Tweet and meme contained. Following methods, the implications for completing the experiment and recommendations for future work are detailed. The overarching experimental design for this thesis focuses on answering the below hypotheses through an analysis of various participant response to a series of Tweets and image macro memes riddled with false information. The survey created helps researchers examine whether age, education level, and/or gender correlates to the acceptance and propagation of false information spread through image macro memes, comparing it to the acceptance and propagation of false information spread exclusively through text blurbs. Additionally, as summarized in Chapter III, it will test the effects of initial categorization on survey response. The experiment's null hypothesis is that age, education level, and gender have no influence on the rate of acceptance of false information via memes. This experiment is designed to test the following hypotheses:

- HA1: Age correlates to the acceptance of false information spread through a Tweet and an image macro meme.
- HA2: Education level correlates to the acceptance of false information spread through a Tweet and an image macro meme.
- HA3: Gender correlates to the acceptance of false information spread through a Tweet and an image macro meme.

Page 2480 of 3957

- HA4: Age correlates to the propagation of false information spread through a Tweet and an image macro meme.
- HA5: Education level correlates to the propagation of false information spread through a Tweet and an image macro meme.
- HA6: Gender correlates to the propagation of false information spread through a Tweet and an image macro meme.
- HA7: Initial categorization has an effect on the acceptance of false information spread through Tweets and image macro memes.
- HA8: Memes will be interacted with (by indication of liking, commenting, or sharing) at a different rate than Tweets.

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2482 of 3957

II. BACKGROUND

To better understand the interplay of social media and influence, a deep dive into the topics of social media, memetics, information disorder, and initial categorization is necessary. By unraveling intricacies within the aforementioned topics, one will gain a better understanding of the literature review in Chapter III and the thought process behind the experimental design detailed in Chapter IV.

A. THE RISE OF SOCIAL MEDIA

While social networking took root in the 1960s with the invention of ARPANET, most social media sites were not built until the 1990s, lining up with the commercial launch of the internet (Edosomwan et al., 2011). Although many social media platforms came before it, MySpace was the most popular social media site in the United States until 2008, when Facebook took over (Edosomwan et al., 2011). Currently, YouTube, Facebook, and Instagram are the most commonly used platforms, with over 40% of all adults using all three applications (Auxier & Anderson, 2021). Twitter, the seventh most popular site, is being used by 23% of adults (Auxier & Anderson, 2021). Naturally, with such a large number of users, social media comes with pros and cons; while these platforms allow individuals from all over the world to connect and find common ground on various topics, it has been shown to increase depression and anxiety, as well as lower sleep quality and self-esteem in its users (Mammoser, 2018). Depression, anxiety, and low self-esteem tend to occur when users over analyze their lives versus another user's life (Mammoser, 2018). Additionally, it has been determined that covering distressing events via media, whether it be posts online or news casts, is harmful to viewers, sometimes even leading to higher acute stress than being at the distressing event itself (O'Brien et al., 2020). Despite knowing that, social media use has been on a steady rise since its inception (Auxier & Anderson, 2021), forming communities for people, serving as a platform for activism and politics, and helping organizations/companies market products and ideas.

Page 2483 of 3957

1. Social Media as a Community

With the rise of social media, researchers began looking into Twitter, Facebook, Instagram, and all other platforms for signs of online communities. What they found was, through the social network perspective, many groups on social media meet the requirements to be considered a community (Gruzd & Haythornthwaite, 2013). By identifying the actors, informal and formal ties, roles, and cliques formed on these sites, one can begin to see how seemingly random interactions may grow into full communities (Gruzd & Haythornthwaite, 2013). For example, two million people follow the account "WeRateDogs" on Instagram. On Twitter, nine million people follow the same account, ran by the same individual. Every day, followers will send pictures of their dogs to Max, the account owner, and he posts them for all to see. The hashtags, which may include something like "#seniorpupsaturday" is then used by those in Max's community, which is evident by clicking on said hashtag and reviewing the similar posts (WeRateDogs, 2021c). In addition, Max has created a merchandise line that all followers can immediately recognize; his "tell your dog I said hi" decals and masks easily help identify members of the WeRateDogs community (WeRateDogs, 2021a). Finally, Max regularly posts GoFundMe pages for dogs in need of medical care, which always get fully funded in under thirty minutes (Weratedogs, 2021b). This example highlights the exchange of information, social support, and play that occurs between members of the WeRateDogs community, legitimizing social media as a community through the lens of the social network perspective (Gruzd & Haythornthwaite, 2013).

2. Social Media and Activism

From the inception of social media, people have been using the platforms to spread awareness for social issues (Weise, 2018). In 2020 alone, nearly a quarter of users changed their viewpoints on a social justice topic based on posts reviewed on one of the many platforms (Perrin, 2020); most of those users stated that "Black Lives Matter" (BLM) as the driver for that change (Perrin, 2020). BLM, which began in 2014 after the deaths of Michael Brown and Eric Garner, started as a movement on Twitter (Carney, 2016). Since 2014, BLM has made multiple resurgences, the most recent beginning in 2020 with the

Page 2484 of 3957

death of George Floyd (McLaughlin, 2020). After the video of George Floyd's death circulated rapidly via social media, more than 20 million people began protesting throughout the United States (McLaughlin, 2020). Despite a worldwide pandemic, this social justice issue, which began and spread via social media, was able to move millions to action, truly highlighting the power of these platforms. Nikita Carney, a researcher with the University of California, Santa Barbara and Louisiana State University, believes this occurs because social media has increased the accessibility to information that previously prevented citizens without access to information from having opinions (2016). While BLM is not the only social issue that has been elevated to grand heights by social media, it is the most influential one to occur in the last year.

3. Social Media and Political Appointees

United States political candidates and elected officials rely heavily on social media to reach a broader public. As of April 2021, the official White House Instagram (@whitehouse) account has over six-million followers, and President Joe Biden (@joebiden) and Vice President Kamala Harris (@kamalaharris) have a combined total of over 32 million followers. On Twitter, the two leaders have just under that same mark (2021). While the use of social media platforms started with former President Barack Obama, his successor, Donald Trump, was the one to employ it nearly every few hours for four years, setting a new precedent (Wharton Business Daily, 2020). Through research efforts, it has been shown that appointed officials actually get large increases in support when they utilize this new communication tool (Wharton Business Daily, 2020). This support increase is hypothesized to occur due to the feeling of accessibility that it brings to constituents (Wharton Business Daily, 2020). Additionally, the utilization of social media by political newcomers may help reduce the barrier to entry into political circles, giving hopefuls a voice and platform without the large funding requirements in the past (Wharton Business Daily, 2020).

4. Social Media and Marketing

Social media marketing may have started as emplaced advertisements, but it now encompasses that and much more; influencers, who are social media users with followings

Page 2485 of 3957

large enough to shape attitudes, partner with brands to bring awareness to products and lifestyle trends (Glucksman, 2017). Through tracking software that monitors engagement with a sponsored post, influencers are able to make money from their partners (Glucksman, 2017). According to experts, for a sponsored post, Instagram influencers should receive $1,000 per 100,000 followers, which allows these individuals/accounts to make a living doing this type of marketing (Mathew, 2018). However, not only is influencer marketing good for the influencer, but 89% of marketers have seen equal or improved return on investment when compared to other marketing techniques (MediaKix, 2019).

Who are these influencers then? Well, some of the most successful ones are seemingly normal accounts that rise to influencer level, not pop culture celebrities (Jin et al., 2019). This is because, as research has shown, people who are perceived to be "normal" or "one of us" are viewed as more sociable and trustworthy to social media users, making them better candidates for marketing partnerships (Jin et al., 2019). While the obvious influencer is the popular person, like Alicia McCarvell who has over 300,000 followers (aliciamccarvell, 2021), other influencers include accounts like @sarcasm_only or @betches, who keep themselves relatively anonymous and post predominantly comedy and meme driven media to their multi-million user followings (2021).

B. WHAT MAKES A MEME, A MEME?

In 1978, Richard Dawkins began using the word "meme" to describe cultural actions that disseminate like genetic material (Mina, 2019). The term has since been coined as the internet phenomenon that describes digital objects sharing the common characteristics of transformation, awareness, imitation, and circulation (Mina, 2019). Those digital objects can take the form of images, texts, videos, performative pieces, and selfies (Mina, 2019). While all listed instances are covered under the formal definition of meme, the image is the most recognizable and the selected independent variable for this study. The image is broken down into two forms: image meme and image macro (Mina, 2019). When an image meme includes text, it becomes an image macro, as shown in Figure 2 (Mina, 2019). Because any individual can create a meme whenever they desire (through websites like imgflip.com), it is very difficult to get an accurate number of their existence

Page 2486 of 3957

online; however, over two years ago, researchers at University College London were able to easily collect 100,700,000 image macro memes for analysis (Cole, 2018). While readers can reflect on that number and hypothesize how many memes exist today, one can assume that the market is saturated.

Although memes are short units of information, they generally convey a specific narrative (Saint Laurent et al., 2021). These narratives, while predominately humorous or ironic, require that the viewer have an established knowledge base in the topic presented (Saint Laurent et al., 2021). While these digital artifacts do not present a plot like those of traditional stories, they do formulate with a beginning, middle, and ending in mind (Saint Laurent et al., 2021). Additionally, memes tend to reference specific characters, like Kermit sipping tea, helping to bring meaning to a variety of topics based on similar context (Saint Laurent et al., 2021). Despite the lack of a central axis, the character development and crossover, as well as the structured manner in which memes fade in and out of relevancy, equates them to mini stories (Saint Laurent et al., 2021).

While image macro memes can be made and posted to Twitter, Instagram, Reddit, 4Chan, etc., by anyone, they are not guaranteed to be seen by a wide audience (aka go "viral"). According to Lin Wang and Brendan Wood, both researchers at the University of New Brunswick, meme propagation occurs like an infectious virus; through social interaction, meme spread spikes early (infectious stage) but begins to decay once a certain number of people have reviewed the content or it begins to lack relevancy (2011). To prove their claim, Wang and Wood utilized a modified susceptible, infective, and recovered (SIR) compartmental modeling approach, which is commonly used by epidemiologist to compute virus spread (2011). Using the Google Trends tool, the researchers were able to utilize historical search data to graphically depict the spread of popular topics (Wang & Wood, 2011). As hypothesized, Wang and Wood found that search volume spikes sharply within the first days that a newly introduced idea becomes content, then begins to taper off after the allure has run out (2011). Recently, however, this concept of going "viral" is being scrutinized by internet culture enthusiasts.

Abby Ohleheiser, a senior editor for the *MIT Technology Review*, makes a case for abolishing the use of the term "viral," and it is not simply because of the real virus

Page 2487 of 3957

spreading throughout the world (2020); Abby, through a conversation with Whitney Phillips, a Syracuse university assistant professor, discusses that "viral" should be reserved for popular online digital objects that contain misinformation (2020). Whitney Phillips points out that, because spreading misinformation, whether knowingly or not, causes harm, like a real virus does, the term should be reserved solely for those instances (Ohleheiser, 2020). Additionally, Ohleheiser considers the role that algorithms play in propagating memetics; as she states, "authentic popularity isn't necessarily real: algorithms incentivize content that people are going to engage with, accelerating its spread, and people have gotten really good at manipulating [it]" (2020, sec. "Manipulated popularity").

Social media algorithms, like those mentioned by Abby Ohleheiser, drive what content a user sees by analyzing what kinds of posts they interact with regularly (Etter & Albu, 2021). Traditionally, a user will notice that their content is personalized, displaying memes that center on topics they commonly like, share, and comment on (Etter & Albu, 2021). The coding for these algorithms allows users to become stuck in loops that display only one or two topics, giving rise to organized collectives of like-minded users (Etter &Albu, 2021). As briefly discussed in Chapter I, this continual reemphasis of specific content may expose certain users to constant extremist viewpoints, like Instagram and neo-Nazism (Zitser, 2021).

From its start in 2010, Instagram has amassed over one billion users (Mohsin, 2021). Of those users, 71% are age 34 or younger and spend a daily average of 53 minutes on the application (Mohsin, 2021). While those numbers sound shocking, the age group and usage time do not account for the 2020 global pandemic stay-at-home orders and have likely increased in the last year. When a user first signs up for an Instagram account, they begin following other accounts and posting to their feed. The accounts range from favorite celebrities, clothing brands, activist groups, political ideations, humor, and many more. Commonly, a user will find a form of memetic on every type of account; whether it be the recreation of popular internet dances, ironic image macro memes making fun of the president, or 10 second videos promoting a new product, a user is not likely to use Instagram without seeing a number of memes. Facebook, another top social networking platform, accounts for the preponderance of these types of digital objects. Much like

Page 2488 of 3957

Instagram, by allowing users to like, share, and comment on things, Facebook enables meme propagation at a very high rate.

What, then, is the algorithm influenced saturated meme market sharing with the world? Well, image macro memes tend to promote products, meld ideologies together, and encourage social activism. Through memetic marketing, like the examples shown in Figure 3 (Slim Jim and BarkBox), companies are able to increase consumer attitudes towards a product, which leads to an increase in purchases (Lee et al., 2019). Co-authors Lee, Liang, Liao, and Chen were able to show this concept by surveying 380 Taiwanese Facebook users about their thoughts towards internet marketing memes (2019). By focusing on both utilitarian attitudes, like functionality representation, and hedonic attitudes, like a representation of fun, the researchers were able to conclude that companies who create memes with hedonic attitudes as the focus can boost online purchases (2019).

Interestingly, memes as marketing strategies are being utilized worldwide, not exclusively in the United States and Asia. In India, a prominent influencer marketing company called Buzzoka has begun meme incorporation (BW Online Bureau, 2020). In fact, their CEO Ashutosh Harbola was quoted saying, “Memes have a definite potential to become a major phenomenon and we as a company are committed to taking the first foot forward” (BW Online Bureau, 2020, para. 4). SBI, after experiencing wide success from a previous meme driven campaign, joined in on a viral Pakistani meme called “Pawri,” which was initially circulated by Pakistani influencer Dananeer Mobeen (The International News, 2021). This “Pawri” meme, meaning “party” in Urdu, was then embraced by a multitude of Pakistani and Indian companies, like Netflix India, Zomato, Swiggy, and Oyo Rooms (News18, 2021). The ability for India and Pakistan to find common ground via memetics, despite the possibility of warfare between the two nations (National Intelligence Council, 2021), highlights the online significant influence generated through memetics.

It is important to understand how memetics drive narratives for controversial topics associated with politics and religion. As stitching devices, memes blend multiple internet platforms, narratives and ideologies, and geopolitics together, unifying people based on shared digital media (Burroughs, 2020). These stitched devices then become calcified and weaponized ideology (Burroughs, 2020); this commonly occurs in politics, like what was

Page 2489 of 3957

seen during the 2016 election season (Figure 4). Too often, memes stitch politics with religion, which is demonstrated rather frequently by conservative individuals or foreign state actors (Burroughs, 2020). Summarily, Benjamin Burroughs, an emerging media researcher for the University of Nevada, explains that "memes have expanded beyond popular culture and humor, they [have] become the grounds for social activism, merging the political and social" ideals (2020, pp. 191-200); this description raises the question that, if memes are now used for social activism, politics, and marketing, what effect do they have on propagating false information online?

Figure 4. 2016 Election meme created and propagated by foreign state actors. Source: *National Post* Staff (2017).

C. WHAT IS INFORMATION DISORDER?

To grasp a better understanding of a particular environment, an individual must gather information (Nissen, 2014); according to Mark Nissen, a professor at the Naval Postgraduate School, one is said to have gathered information when they can glean meaning from a situation (2014). For example, if you were to give the number 120/80 to a

person on the street, they would not know what you wanted them to do with it (Nissen, 2014). Are they dividing 120 by 80? Is it some sort of ratio? After telling the individual that 120/80 is a blood pressure reading, the numbers are transformed from data to information (Nissen, 2014). Depending on the level of knowledge the person has on blood pressure, they can determine what to do with said information (Nissen, 2014). As mentioned previously, memes act as stitching devices, pulling different ideologies and narratives together. Thus, unless a meme viewer can place meaning behind the digital object, the image is simply data, not information. The issue then becomes this: Is the meaning a viewer places on the meme accurate or is the creator attempting to create a false meaning in the viewers mind? If the meaning gleaned from the meme is untrue, the creator has succeeded in employing information disorder.

In 2017, Claire Wardle and Hossein Derakhshan created a new conceptual framework to examine information disorder (Figure 5). This framework breaks down the spread of false information into three categories: misinformation, disinformation, and malinformation and classifies them as "false" and/or "harmful" (cause an adverse effect) (Wardle & Derakhshan, 2017). Misinformation is the spread of false information without the intent of causing an adverse effect, or harm (Wardle & Derakhshan, 2017). Disinformation, on the other hand, is the spread of false information with the intent to cause harm (Wardle & Derakhshan, 2017). Finally, weaponized true information, known as Malinformation. that is spread with the intent to cause an adverse effect, will traditionally appear out of context and frame the information in a way that is no longer truthful (Canan & Akil, 2020; Wardle & Derakhshan, 2017). Commonly, individuals refer to the notion of information disorder as "fake news," which poorly describes the complexities of this domain and encourages a lack of trust in mainstream media (Wardle & Derakhshan, 2017). In an attempt to prevent the undermining of free press, the term information disorder (or one of the three respective types of information), vice fake news, will be used throughout this thesis.

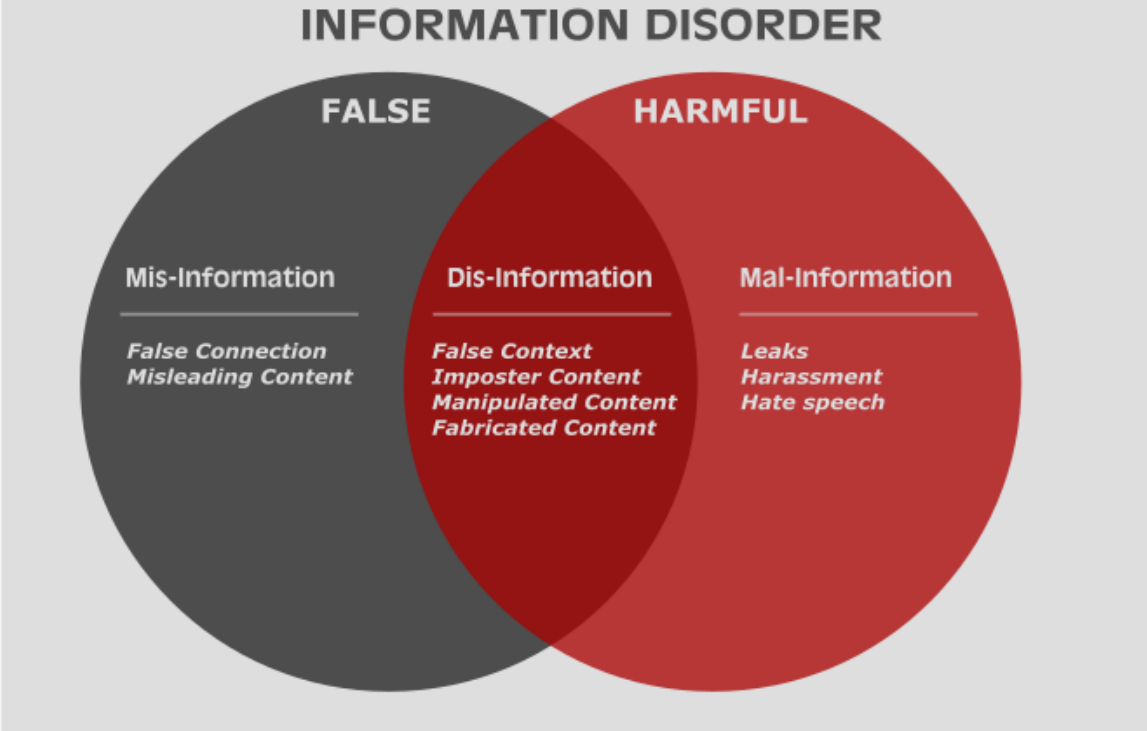


Figure 5. Components of information disorder. Source: Wardle and Derakhshan (2017).

This concept of information disorder is commonly applied in politics (Andrejevic, 2020), journalism (Wardle, 2020), and even marketing (Liu et al., 2020). In fact, according to former President Obama's communications director Dan Pfeiffer, "every policy, speech, interview, Tweet, meme, video, and photograph needs to be thought of as a piece of content that can be used to persuade voters" (Pfeiffer, 2020, para. 7). In the current political realm, information disorder serves a predominant right-leaning audience with an overall goal of preventing change rather than calling for it (Andrejevic, 2020). Commonly, a disinformation creator will weaponize irony, praying on preexisting prejudices with a focus on what can be achieved through widespread distribution (Andrejevic, 2020). For example, in 2018, Cambridge Analytica, a data firm utilized by former President Donald Trump's campaign, was shown to have collected social media information on 50 million Americans in hopes of using it to manipulate voters (Rushkoff et al., 2018). This realization led Congress to call upon Facebook CEO Mark Zuckerberg to testify on his company's data collection practices (Rushkoff et al., 2018). To combat the use of political information

disorder, Mark Andrejevic, a communications and media studies professor and researcher, states that we must develop conditions for recognition vice countering information disorder with more information disorder (2020).

Journalism, which can encompass political information disorder, constitutes a much larger realm of misinformation and disinformation (Wardle, 2020); journalism opens the door to false narratives about any topic, whether it be celebrity news or the COVID-19 pandemic (Wardle, 2020). During the era of former president Donald Trump, "fake news" became a way to describe subpar reporting by journalist in mainstream media (Wardle, 2020). However, "fake news" in journalism truly refers to information disorder and consists of manipulation in the form of "satire, clickbait, inaccurate captions, visuals, statistics, genuine content shared out of context, manipulated quotes and imagery, and outright fabricated stories" (Wardle, 2020, pp. 71-85). In order to combat this issue, Claire Wardle, the co-founder and Leader of the non-profit mis and disinformation research organization *First Draft*, recommends more research into the scale and complexities of information disorder (Wardle & Derakhshan, 2017).

Finally, marketing, which may not be the first topic of conversation when discussing information disorder, constitutes of a large number of campaigns (Newsguard, 2021). For example, researchers Jessica Liu, Sheila McLaughlin, Adrienne Lazaro, and Bonnie Halper-Felsher investigated the marketing of e-cigarettes and marijuana use, which focuses predominantly on young adults (2020). Recognizing that social media has led to a drastic increase in the use of said smoking products, the four women set out to determine what appealed to users most (Liu et al., 2020). Through a series of interviews, they were able to conclude that tobacco and marijuana users were exposed to information about the products without even subscribing to them (Liu et al., 2020). In fact, memes were one of the most widely used digital objects leading adolescents to exposure on the subject matter (Liu et al., 2020). Interestingly, however, "participants reported awareness of the tobacco industry's underlying profit-driven motives" but chose to partake anyway (Liu et al., 2020, sec. "Lack of trust in industry"). Additionally, the participants appeared to rely heavily on their friends and social media influencers for "credible" information about e-cigarettes and marijuana use (Liu et al., 2020). The research goes on to state that "recent evidence that

Page 2493 of 3957

companies such as JUUL [e-cigarettes] use celebrities and young-looking influencers plays into this idea of trusting the source" (Liu et al., 2020, sec. "Discussion"). Liu et al.'s research accurately represents the idea that corporations, through memes and social media, can utilize information campaigns to their advantage; despite the research suggesting long-standing health problems from smoking (Blaha, 2021), they are still able to mold a narrative and sell products.

Allowing information to flow without many restrictions, like what occurs online and on social media, leads to issues for individuals attempting to sort fact from fiction. The predominance of problems that arise when analyzing information disorder occur in the mass communication and media psychology fields (Bowman & Cohen, 2020). According to Nicholas Bowman and Elizabeth Cohen, individuals face issues detecting false information due to the following reasons: cognitive dissonance, confirmation biases, cognitive shortcuts, emotional responses, social influences, mistrust, and misunderstandings (2020). After detailing the correlations between the aforementioned terms and information disorder, the authors acknowledge that they have no answers to solve the underlying problem (Bowman & Cohen, 2020). This lack of viable solutions sets the stage for a wide array of research in the area of information disorder, including the experiment designed in response to the hypotheses proposed in this thesis proposal.

D. A MEME'S ROLE IN INFORMATION DISORDER CAMPAIGNS

Briefly discussed above and in Chapter I, memes tend to blend different topics together with the intent of invoking an emotional response from the viewer (Posetti & Bontcheva, 2020). Knowing that, many state and non-state actors have begun using memes to impart meaning on topics that fit their narrative, not the true narrative (U.S. Senate, 2019). Since the 2016 presidential election, Russia has continued to "infiltrate audiences on both the left and the right, and try to pit them against each other across race, socioeconomic status, religion, and any social issue" (Graff, 2018, para. 12). In 2019, this accusation was further supported on a national level by volume two of the Select Committee on Intelligence report from the U.S. Senate, which detailed Russia's social media use during said election. For example, Figure 4 shows an image propagated on social

Page 2494 of 3957

media by Russia in 2016 (Wyrich, 2017). These attacks are conducted by a corporation known as the Internet Research Agency (IRA), which is directed by Yevgeniy Viktorovich Prigozhin, a close ally of Vladimir Putin (Graff, 2018). Within the agency, Prigozhin funded an operation known as "Project Lakhta," whose purpose was to widen the political divide within the United States (Graff, 2018). Additionally, after failed attempts to influence American attitudes via Twitter, China "built a machinery of online controls that far exceed any other country's" (Meyers & Mozur, 2019, para. 14). In fact, evidence has concluded that China is now working similarly to Russia, "promoting negative messages about other states" in an attempt to divide groups (Weitz, 2020, para. 1). Even more concerning, the two nations have agreed to work together in future disinformation campaigns (Weitz, 2020). The success that Russia has seen in operations waged at free societies, specifically in the 2016 election, should raise concerns for all American citizens, especially if two peer threats are now corroborating (Calabresi, 2017; Weitz, 2020).

Although 2016 was previously considered the most meme-filled presidential election, according to *CNN* and *BBC* journalists, the 2020 one was even more fraught with them (Cillizza, 2020; Fabbri, 2020). Chris Cillizza, the editor for CNN's "Point" newsletter, discussed that, because former President Donald Trump was the most memed president in history, it set the stage for political campaigns run the same way (2020). Unsurprisingly, the American people like it this way; as a nation, we have become dependent on skimming for information, not actually reading, and memes allow us to gain info and move on quickly (Cillizza, 2020). According to Thomas Fabbri, a data analyst for *BBC News*, five main voices, running four overall accounts, were behind the memes of the 2020 election: Dan Bongino, Franklin Graham, James Woods, and Rafael and Omar Rivero (2020). Dan Bongino, who created and shared far-right conservative memes and commentary on his Facebook, was receiving more shares than *Fox News*, *CNN*, and *The New Work Times*, amassing to seven million in October of 2020 (Fabbri, 2020). Franklin Graham and James Woods, more conservative political election influencers, were also among the top meme generators and propagators, consistently spreading conspiracy theories about the left agenda. Finally, twins Rafael and Omar Rivero, who run the account "Occupy Democrats," were the main source of democratic memes during the election,

Page 2495 of 3957

gaining more shares than former President Trump's account on multiple occasions (Fabbri, 2020). While those five men all reside in the United States, many suspect that Russia, China, and Iran implanted their own meme driven narratives like the 2016 election (Corera, 2020). In fact, the United States government recently imposed sanctions on Russia for their state-sponsored roles in influencing the 2020 election (White House, 2021). While a full report, like that detailing the use of memes in the 2016 election will not be available for some time, it is likely that their involvement only went up after seeing previous success.

However, the use of memes in information disorder does not stop with political elections. In April 2020, the International Center for Journalists and the United Nations (UN-ICFJ) conducted a review of the disinformation being spread during the current COVID-19 pandemic (Posetti & Bontcheva, 2020). Their research revealed that, of the four main formats used for disinformation spread, memes accounted for two: emotive narrative constructs and memes, and "fraudulently altered, fabricated, or decontextualized images and videos" (Posetti & Bontcheva, 2020, sec. "The four main formats of COVID-19 disinformation"). The first format often mixes elements of truth with emotion, lies, and personal opinion, while the second format attempts to spread false stories, create confusion, and generate distrust (Posetti & Bontcheva, 2020). Although some memes have been used to propagate simple jokes or awareness of the deadliness of the virus, like Ghana's dancing pallbearers (BBC, 2020), others have been used with malicious intent; during the initial ages of COVID-19 spread, China began using memes and other techniques to convince European nations and Japan that U.S. service members spread the virus in their countries (Weitz, 2020). Additionally, the Chinese Communist Party offered to pay Twitter users with greater than 10,000 followers to share propaganda that discussed their superior handling of the pandemic (Kao & Li, 2020). The utilization of memes to spread disinformation about an ongoing pandemic solidifies the importance of studying what groups are more susceptible to this type of messaging.

E. TWITTER'S ROLE IN INFORMATION DISORDER

Dan Pfeiffer, a former White House communications director, states that "political campaigns are now modern information warfare—massive state-adjacent propaganda

Page 2496 of 3957

operations with Twitter bots that fuel outrage and drive media coverage" (Pfeiffer, 2020, para. 2). When attempting to spread a misleading narrative via Twitter, many organizations utilize software robots, or bots (Bessi & Ferrara, 2016). Bots, which have been used to influence politics since 2010, are somewhat difficult to identify with the untrained eye (Bess & Ferrara, 2016). However, using a public website and Python code, the machine learning framework known as BotOrNot identifies fake accounts with 95% accuracy (Bess & Ferrara, 2016). Utilizing BotOrNot and Twitter Search API, researchers Alessandro Bessi and Emilio Ferrara were able to show that, between the five weeks leading up to the 2016 presidential election, bots created 19% of all election-related Tweets, amassing to an astounding 3.8 million posts (2016). After identifying all the robot Tweets, Bessi and Ferrara applied SentiStrength, a sentiment analysis tool, to the bot posted Tweets and compared them to human-generated Tweets (2016). In doing so, Bessi and Ferrara showed that all Donald Trump related Tweets, human and bot, were positive in nature (2016). However, the Hilary Clinton Tweets published by bots were slightly less positive than those published by humans (2016). This difference in SentiStrength score highlights the importance of understanding who is running these bot accounts, which, in the following years, was found to be predominately Russian based offensive attacks aimed at influencing the presidential election (Timberg & Dwoskin, 2018).

While any user has the ability to post whatever he or she desires, a set of rules determine what remains online; in fact, between January 2019 and June 2020, Twitter suspended over 2.5 million accounts for things like terrorism, violent extremism, and child sexual exploitation (Twitter, 2021). While no Twitter suspensions are explicitly stated as contributing to misinformation, the website maintains guidelines and policies that restrict the spread of false information; for example, the COVID-19 misleading information policy explicitly states that "you may not use Twitter's services to share false or misleading information about COVID-19 which may lead to harm" (Twitter, 2021b, sec. "Overview"). However, after a scan of the Twittersphere (also known as Twitterverse), it is fraught with it.

Page 2497 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2498 of 3957

III. RELATED WORK

It is important to understand where current research stands on memetics, Twitter, information disorder, and initial categorization to better grasp the experimental design detailed in the follow-on chapter. The sub-sections under each section denote the names of published articles, all of which were released in 2015 or later, and the body below summarizes the research conducted and its findings.

A. RESEARCH ON INFORMATION DISORDER WITH MEMES

The following sub-sections provide insight into information disorder research that focuses on the use of memetics on social media.

1. Political Memes and Fake News Discourses on Instagram

Ahmed Al-Rawi, an Assistant Professor of News, Social Media, and Public Communication at Simon Fraser University, devoted time to researching information disorder on Instagram by collecting 293,7773 posts with a search for "#fakenews" (2021). While the tools used to collect the posts pulled from 2012 to 2018, there appeared to be a central topic: politics (Al-Rawi, 2021). Through topic modeling and pivot tables, Ahmed Al-Rawi was able to determine that 69.2% of posts utilizing fake news discourse originated from Pro-Trump communities, with the next closest community being Anti-Trump at 13.9% of posts (Al-Rawi, 2021). Interestingly, most of the top 20 active users posting #fakenews images are self-proclaimed meme sites, like @conservative_americans and @Captain_Kekistan (Al-Rawi, 2021). With this information, we can hypothesize that Pro-Trump groups are aware of information disorder around them, but it is unclear if they are simply using the fake news hashtag for anything that goes against their belief system or truly believe the shared information is inaccurate.

2. Inferring Social Influence and Meme Interaction with Hawkes Processes

In 2015, researchers Chuan Luo, Xiaolong Zheng, and Daniel Zeng, who work at the Chinese Academy of Sciences State Key Laboratory of Management and Control for

Page 2499 of 3957

Complex Systems, noticed that no model existed to explain social influence and meme interaction (2015). Their study aimed to predict what effect influence had on users posting memes about the same or a similar topic; for example, if user X posts a meme about a democratic political candidate, user Y may be influenced to post the same meme or, perhaps, a republican one (Luo et al., 2015). Using a multidimensional Hawkes processes, which is a statistical method for explaining "that each arrival increases the rate of future arrivals for some period of time" (Laub et al., 2015, p. 1), Luo, Zheng, and Zeng, created a model that accurately displayed the user behavior related to 15 million Twitter posts centered on political events in Spain (2015). This successful model application allows follow-on researchers to estimate the propagation rate of memes regarding a specific topic, whether they are misinformation or true information.

3. The Evolution of Political Memes: Detecting and Characterizing Internet Memes with Multi-Modal Deep Learning

David Beskow, Sumeet Kumar, and Kathleen Carley, researchers at the School of Computer Science Carnegie Mellon University, hypothesized that, as memes propagate, they transform, eventually reaching greater depths of the internet than traditional images (2020). Through the utilization of various deep learning methods, the researchers were able to classify 5,000 meme and 5,000 non-meme images related to the 2018 U.S. midterm elections into various groups of content, or families (Beskow et al., 2020). Using Google Vision API to conduct a reverse image lookup, Beskow, Kumar, and Carley found that the meme images returned 62,475 matching links, while the non-meme images only returned 9,536. Crunching those numbers, the researchers found that memes were four times more likely to return search results, demonstrating that memes propagate to wider areas of the internet than images alone (Beskow et al., 2020).

B. RESEARCH ON INFORMATION DISORDER USING TWITTER

The following sub-sections provide insight into information disorder research that uses Twitter as a propagation platform.

Page 2500 of 3957

1. Coronavirus Goes Viral: Quantifying the COVID-19 Misinformation Epidemic on Twitter

In 2020, 10 medical faculty at the American University of Beirut ran an experiment that reviewed Tweets based solely on COVID-19 (Kouzy et al., 2020). In a single day, the researchers collected 673 Tweets that corresponded to 14 trending hashtags (Kouzy et al., 2020). Upon review of all Tweets, Kouzy et al. found that, while 81.4% of Tweets had true information, 24.8% included misinformation, meaning some Tweets contained both (2020). Interestingly, 33.8% of personal/group Twitter accounts contained misinformation, while only 18.6% of news outlets/journalist Tweets reviewed contained misinformation (Kouzy et al., 2020). Finally, the researchers did not find any correlation between the number of likes or retweets and the occurrence of misinformation (Kouzy et al., 2020).

2. The Spread of True and False News Online

Rather than focus on the spread of false information centered on one topic, researchers Soroush Vosoughi, Deb Roy, and Sinan Aral from the Massachusetts Institute of Technology (MIT) looked at how true and false information propagate as a whole (2018). The MIT researchers pulled approximately 126,000 true and false news focused Tweets from 2006 to 2017 that had cascaded via retweets and comments more than 4.5 million times (Vosoughi et al., 2018). From there, Vosoughi et al. was able to quantify depth, size, breadth, and structural virality of the cascades (2018). Interestingly, the researchers found that "falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information" (Vosoughi et al., 2018, sec. "Abstract"). In fact, the model used by the researchers showed that false Tweets are retweeted 70% more often than true ones (Vosoughi et al., 2018). Additionally, Vosoughi et al. analyzed false Tweets to speculate on why they were being retweeted at greater rates, which led them to determine that they contained more novelty than true Tweets (2018). The authors noted that novelty was only speculation and more research was needed to determine the true reason false Tweets are spread at greater rates (Vosoughi et al., 2018); the experiment designed in this thesis aims to draw some conclusions between that gap in literature.

C. INFLUENCE EFFECTIVENESS OF INFORMATION DISORDER

The following sub-sections provide insight into the effectiveness of information disorder and propaganda. Currently, the research involving information disorder influence effectiveness on social media is limited, so the topics summarized below span an array of delivery methods. Propaganda, which uses both true (like malinformation mentioned in the previous chapter) and false information to push a specific narrative, is a common term used when reading about information disorder (Wardle & Derakhshan, 2017). Propaganda and information disorder, however, vary slightly in that propaganda emphasizes emotional response at greater depths than information disorder (Wardle & Derakhshan, 2017). However, both are influence operations, making propaganda effectiveness an important aspect of this thesis.

1. Does Russian Propaganda Work?

Beginning in the mid-2000s and increasing when Vladimir Putin regained office in 2012, Russia has been utilizing propaganda to influence its citizens and those abroad (Gerber & Zavisca, 2016). The propaganda, which begins as official government statements and propagates through mass media and social media, seeks to legitimize current government efforts and project power internationally (Gerber & Zavisca, 2016). Understanding the political influence state-run propaganda can have, researchers Theodore Gerber, a sociology professor at the University of Wisconsin-Madison, and Jane Zavisca, the associate dean for Research, College of Social & Behavioral Sciences at the University of Arizona, sought to determine how effective the Russian propaganda had been on its audiences (2016). To answer their research questions, Gerber and Zavisca surveyed citizens in Russia, Ukraine, Azerbaijan, and Kyrgyzstan (2016). Upon review and analysis, they found that the Russian propaganda was effective within the borders of their country, but not nearly as effective outside of it (Gerber & Zavisca, 2016). From their research, Gerber and Zavisca found that 85% of Russians surveyed viewed the United States as an enemy or rival, while only 8% of Ukrainians felt the same way (2016). Azerbaijan, which totaled 24% for enemy or rival, was nearly even with Kyrgyzstan, who totaled to 23% (Gerber & Zavisca, 2016). In their conclusion, Gerber and Zavisca note that there is not a

Page 2502 of 3957

great solution to counter the propaganda that has been effective in neighboring Russian countries because the media is greatly controlled by Russia (2016).

2. Understanding What Makes Terrorist Groups' Propaganda Effective: An Integrative Complexity Analysis of ISIL and Al Qaeda

According to Michael Leiter, the former director of the U.S. Counterterrorism Center, ISIL maintains a constant presence on social media, pushing out propaganda nearly 24 hours a day (Houch et al., 2017). In 2015, it was estimated that, along with other media utilization, ISIL consistently gained 1,000 members monthly (Houch et al., 2017). Through an analysis of the integrative complexity seen in ISIL propaganda, researcher Shannon Houck from Syracuse and researchers Meredith Repke and Lucian Conway III from the University of Montana evaluated what makes ISIL propaganda more effective than Al Qaeda (2017). Houck et al. determined that ISIL used increasingly more simplistic messaging than Al Qaeda, hypothesizing that either ISIL realizes complexity of messaging fails to reach target audiences or they just happen to be sending out simpler propaganda (2017). The research completed by this team backs up previous research that showed "when a group is seeking to gain power, less complexity is more effective for garnering power and achieving political success" (Houck et al., 2017, sec. "Why might Al Qaeda and ISIL differ?").

D. CATEGORIZATION AND DECISION MAKING

When an individual reaches a decision point, like a judge determining if a defendant is guilty, they must assign a category (Wang & Busemeyer, 2016). This categorization, like the judge determining that he/she is, in fact, guilty, leads to follow-on action, like assigning punishment (Wang & Busemeyer, 2016). In the cognitive sciences field, researchers hypothesize that, if an individual is required to announce their categorization prior to action, they may make a different choice than had they acted without reporting first (Wang & Busemeyer, 2016). For example, if a police officer categorizes an individual as having a weapon, then reports that the suspect has a weapon prior to acting, rather than shooting immediately, the outcome may be different (Wang & Busemeyer, 2016). Knowing that, the experimental design detailed in Chapter Four incorporates initial categorization,

Page 2503 of 3957

attempting to address whether said categorization truly affects the way an individual interacts with information. Below, recent works in the field of categorization and decision making are summarized, allowing the reader to gain an understanding that will translate when viewing the follow-on chapter.

1. Interference Effects of Categorization on Decision Making

Researchers Zheng Wang of The Ohio State University and Jerome Busemeyer of Indiana University utilized multiple models, including the Markov model, Signal detection model, and Quantum model, to study category-decision linked tasks (2016). During three slightly varied experiments, the researchers presented participants with images of faces where some had been categorized (through a label) as displaying a good guy (g) or bad guy (b), some were required to be categorized by the participant, and some lacked categorization completely (Wang & Busemeyer, 2016). Once viewing the face, and categorizing as necessary, participants would decide whether to attack the individual or withdraw (Wang & Busemeyer, 2016). After reviewing the results and applying the three models listed previously, Wang and Busemeyer were able to identify inference effects (statistical conclusions about the data) that occurred between trials with categorization and without categorization (2016). The occurrence of these inference effects, which existed in some predicted and some unpredicted places, highlights the ability for categorization to change the way an individual views something, as well as their follow-on decision (Wang & Busemeyer, 2016).

2. An Evidential Dynamical Model to Predict the Interference Effect of Categorization on Decision Making Results

While the above experiment utilized the Quantum, Markov, and Signal Detection models to find inference effects, researchers Zichang He and Wen Jiang of Northwestern Polytechnical University created a new evidential dynamic model (2018). Through the integration of Dempster-Shafer evidence theory and quantum dynamical modelling, He and Jiang's model successfully illustrated category-decision task inference effects without the need for integrating multiple experiments and models together (2018). To be successful, He and Jiang created the model to measure the handling of uncertain states in

Page 2504 of 3957

action, which is different than the aforementioned, which measures an "entanglement of beliefs and actions" (2018, p. 140). By creating a new model that provides the same effectiveness and efficiency of previous models, He and Jiang were able to show once again that categorization influences follow-on decision making (2018).

Page 2505 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2506 of 3957

IV. METHODOLOGY

The experiment designed in this chapter aims to answer the hypotheses presented in Section A by creating a survey that can, if released for public participation, highlight possible correlations between the acceptance and propagation of false information and age, education, and gender, as well as the effect of initial categorization on decision making. In Section A, the hypotheses from Chapter I are presented again. In Section B, an overview of the experiment is detailed, which includes information on the participants and setting (online delivery). In Section C, the Tweets and memes used in the experiment are presented. Section D contains a detailed description (with figures) of how the experiment was built in Qualtrics. Finally, Section E discusses limitations of the experiment designed.

A. HYPOTHESES

The experiment designed in this chapter aims to answer the following hypotheses:

- HA1: Age correlates to the acceptance of false information spread through a Tweet and an image macro meme.
- HA2: Education level correlates to the acceptance of false information spread through a Tweet and an image macro meme.
- HA3: Gender correlates to the acceptance of false information spread through a Tweet and an image macro meme.
- HA4: Age correlates to the propagation of false information spread through a Tweet and an image macro meme.
- HA5: Education level correlates to the propagation of false information spread through a Tweet and an image macro meme.
- HA6: Gender correlates to the propagation of false information spread through a Tweet and an image macro meme.

Page 2507 of 3957

- HA7: Initial categorization has an effect on the acceptance of false information spread through Tweets and image macro memes.
- HA8: Memes will be interacted with (by indication of liking, commenting, or sharing) at a different rate than Tweets.

B. EXPERIMENTAL DESIGN OVERVIEW

If individuals were to take the experiment as it is designed currently, the participants first view instructions for the experiment, then provide consent to participate, and finally give their age, gender, and education. Age is broken down into the following groups: 18–25, 26–33, 34–41, 42–49, 50–57. Gender is disclosed as preferred sex (not assigned), containing options for male or female. Education is broken down by the following selections: high school diploma, associate's degree, undergraduate level schooling in progress, bachelor's degree, graduate-level schooling in progress, master's degree, doctorate-level schooling in progress, and doctorate degree. Please see Table 1 for an overview of the variables collected.

Table 1. Variables collected during the experiment

Factors	Levels
Age	5 levels
Education	8 levels
Gender	2 levels
Meme (With and Without) Tweet	2 levels
Categorization (With and Without) Tweet	2 levels

Following those selections, participants will begin the experiment. Each participant will randomly start with one of the following four groups and proceed on the path outlined in Figure 6: seven simulated Tweets with initial categorization questions (set one), seven simulated Tweets without initial categorization questions (set two), seven image macro memes with initial categorization questions (set one), or seven image macro memes without initial categorization questions (set two). All Tweets and image macro memes contain inaccurate information centered on COVID-19 and can be viewed later in this

Page 2508 of 3957

chapter. Set one and Set two denote the line of questioning that appears with the Tweet or image macro meme and can be viewed below the experimental flow chart.

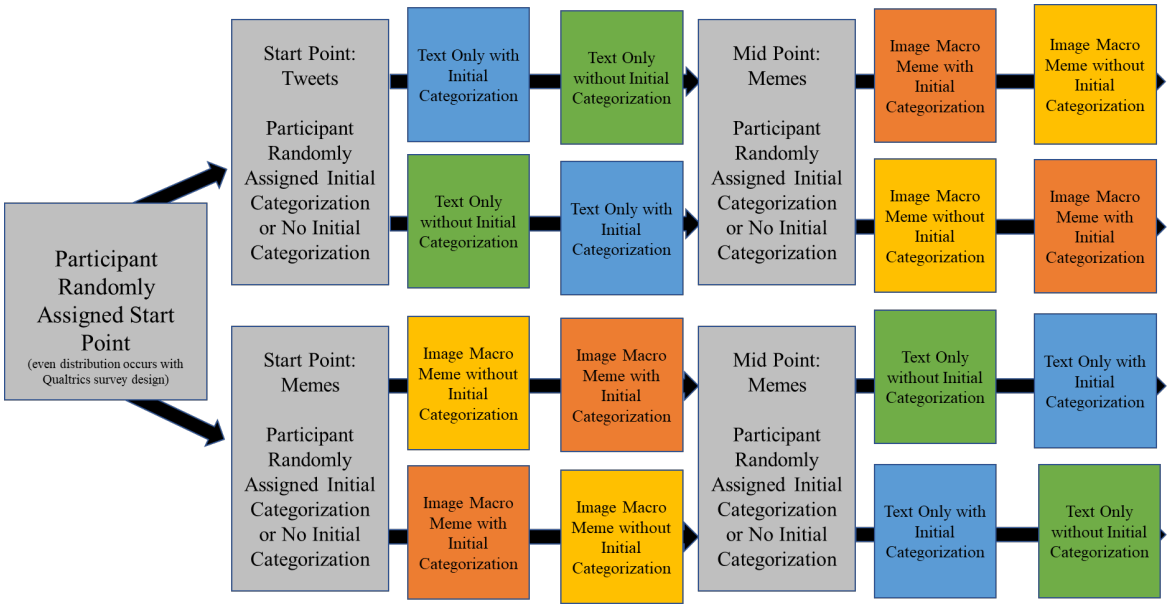


Figure 6. Experiment flow chart

When designing the questions, it was important to offer participants a selection for any reason they may interact with the Tweet or meme. Because memes are generally viewed as humorous, that was included in the top spot. A selection of "A" or "C" (Affiliated with my personal views) in question set one or two will help guide research analysis; interacting with a Tweet or meme because it is humorous or affiliated with person views will help propagate but does not indicate susceptibility to information disorder. However, because the experiment is built to measure susceptibility between different independent variables, participants may select "Accurate information" or a combination of "Accurate information" with "Humorous" or "Affiliated with my personal view." If that is selected, it will assist researchers in finding correlations between susceptibility and the independent variables. Below, the question sets are presented. Set one includes initial categorization, while set two does not.

Page 2509 of 3957

Set One of questioning:

1. Would you interact with this Meme/Tweet on social media (Facebook, Instagram, Twitter, etc.) by liking, commenting, or sharing the post?
    a. Yes
    b. No
2. If YES, why would you interact with this Meme/Tweet on social media?
    a. Humorous
    b. Accurate information
    c. Affiliated with my personal views
    d. Humorous and Accurate Information
    e. Humorous and Affiliated with my personal view
    f. Accurate information and Affiliated with my personal views
    g. Disagree with information
3. If NO, why wouldn't you interact with this Meme/Tweet on social media?
    a. Not active on social media
    b. Inaccurate information
    c. Goes against my personal views
    d. Not active on social media and Inaccurate information
    e. Not active on social media and Goes against my personal views
    f. Inaccurate information and Goes against my personal views
    g. Disagree with information

Set Two of questioning:

1. Why would you interact with this Meme/Tweet on social media (Facebook, Instagram, Twitter, etc.) by liking, commenting, or sharing the post?
    a. Humorous
    b. Accurate information
    c. Affiliated with my personal views
    d. Humorous and Accurate Information
    e. Humorous and Affiliated with my personal view
    f. Accurate information and Affiliated with my personal views
    g. Disagree with information
    h. I would not interact with this on social media

After each participant has completed all four sections, they are shown a disclaimer that tells them that all the information seen in the experiment was manipulated into false information. This will prevent any participant from falling victim to misinformation as a result of this research. The way in which the information was manipulated is described below each tween and meme presented in the next section.

Page 2510 of 3957

C. TWEETS AND MEMES USED

Below, every Tweet and image macro meme used in the experimental design is presented. Underneath each figure, the reasoning for the particular Tweet or meme is detailed. First, all 14 Tweets will be presented. Following that, all 14 memes will be presented.

1. Tweets Used in the Experimental Design

To create the 14 Tweets used in this experiment, many things were taken under consideration. First and foremost, the creation source was selected: www.tweetgen.com. This site allows the user to adjust the theme, add a profile picture, create a name, insert a Twitter handle, make the account verified, add Tweet content, insert an image, and adjust the time, date, retweets, and likes. Next, it was important to select a widely recognizable news sources' Twitter profile and mimic it exactly. Had a lesser-known source been selected, it was feared that participants would not trust the source, and, in turn, that would skew their answers to the experiment questions.

Having 48.7 million followers on Twitter, *The New York Times* was deemed a good model and all Tweets were created to match its profile. As seen in Figure 7, the image, name, and Twitter handle is the same as the real version. Additionally, the account appears verified, just like it is online. Finally, if the Tweet was modeled directly after a real *The New York Times* Tweet, the retweets and likes were also modeled directly after the original Tweets retweets and likes at the time of creation. However, if the Tweet was modeled after a different source, the retweets and likes were randomly generated on the www.tweetgen.com site.

Below, all 14 Tweets used are presented. Beneath each Tweet, the reasoning for the Tweet content is briefly explained.

Page 2511 of 3957

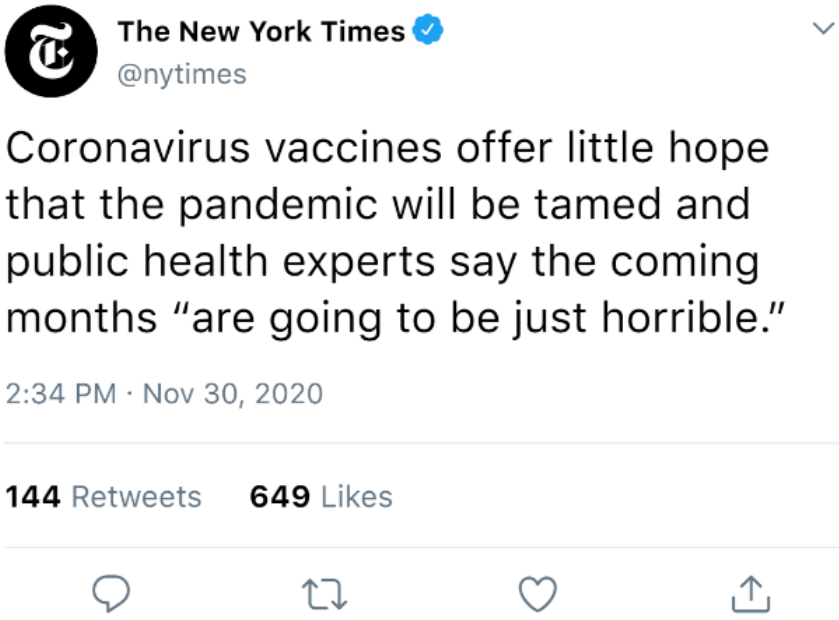


Figure 7. Tweet number one. Adapted from *The New York Times* (2021).

Tweet number one was modeled directly after a Tweet posted by *The New York Times* on November 30, 2020, that stated: "Good news about coronavirus vaccines offers hope that the pandemic will be tamed. But public health experts say the coming months "are going to be just horrible." In an attempt to make it misinformation, the Tweet was altered to remove the beginning words and now contains the word "little" before "hope." As a result, the fake Tweet does not make the COVID-19 vaccine look like a solution to the pandemic and creates a sense of doom.

Page 2512 of 3957

Figure 8. Tweet number two. Adapted from *The New York Times* (2021).

Tweet number two was created in response to real conspiracy theories that claim hospitals are inflating numbers of COVID-19 related deaths in an attempt to benefit financially (Knight & Appleby, 2020).

Figure 9. Tweet number three. Adapted from *The New York Times* (2021).

Tweet number three was modeled directly after a Tweet posted by *The New York Times* on February 16, 2021, that stated: "North Korea has tried to steal Covid-19 vaccine and treatment technology by attempting to hack international pharmaceutical companies, including Pfizer, a South Korean lawmaker said on Tuesday after a briefing by intelligence officials." The date, reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). To make this misinformation, the country of North Korea was replaced with Russia, and the identifier of "South Korean lawmaker" was removed. As a result, the Tweet presents Russia as the intelligence threat, not North Korea.

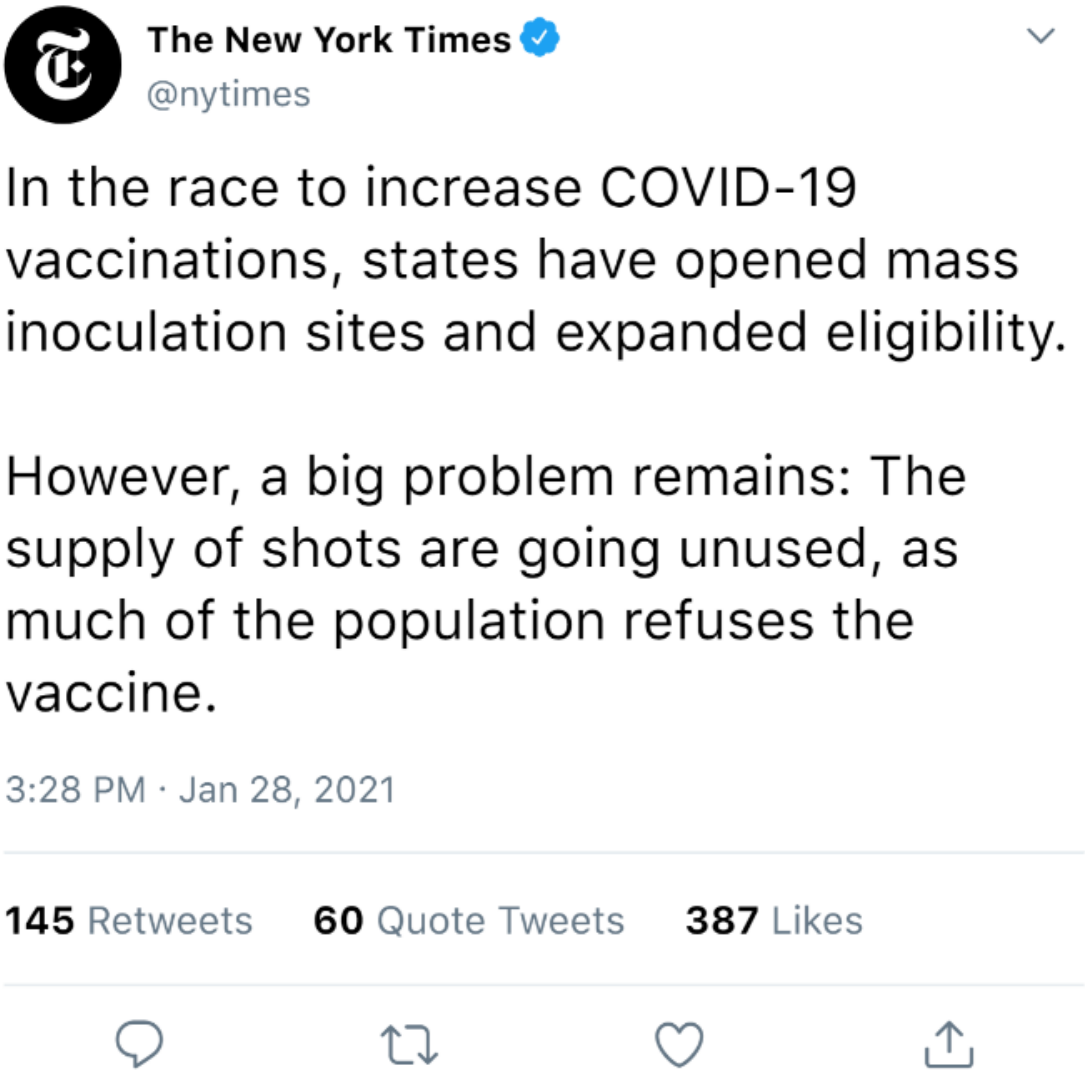


Figure 10. Tweet number four. Adapted from *The New York Times* (2021).

Tweet number four was modeled directly after a Tweet posted by *The New York Times* on February 15, 2021, that stated: "In the race to increase Covid-19 vaccinations, states have opened mass inoculation sites and expanded eligibility. But a big problem remains: The supply of shots isn't increasing fast enough." The reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). To make this misinformation, the big problem was changed to a lack of participants instead of vaccine supply.

Page 2515 of 3957

Figure 11. Tweet number five. Adapted from *The New York Times* (2021).

Tweet number five was modeled directly after a Tweet posted by *The New York Times* on February 14, 2021, that stated: "A team of experts selected by the WHO to investigate the origins of the coronavirus returned last week from Wuhan. They plan to produce a joint report on the virus, which they agree most likely originated from an animal – and not a lab." The date, reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). In the manufactured Tweet, the virus was said to be manufactured in a lab (vice naturally occurring in an animal), appealing to individuals that believe COVID-19 was created as a bioweapon.

Page 2516 of 3957

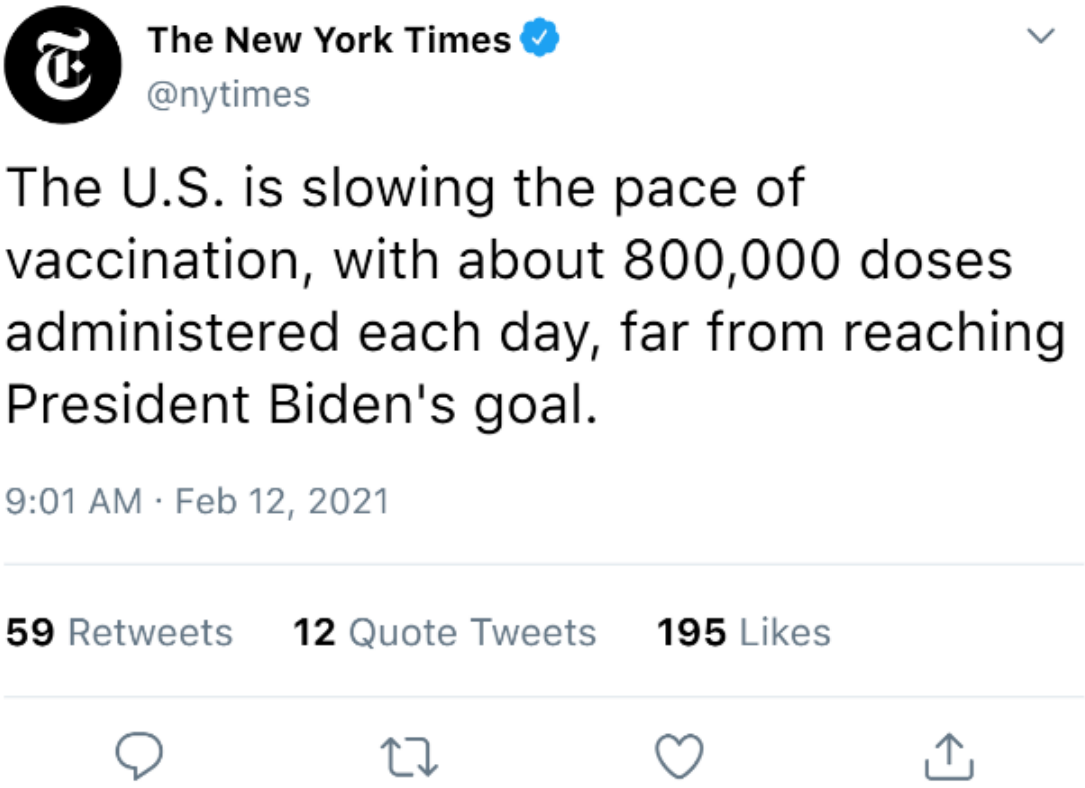


Figure 12. Tweet number six. Adapted from *The New York Times* (2021).

Tweet number six was modeled directly after a Tweet posted by *The New York Times* on February 12, 2021, that stated: "The U.S. is also picking up the pace of vaccination, with about 1.6 million doses administered each day, exceeding President Biden's goal." The date, reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). The number of vaccinations occurring daily, as well as the perceived pace (slowing vice picking up) was altered to make it appear like President Biden is not reaching his goal for the nation.

Page 2517 of 3957

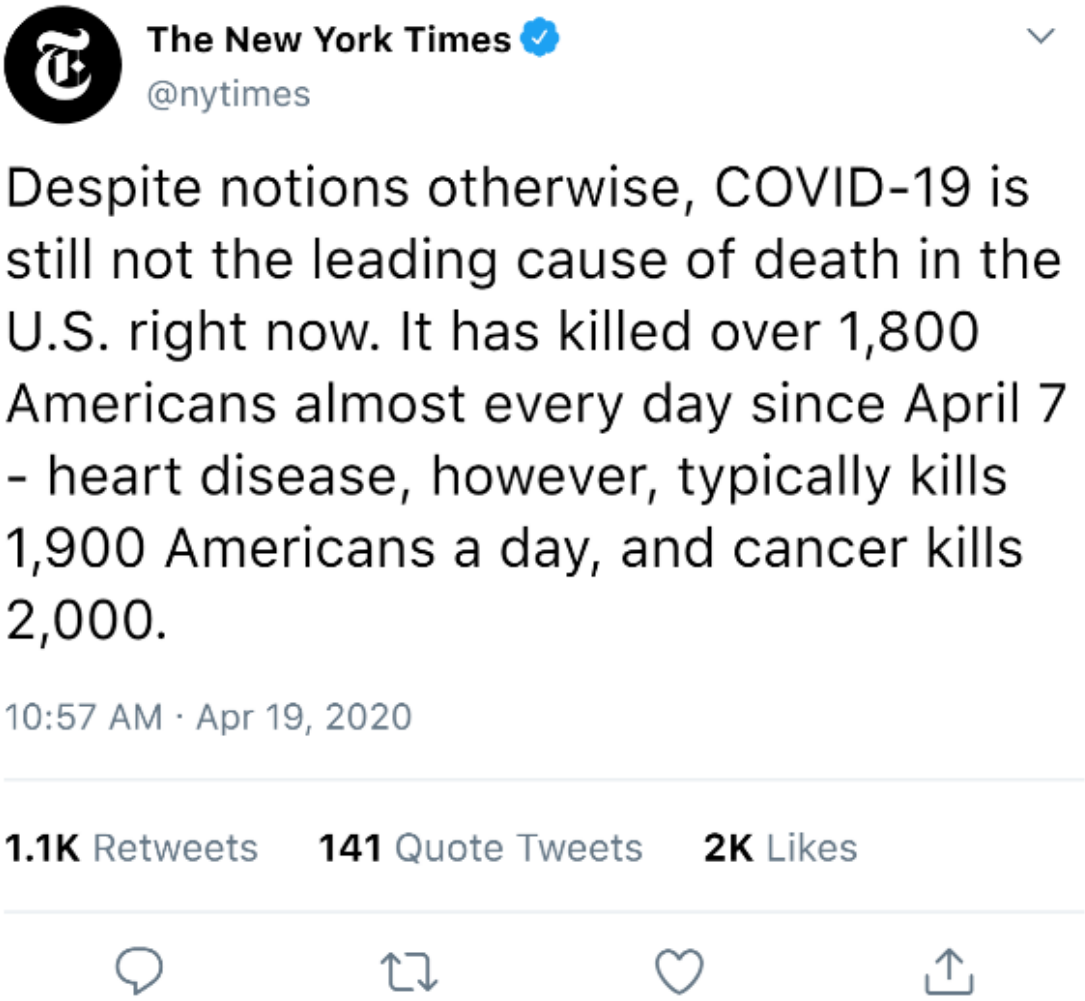


Figure 13. Tweet number seven. Adapted from *The New York Times* (2021).

Tweet number seven was modeled directly after a Tweet posted by *The New York Times* on April 19, 2020, that stated: "COVID-19 is arguably the leading cause of death in the U.S. right now. It has killed over 1,800 Americans almost every day since April 7 – heart disease typically kills 1,774 Americans a day, and cancer kills 1,641." The date, reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). This manufactured Tweet was altered to make heart disease and cancer a bigger threat than COVID-19.

Figure 14. Tweet number eight. Adapted from *The New York Times* (2021).

Tweet number eight was modeled directly after a Tweet posted by *The New York Times* on January 9, 2020, that stated: "There's no evidence that the virus, a coronavirus, is readily spread by humans, and it has not been tied to any deaths. But health officials in China and internationally are watching it carefully." The date, reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). The alteration of the original Tweet creates a narrative that world leaders knew the early dangers of COVID-19 and chose to ignore them.

Figure 15. Tweet number nine. Adapted from *The New York Times* (2021).

Tweet number nine was modeled directly after a Tweet posted by *The New York Times* on May 10, 2020, that stated: "What's clear: A one-time social distancing effort won't be sufficient to control the coronavirus, and it will take a long time to reach herd immunity. Without an effective vaccine, our pandemic state of mind may persist well into 2021 or 2022." The date, reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). Changing the Tweet to state that one-time social distancing will, in fact, be enough to combat the pandemic, transforms the original message to misinformation.

Figure 16. Tweet number ten. Adapted from *The New York Times* (2021).

Tweet number ten was modeled directly after a Tweet posted by *The New York Times* on December 19, 2020, that stated: "Early in the coronavirus outbreak, Chinese authorities clamped down on information to make the virus look less severe, and the government more capable, thousands of secret government directives and other documents reviewed by @nytimes and @propublica show." The date, reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). By replacing "Chinese" with "U.S." authorities, we create mistrust towards our government, which is rooted in misinformation.

Figure 17. Tweet number eleven. Adapted from *The New York Times* (2021).

Tweet number eleven was modeled directly after a Tweet posted by *The New York Times* on December 8, 2020, that stated: "The coronavirus vaccines will probably prevent you from getting sick with Covid-19. But it's not yet clear whether you can still get infected asymptomatically and silently spread the virus." The date, reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). Slightly changing the Tweet to state that the vaccine will not prevent you from catching the virus, vice maintaining an unsure position, turns this into subtle misinformation.

Page 2522 of 3957

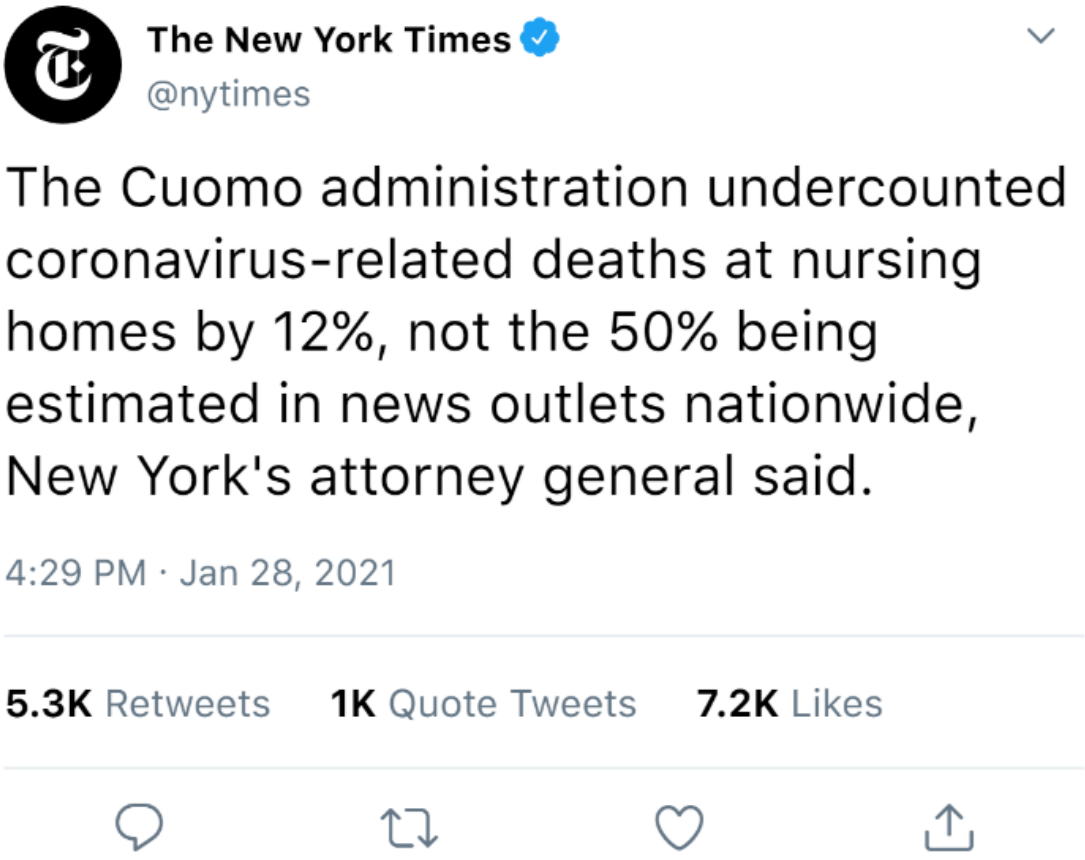


Figure 18. Tweet number twelve. Adapted from *The New York Times* (2021).

Tweet number twelve was modeled directly after a Tweet posted by *The New York Times* on January 28, 2021, that stated: "The Cuomo administration undercounted coronavirus-related deaths at nursing homes by as much as 50%, New York's attorney general said." The date, reTweets, quote Tweets, and likes were taken directly from the original Tweet (on February 16, 2021). This misinformation alteration attempts to delegitimize the accusations that New York Governor Cuomo greatly underreported COVID-19 deaths in nursing homes, while the truth is quite the opposite.

Figure 19. Tweet number thirteen. Adapted from The *New York Times* (2021).

Tweet number thirteen was modeled directly after a Tweet posted by *The New York Times* on February 16, 2021, that stated: "The pandemic has taken over most children's lives – shutting down in-person school, sports and socializing. That has prompted some teenagers, who otherwise feel powerless, to fight back by volunteering for vaccine trials." The date was taken directly from the original Tweet, while the reTweets, quote Tweets, and likes were randomized by the Tweet generation website. The manipulation of this Tweet creates misinformation by framing teenagers as rude and vindictive.

Page 2524 of 3957

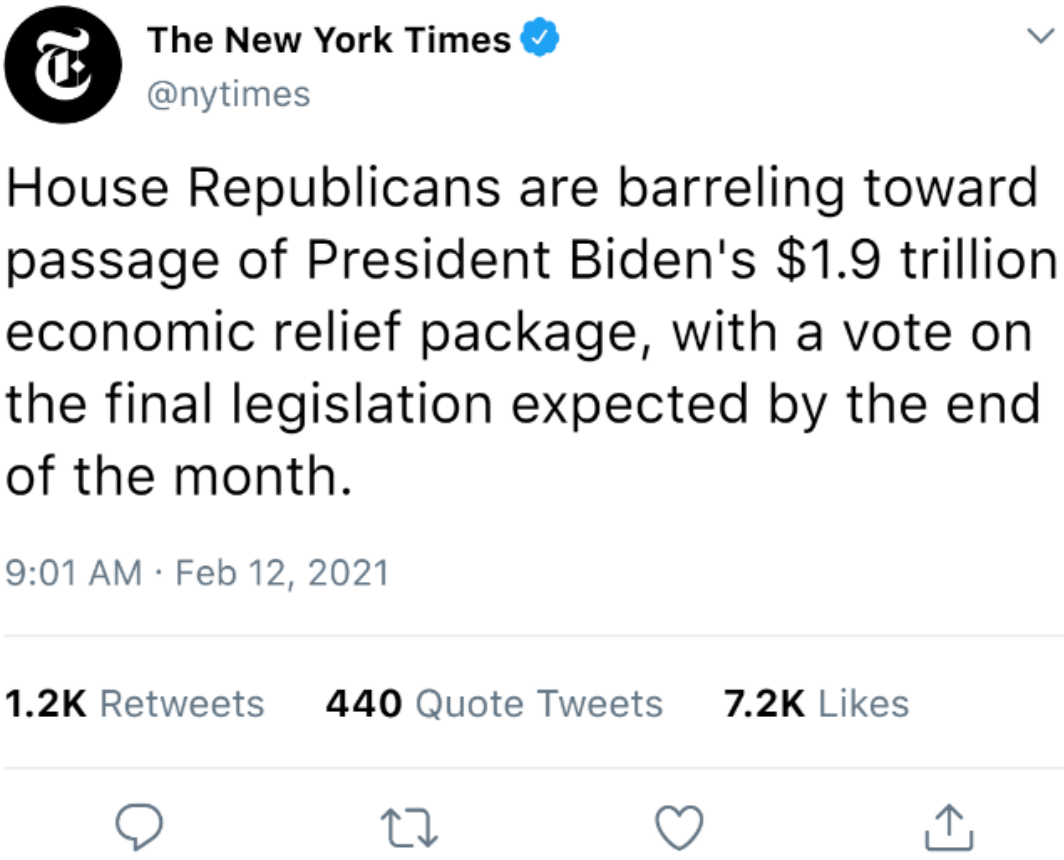


Figure 20. Tweet number fourteen. Adapted from *The New York Times* (2021).

Tweet number fourteen was modeled directly after a Tweet posted by *The New York Times* on February 16, 2021, that stated: "House Democrats are barreling toward passage of President Biden's $1.9 trillion economic relief package, with a vote on the final legislation expected by the end of the month." The date, reTweets, quote Tweets, and likes were randomized on the Tweet generation website. Changing "Democrats" to "Republicans" paints the picture that there is bipartisan support, making the overall message into misinformation.

2. Memetics Used in Experimental Design

The image macro memes used in this experiment were created by the author on the website https://www.imgflip.com/memegenerator. All images used were selected from the

"Expanding Brain" on the imgflip site, specifically under the "Popular" tab. A link to the meaning of each image selected is provided in the description of each meme created. The various content of the memes were inspired by conspiracy theories and popular misinformation campaigns that have been widespread throughout the current pandemic.

Figure 21. Meme number one. Adapted from Bremmer (2020).

Meme number one was inspired by a *Time* article entitled "The Best Global Responses to COVID-19 Pandemic" (Bremmer, 2020). The article protests that, as of June 2020, the epicenter of the pandemic was in the United States (Bremmer, 2020). Following that, it lists other nations that did a better job than the United States at controlling the spread of the virus (Bremmer, 2020). By suggesting that every other nation, not just some nations, have slowed the spread better than the U.S., this misinformation memetic spreads distrust in the U.S. Government handling of the pandemic itself. To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/but-thats-none-of-my-business.

Page 2526 of 3957

Figure 22. Meme number two. Adapted from Lynas (2020).

Meme number two was inspired by a widespread conspiracy theory that 5G is spreading COVID-19 via the electromagnetic spectrum (Lynas, 2020). According to believers, the rollout of 5G and the rapid takeover of coronavirus were identically timed, allowing them to link the two events together (Lynas, 2020). To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/i-bet-hes-thinking-about-other-women.

Figure 23. Meme number three. Adapted from Lynas (2020).

Meme number three was inspired by the conspiracy theory that big pharmaceutical companies are hyping up COVID-19 to appear worse than it is in order to sell more products (Lynas, 2020). For example, Joseph Mercola, an anti-vax medical professional, was banned from Google for pushing his products through claims that they cure and prevent COVID-19 (Lynas, 2020). According to Lynas at Cornell Alliance for Science, "big pharma conspiracies are a staple of anti-vaccination narratives, so it is hardly surprising that they have transmuted into the age of coronavirus" (2020, sec. "COVID is a plot by Big Pharma). To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/disaster-girl.

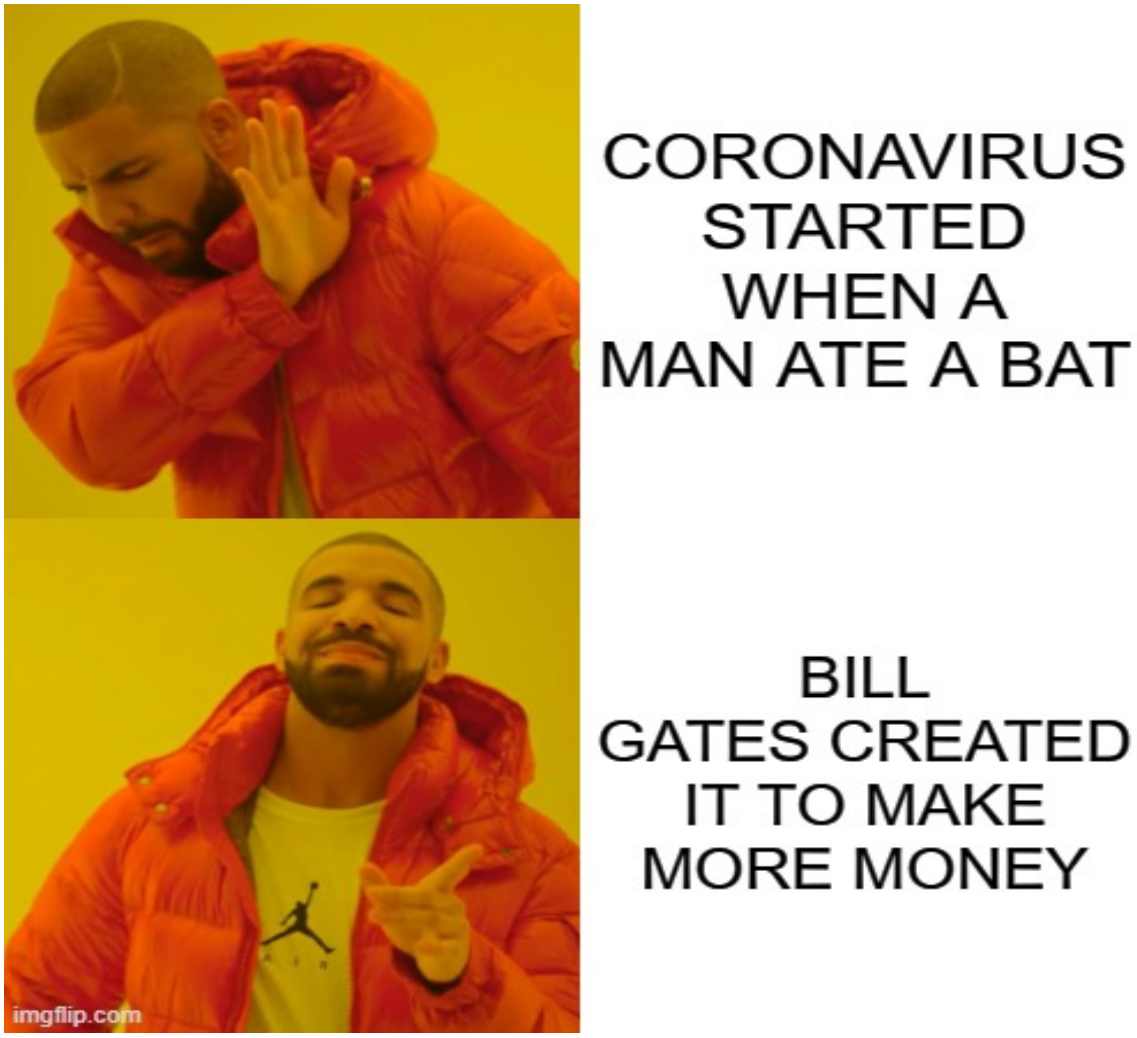


Figure 24. Meme number four. Adapted from Lynas (2020).

Meme number four was inspired by the theory that Bill Gates knew about an impending pandemic and, either created the virus, or invested in vaccination technology to profit off of it (Lynas, 2020). According to QAnon and far-right political members, previous Bill Gates Ted talks allude to his knowledge of an impending global pandemic (Lynas, 2020). Some protestors to this conspiracy theory believe it is the result of Gates criticizing former President Trumps move to defund the World Health Organization (Lynas, 2020). To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/drakeposting.

Figure 25. Meme number five. Adapted from Lewis (2020).

Meme number five was inspired by a conspiracy theory that believes COVID-19 was released from a Chinese lab as a bioweapon (Lewis, 2020). Although the true origin is said to be naturally occurring in Wuhan, China, former President Trump and many supporters claim it started in Chinese virologist Shi Zhengli's lab (Lewis, 2020). To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/distracted-boyfriend.

Figure 26. Meme number six. Adapted from Pinsker (2021), Beals (2020), Bazelon (2020), & Clarke (2020).

Meme number six was inspired by the continued question that has plagued American minds since March 2020: When will life be normal again? (Pinsker, 2021). Initially, citizens were told that COVID-19 would likely diminish in the summer of 2020 (Beals, 2020). Following the realization that that was not the case, Americans in many states were in disarray over the continuous closure of the economy, wondering when that would reopen (Bazelon, 2020). As much of the world transitioned to 2021 still in state-wide lockdowns, hopeful citizens pushed their winter travel to 2021 (Clarke, 2020). The final section of the meme, stating "the government is handling this well," is simply a way to make it appear controversial. To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/putting-on-clown-makeup.

Figure 27. Meme number seven. Adapted from Lee (2020), & Naishadham et al. (2020).

Meme number seven was inspired by the idea that selfishness has led to many infections and untimely COVID-19 related deaths. Currently, there are a number of opinion pieces found online that link selfishness to the deaths of loved ones. For example, on *The Colorado Sun* website, you can find an article entitled, "Selfishness during a pandemic may have killed my father. It shouldn't have ended this way" (Lee, 2020). Additionally, on the *Chicago Tribune* website, you will see an article titled, "Too many people are selfish: As

Americans resist COVID-19 restrictions, U.S. nears 5 million infections" (Naishadham et al., 2020). To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/daily-struggle.

Figure 28. Meme number eight. Adapted from Pitofsky (2021).

Meme number eight was inspired by the large number of the U.S. population that claims they will not get the COVID-19 vaccine due to safety concerns (Pitofsky, 2021). According to an article on *The Hill*, 30% of Americans surveyed said they would not get the COVID-19 vaccine (Pitofsky, 2021). Of that 30%, 48% claimed they were waiting to review long-term effects and safety numbers (Pitofsky, 2021). Another survey conducted by the Center for Disease Control and Prevention states that 24% of Americans will not get the vaccine, 50% of said 24% were also waiting to see if it was safe (File & Mohanty, 2021). This meme perpetuates the idea that the vaccine is not, in fact, safe, and the U.S.

government is giving it out anyway. To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/who-killed-hannibal,

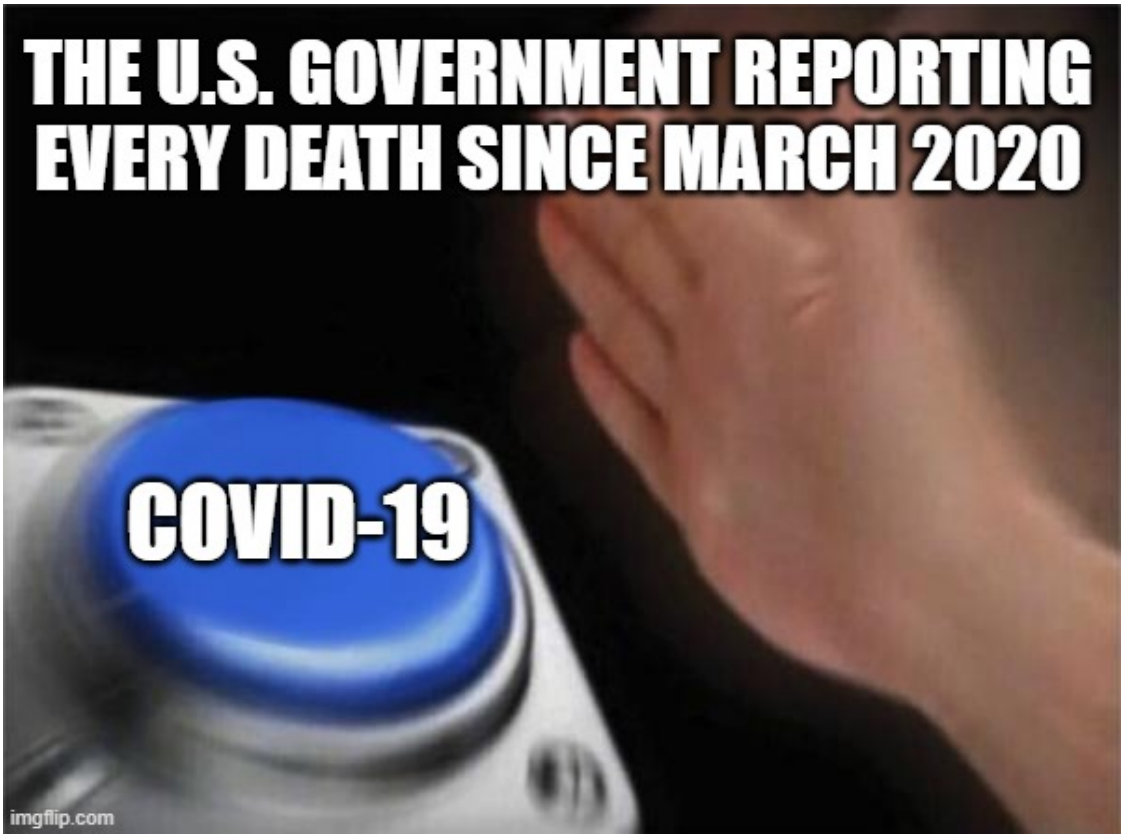


Figure 29. Meme number nine. Adapted from Lynas (2020).

Meme number nine was inspired by the conspiracy theory that death certificates are being manipulated to make all deaths a result of COVID-19 (Lynas, 2020). This conspiracy theory was perpetuated by Annie Bukacek, who spoke in a YouTube video describing the death certificate manipulation (Lynas, 2020). After amassing over 250,000 views, the doctor was exposed as a far-right, anti-vax activist likely speaking with an agenda (Lynas, 2020). Despite that knowledge, many people continue to spread this message. To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/invest-button.

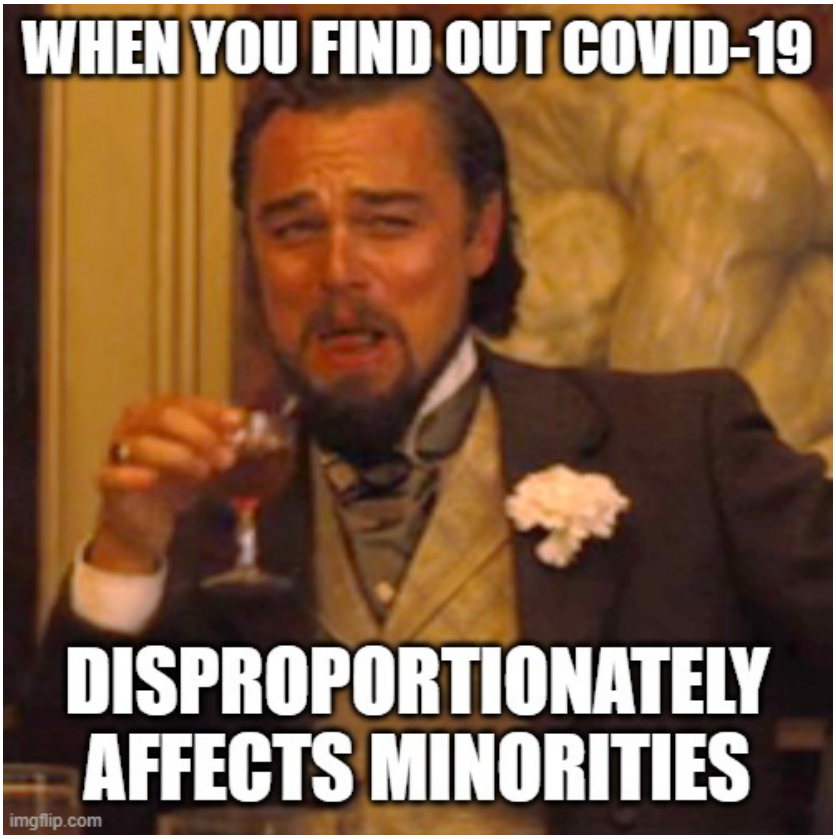


Figure 30. Meme number ten. Adapted from CDC (2021).

Meme number ten was inspired by the growing evidence that COVID-19 disproportionately affects minorities (CDC, 2021). By placing this specific image in the background, it appeals to a white nationalist audience, spreading the false idea that white people are superior to minorities. To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/leonardo-dicaprio-laughing.

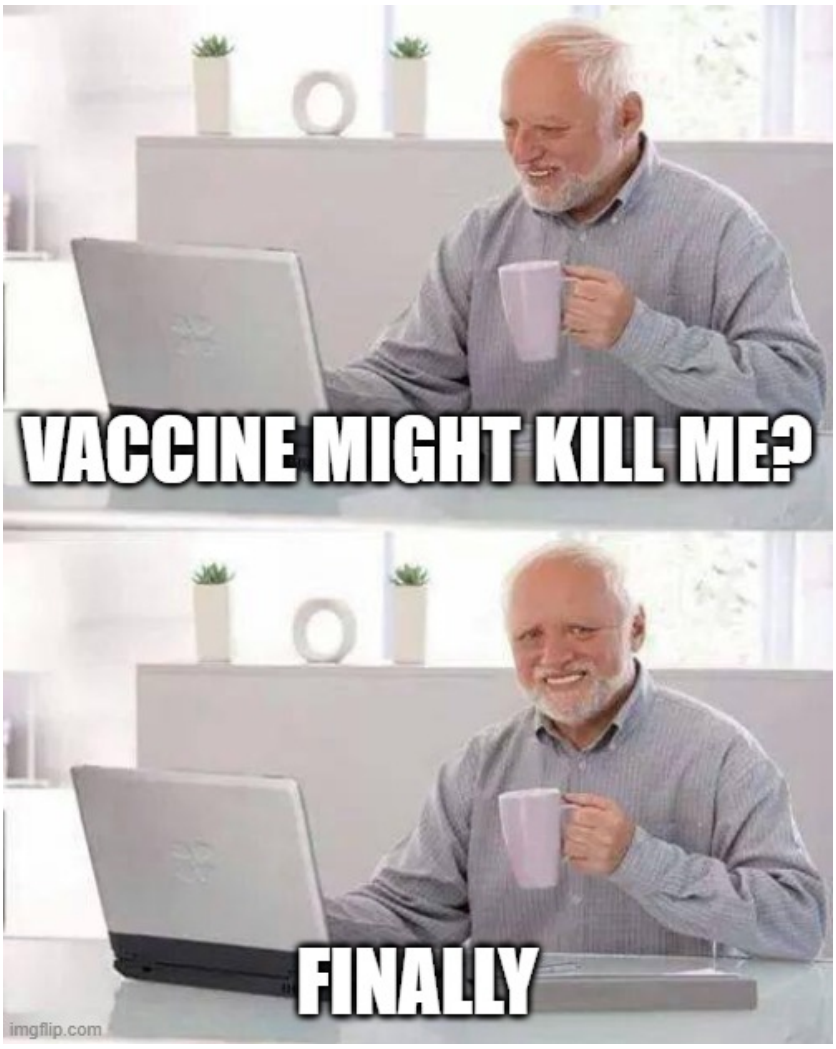


Figure 31. Meme number eleven. Adapted from Pitofsky (2020).

Meme number eleven was inspired by the same statistics presented earlier for meme eight. To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/hide-the-pain-harold.

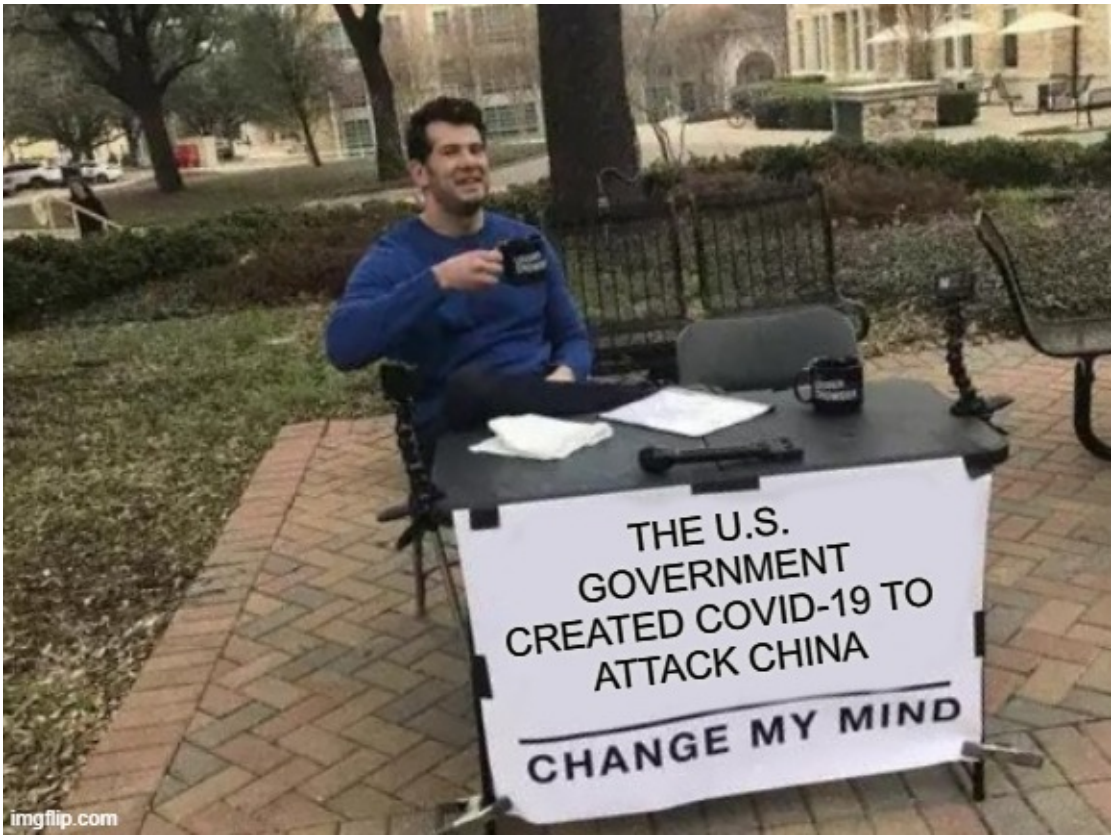


Figure 32. Meme number twelve. Adapted from Klepper et al. (2021).

Meme number twelve was influenced by the conspiracy theory that "the U.S. created the virus and used it to attack China" (Klepper et al., 2021, sec. "Igor Nikulin"). A prominent Russian political Figure, Igor Nikulin, who has supported weaponizing misinformation, appeared on Russian state television to spread this narrative 18 times between the months of January 2020 and April 2020 (Klepper et. al., 2021). To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/steven-crowders-change-my-mind-campus-sign.

Figure 33. Meme number thirteen. Adapted from Lynas (2020).

Meme number thirteen was inspired by the idea that COVID-19 isn't real. David Icke and Alex Jones, both of which are professional conspiracy theorist, spread the narrative that COVID-19 was created as "a plot by the globalist elite to take away our freedoms" (Lynas, 2020, sec. "COVID-19 doesn't actually exist"). To learn more about the image behind this meme, visit https://www.dictionary.com/e/memes/expanding-brain-meme/.

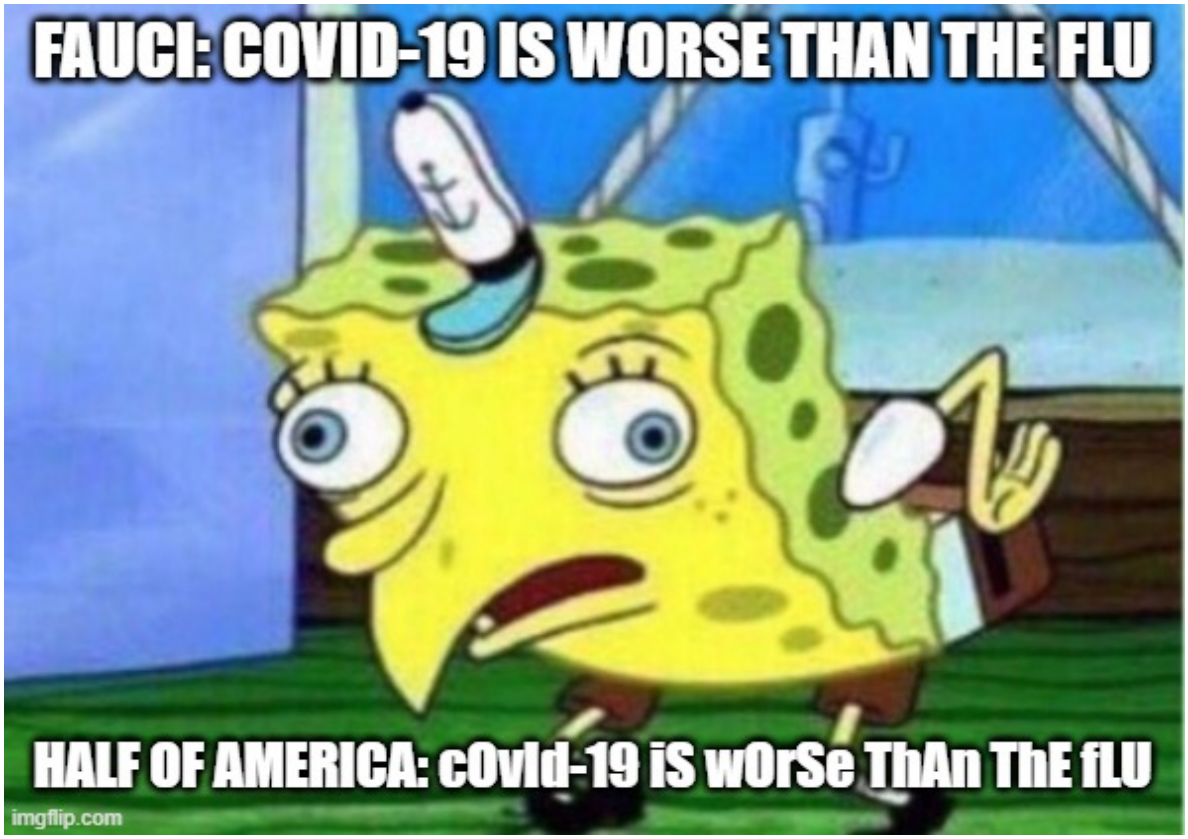


Figure 34. Meme number fourteen. Adapted from Lewis (2020).

Meme fourteen was created as a response to former President Trump's claims that the coronavirus was "no more dangerous than the seasonal influenza" (Lewis, 2020, para. 4). Many U.S. citizens went on to believe this claim because their leader was explicitly stating it (Lewis, 2020). To learn more about the image behind this meme, visit https://knowyourmeme.com/memes/mocking-spongebob.

D. QUALTRICS

To build this experiment, Qualtrics was utilized. Qualtrics is an online platform that allows users to build very complex surveys for use in data collection for businesses, research, and other organizations (Qualtrics, 2021). To build this specific experiment, a "Brand Administrator" type of account was purchased and used. After creating an account, "Create New Project" was selected and the experimental design began.

1. Steps to Create the Experiment Designed in this Thesis

1. Use the default question block to create the introduction and instructions notification. This can be done by clicking on the Q1 and keeping the question type as “Multiple Choice,” ensuring the answer type is set to “Allow one answer,” and the number of choices is set to “2.” After filling in the text and answer choices, the question behavior “Skip Logic” was added. If an individual selects “I do not wish to participate in this experiment” then he/she will be taken directly to the default end page. Figure 35 will show what text is present in the experiment designed in this thesis.

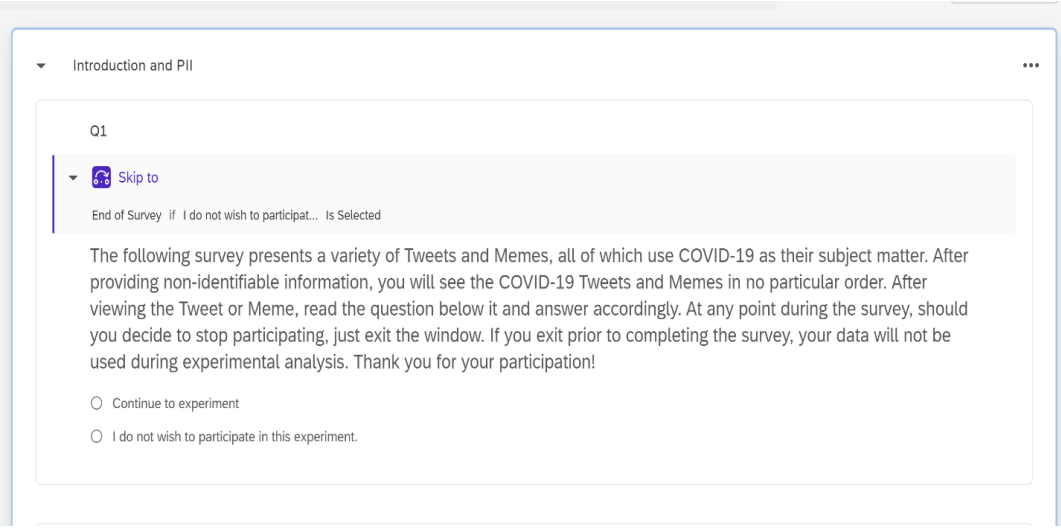


Figure 35. Question one example

2. Click the plus sign within the first question block to add another question. This question will be set up exactly like the previous question but contain consent information, which can be reviewed in Figure 36. In this case, the “skip logic” is tied to “I do not consent to participate in this experiment.”

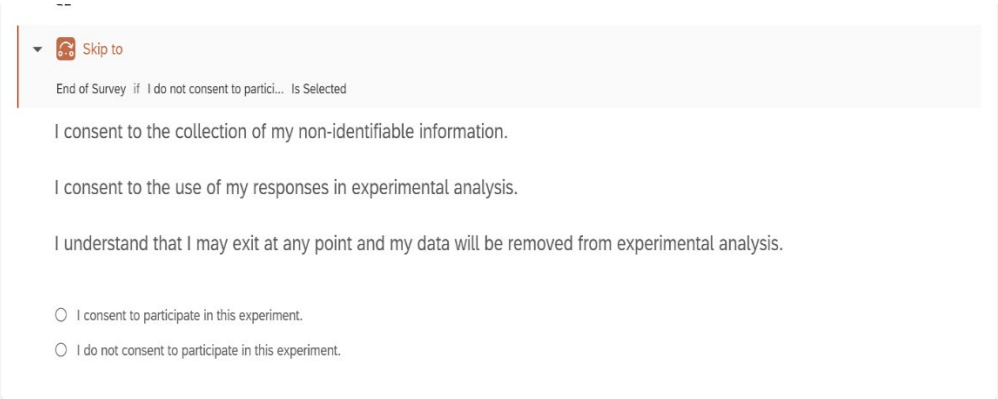


Figure 36. Question two example

3. Click the plus sign within the first question block to add another question. This question is set up like the previous two. However, it asks the participants to provide their age group, requiring seven answer choices vice two. After inputting the age groups listed in Section B of this chapter, options for "Under 18" and "58 or older" are included. Because we are not measuring individuals below/above this age range, those answer choices contain "skip logic" that takes the participant to the end of the survey.

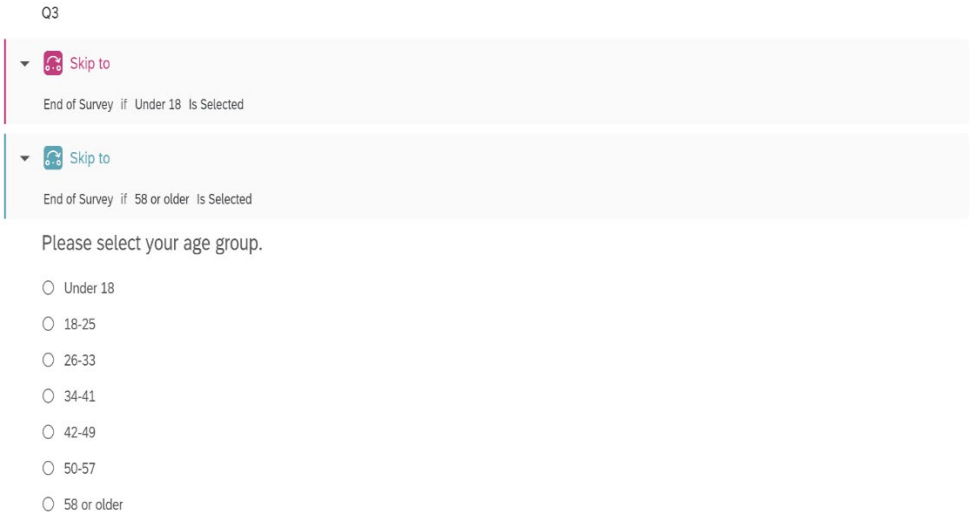


Figure 37. Question three example

Page 2541 of 3957

4. Click the plus sign within the first question block to add another question. This question is set up like the previous three. However, it asks the participants to provide their gender, requiring three answer choices. In this case, the "skip logic" is tied to "None of the Above" because one goal of the experiment is to correlate survey answers to gender. If they do not fall into a category, we cannot correlate them properly.

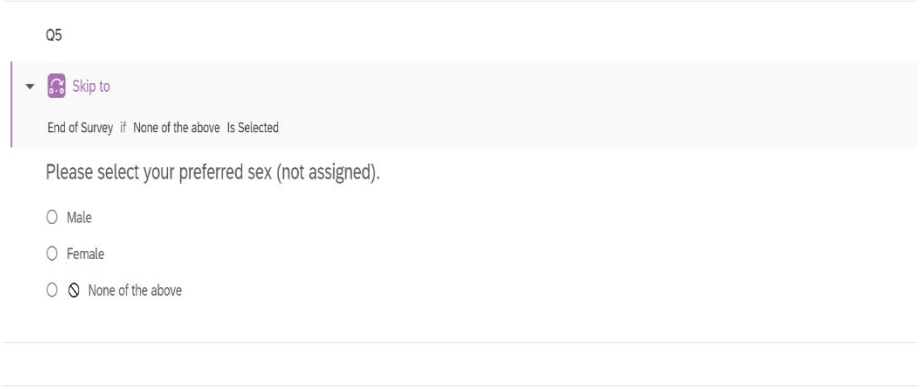


Figure 38. Question four example

5. Step 5: Click the plus sign within the first question block to add another question. This question is set up like the previous four. However, it asks the participants to provide their education level, requiring nine answer choices. In this case, the "skip logic" is tied to "None of the Above" because one goal of the experiment is to correlate survey answers to education level. If they do not fall into a category, we cannot correlate them properly.

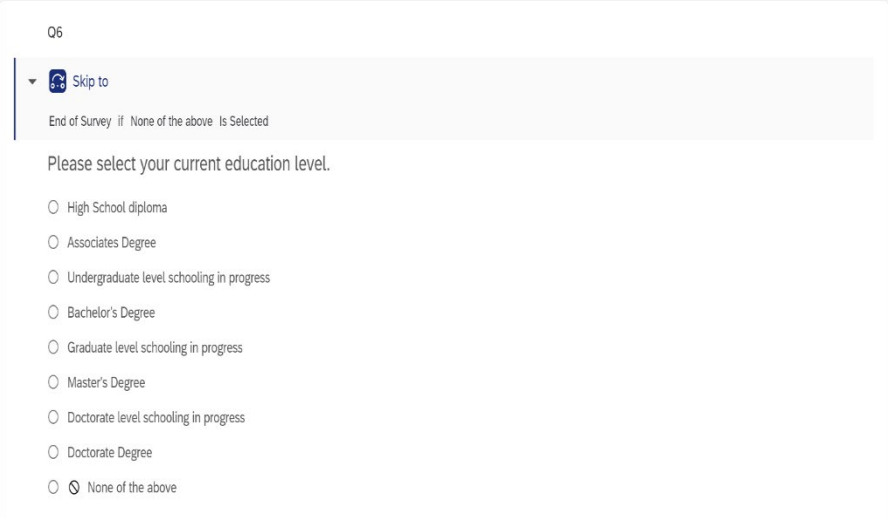


Figure 39. Question five example

6. Create a new block by selecting "Add Block." This block will be labeled "No Initial Categorization (Meme 1)." Open the block add a new "Text/Graphic" question. Then, change the content type to graphic. Without adding a graphic, add a new multiple-choice question to this block. Because this block is labeled as "No Initial Categorization," we will input question set two from Section B of this chapter, which contains eight answer choices. The block created will look like Figure 40.

Page 2543 of 3957

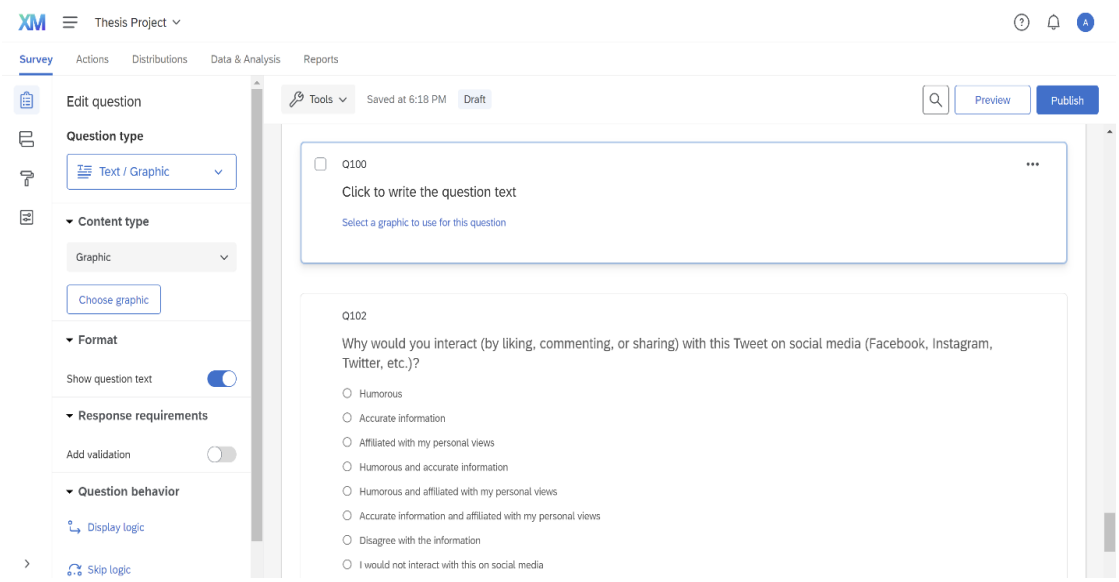


Figure 40. No initial categorization block example

7. After completing the above block, click the three dots to the right of the block title. Click "copy" and insert "No Initial Categorization (Meme 2)" into the "Please type a brief name/description of the new block:" box. After copying the block once, continue until you have created enough blocks for seven no initial categorization memes and seven no initial categorization Tweets.

8. Step 8: Create a new block and label it "Initial Categorization (Meme 1)." Add a "Text/Graphic" question to the block and change the content type to graphic. Without adding a graphic, add three new multiple-choice questions to this block. Because this block is labeled as "Initial Categorization," we will input question set one from Section B of this chapter, which contains three questions, one with two answers and two with seven answer choices. On the "IF YES" and "IF NO" questions, add the question behavior "Display Logic." Click "Question," then select the yes/no multiple-choice question in the block you are working in, and select answer choice yes/no depending on the associated question. The block created will look like Figure 41 below.

Page 2544 of 3957

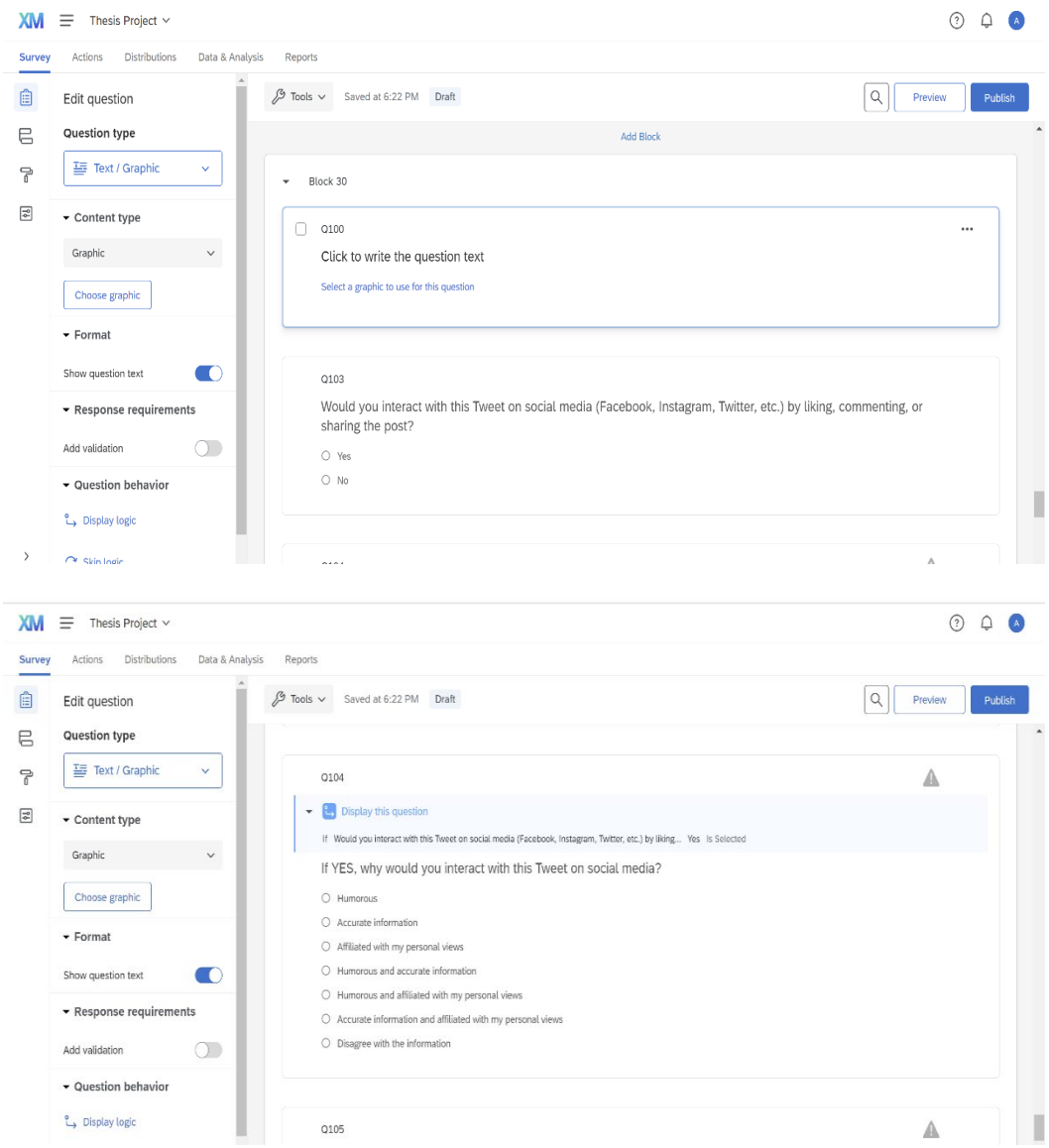


Figure 41. Initial categorization block example

9. After completing the above block, click the three dots to the right of the block title. Click “copy” and insert “Initial Categorization (Meme 2)” into the “Please type a brief name/description of the new block:” box. After copying the block once, continue until you have created enough blocks for seven initial categorization memes and seven initial categorization Tweets.

Page 2545 of 3957

10. At the top of the webpage, click the three lines next to the Qualtrics logo. After clicking, select the "Library" from the drop down. Click on "Graphic Library" right below the logo and three lines.

11. Click "New Folder" and title it "No Initial Categorization Memes." Then, hit "Upload Graphic" and upload the seven images that will be used for the "No Initial Categorization Memes." After they are uploaded, click the gray box under the first image and label it "NIC M1," which stands for "No Initial Categorization Meme 1." Label the remaining six images, ensuring to change the number after each "M."

12. Repeat step 11 until folders for "No Initial Categorization Tweets," "Initial Categorization Memes," and "Initial Categorization Tweets" are complete. Ensure that the picture labeling is altered in each new folder, accurately depicting what graphic folder and graphic number it is assigned.

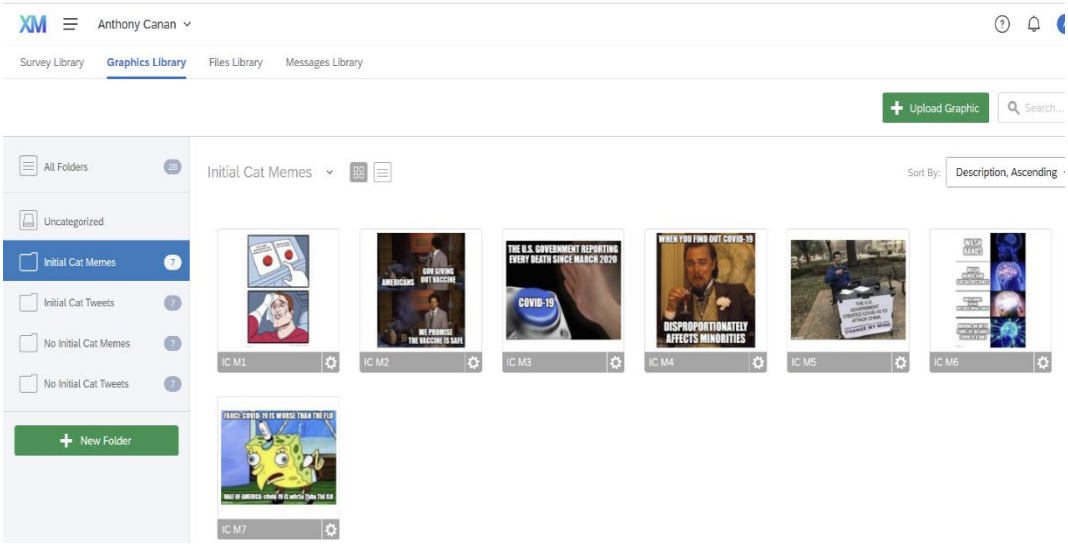


Figure 42. Complete Qualtrics image library

13. Return to your project. On the block titled "No Initial Categorization (Meme 1)," click on the empty "Text/Graphic" question. Click "Choose

Page 2546 of 3957

graphic." Match the block title to the graphic label. For example, click the image labeled "NIC M1" and it will automatically appear in the question.

14. Move to the next empty block and repeat step 13, ensuring that the block title and the graphic title match. Continue until all 28 blocks have graphics inserted.

15. Add a final block with a "Text Entry" question. This question alerts the participant that the survey is over and that all information they were presented with was false. It also requires that they acknowledge that they viewed misinformation and are complete with the survey. See Figure 43 for an example.

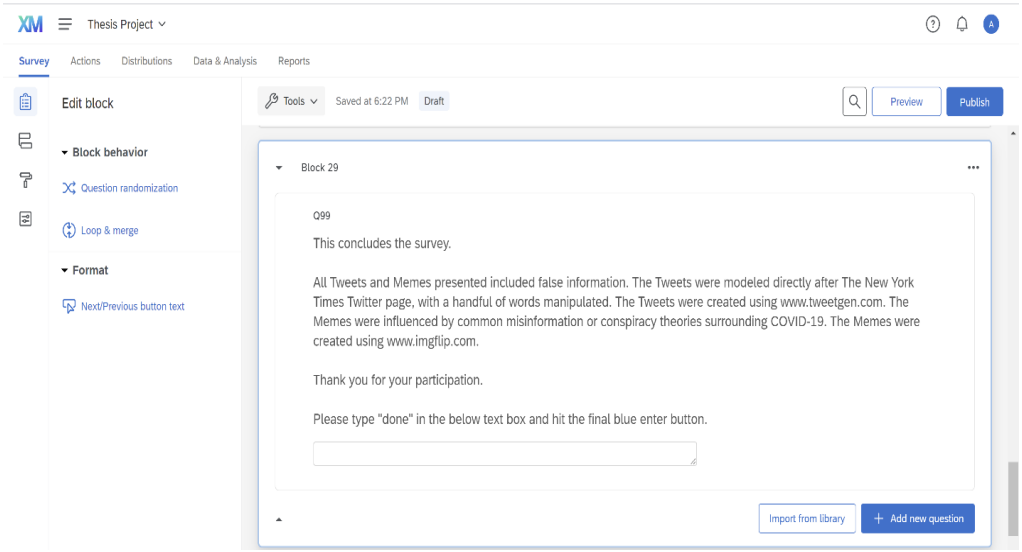


Figure 43. End of survey acknowledgement

16. Click on the "Survey Flow" icon on the left side of the screen. Currently, all the blocks will be left justified in a single line. In order to get the survey to flow like the diagram in Section B, adjustments need to be made. Click "Add a New Element Here" and select "Randomizer." On the new element, click "Evenly Present Elements." Under your new element, click "Add a New Element Here" and select "Randomizer" again. Again,

Page 2547 of 3957

click “Evenly Present Elements” on the newest “Randomizer.” Finally, under your newest element, hit “Add a New Element Here” and select “Randomizer” for a third time. Under the third “Randomizer,” click “Add a New Element Here” and select “Block.” Add all seven blocks for “No Initial Categorization (Meme X)” here. See Figure 44 for an example.

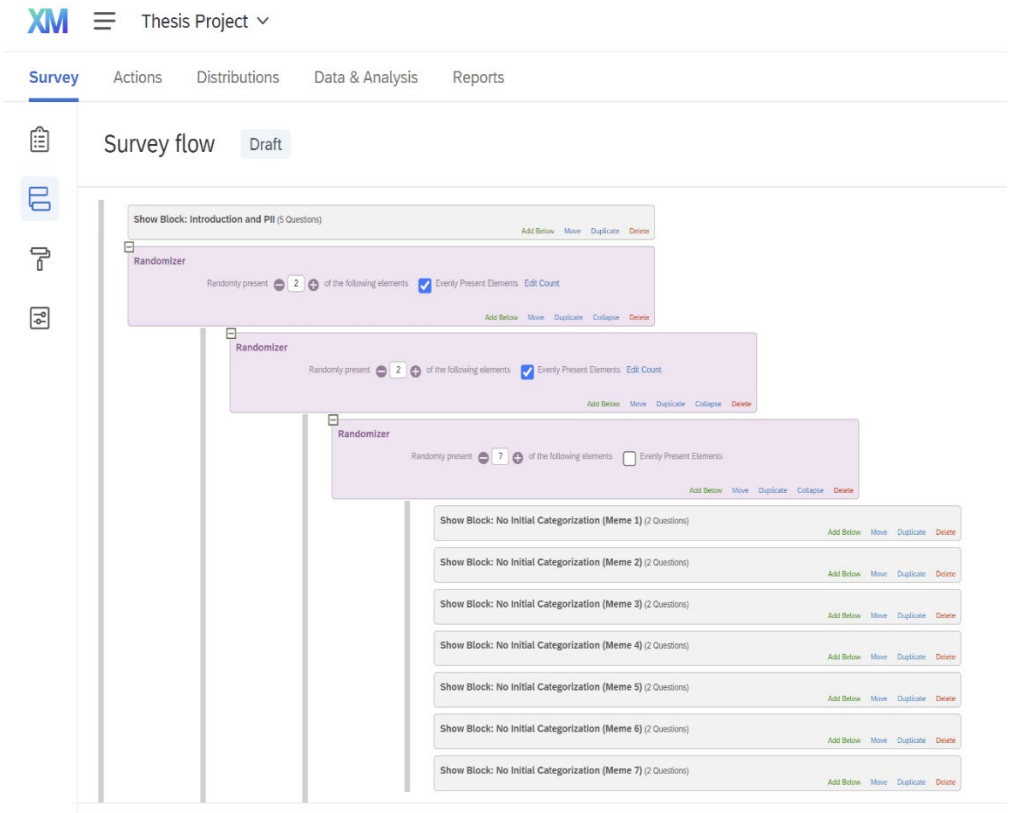


Figure 44. First set of the survey flow

17. Under your second “Randomizer,” not the most right justified, click “Add a New Element Here,” and select another “Randomizer.” Under the new “Randomizer,” add all seven of the “Initial Categorization (Meme X)” blocks. See Figure 45 for an example.

Page 2548 of 3957

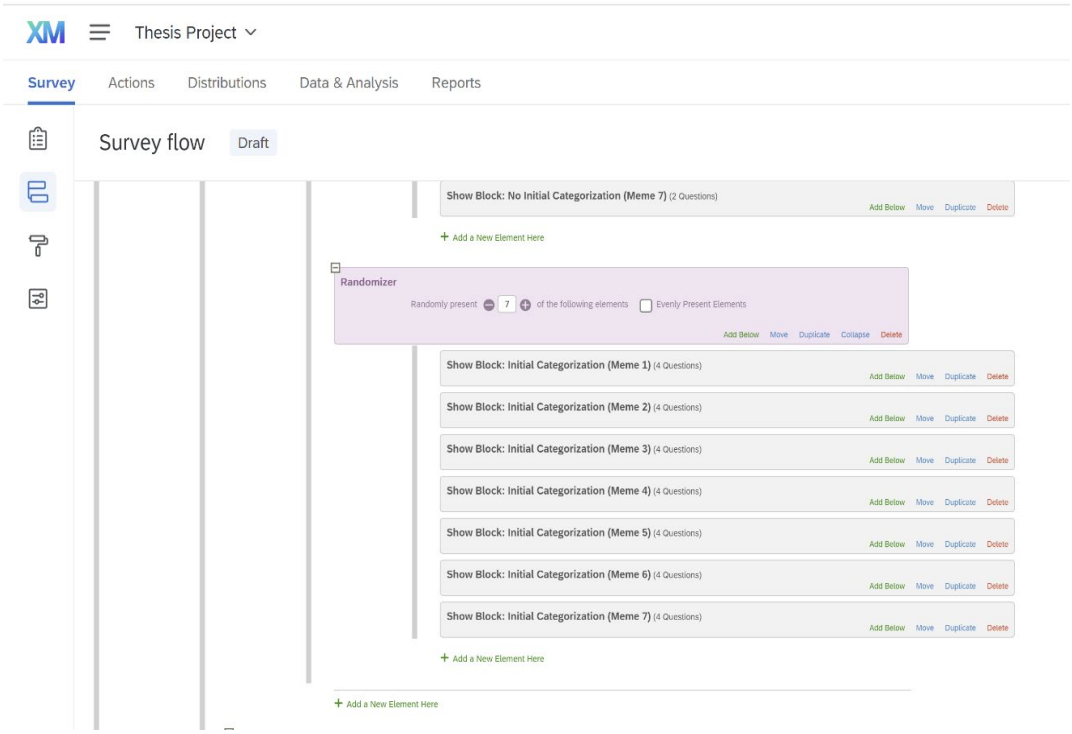


Figure 45. Second set of the survey flow

18. Under the left most justified "Randomizer," select "Add a New Element." Click "Evenly Present Elements."

19. Add an additional "Randomizer" onto the newest "Randomizer" created in step 17. Under the newest randomizer, add all seven of the "No Initial Categorization (Tweet X)" blocks. Repeat this step by adding another "Randomizer" and all seven of the "Initial Categorization (Tweet X)" blocks.

20. On the left most justified line, add a final new element as a "Block" and select "Show Block: End of Survey Acknowledgement."

21. In the top right corner, select the "Preview" button and ensure the survey is working as intended. The first page will look like Figure 46.

Page 2549 of 3957

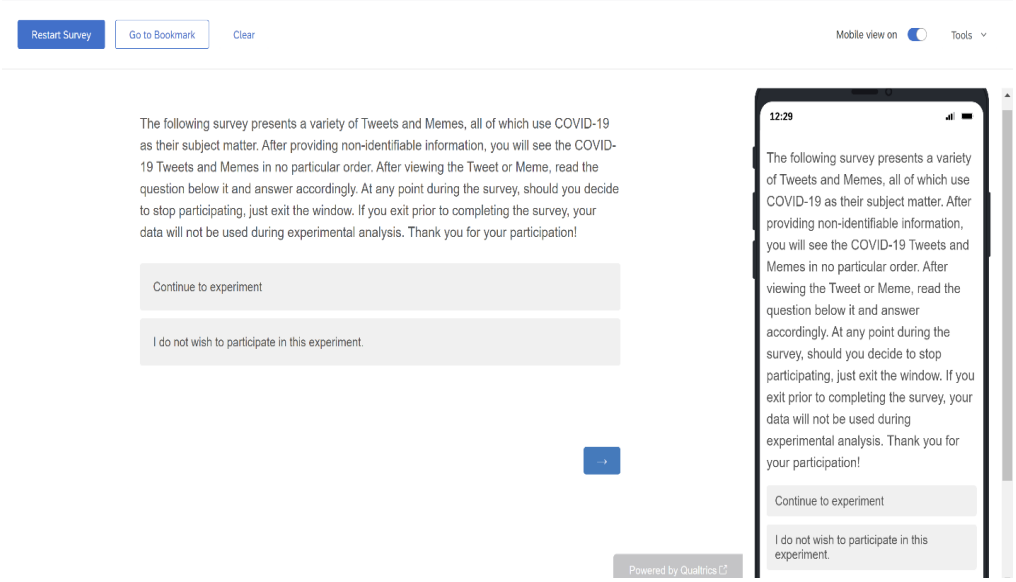


Figure 46. Preview of the survey

2. Testing the Survey

Once the Qualtrics building portion was complete, the survey was tested by four individuals, verifying that it works as intended. No results were recorded.

E. LIMITATIONS

The greatest limitation to this experimental design is the use of one type of meme. As mentioned previously, memes encompass a wide array of digital objects. This experiment, however, is only designed to draw correlations with image macro memes. Additionally, this experiment uses Tweets that only include text blurbs. On Twitter, users can imbed images and links, which may affect the way users interact with the digital objects. Finally, the experiment is designed to be run online using Mechanical Turk or a similar experiment platform. While these platforms are used to run many experiments, individuals of certain socio-economic statuses may not have means to access and perform the experiment, possibly removing a large audience from survey results.

Page 2550 of 3957

V. FUTURE WORK, IMPLICATIONS, CONCLUSION

A. FUTURE WORK

First and foremost, it is recommended that this experiment be run to its fullest capacity. Once conducted, it is recommended that researchers adjust the type of meme to test for correlations between type and the selected independent variables. Additionally, it is recommended that the Tweets be imbedded with images or links to see if that affects participant interaction rate. Finally, it is recommended that the experiment be conducted world-wide to determine if various nations respond differently to the use of Tweets and memes to spread false information.

B. IMPLICATIONS

Throughout this thesis, it has been made apparent that memes are wide-scale information dissemination tools that are poorly understood by much of academia. Despite that, memes are being utilized to spread false narratives on a global scale. While research suggests that memes reach depths greater than traditional images, and misinformation gets shared at far greater rates than true information, there is extremely limited text detailing who is responsible for this phenomenon. The experiment designed in this thesis will add to a new body of work that attempts to determine who is influenced by and propagates the majority of Tweet and meme information disorder. After conducting the experiment and drawing correlations, the relationships identified can be acted upon on both a defensive and offensive level by a multitude of entities.

If it is noted that certain genders, age groups, or education levels interact with and believe false information at greater rates than others, individuals and organizations, like the military, will be able to create and conduct targeted information disorder training. As a defensive tactic, said organizations can protect their at-risk members from falling victim to and propagating memes that involve information disorder. Whether it be political, extremist, social-activist, or marketing based, the results of this experiment, when properly acted upon, can help curb the belief and spread of dangerous narratives related to those topics.

Page 2551 of 3957

This experiment has extreme potential in the offensive realm. As noted throughout this thesis, other countries have begun using meme information disorder on American citizens. However, it is unlikely that they know who is most influenced by the narratives that they spread. The military would be able to infiltrate adversary social media platforms (which are different than the popular ones in the United States) and imbed information disorder that spreads a western narrative. Additionally, marketing firms can utilize the same tactics to reach greater levels of exposure, likely boosting sales. Conducting the experiment detailed in the previous chapter has the ability to show a more effective route to meme influence when targeting a hostile audience and provide a method for identifying potential vulnerabilities to nefarious actors' attempts to target domestic audiences.

C. CONCLUSION

The use of social media has been growing every year since inception. With that, individuals, organizations, businesses, and nations have created clever ways to spread messages to large audiences. However, in the last decade, those same entities have begun utilizing social media to spread false narratives that fit their agenda. Using Tweets and memes, non-state and state actors have successfully influenced elections, incited riots, and increased membership. Current academic research does not describe who is most susceptible to this new type of information disorder. For that reason, the experiment detailed in this thesis was designed. When conducted, it will reveal correlations between the acceptance and propagation of false information spread through Tweets and memes and the age group, gender, and education level of those most likely to interact with the false information. Once complete, defensive and offensive measures can be put in place by individuals, organizations, businesses, and nations to defend or attack the most at-risk groups.

Page 2552 of 3957

LIST OF REFERENCES

Aliciamccarvell [@aliciamccarvell]. (2021, May 28). Examination of Instagram follower count. Instagram. https://www.instagram.com/aliciamccarvell/

Al-Rawi, A. (2021). Political memes and fake news discourses on Instagram. *Media and Communication* (Lisboa), *9*(1), 276–290. https://doi.org/10.17645/mac.v9i1.3533

Astapova, A., & Navumau, V. (2018). Veyshnoria: A fake country in the midst of real information warfare. *Journal of American Folklore*, *131*(522), 435–443. https://doi.org/10.5406/jamerfolk.131.522.0435

Andrejevic, M. (2020). The political function of fake news: Disorganized propaganda in the era of automated media. In M. Zimdars & K. McLeod (Eds.), *Fake news: Understanding media and misinformation in the digital age* (pp. 19–28). The MIT Press.

Auxier, B. & Anderson, M. (2021. April 7). *Social Media Use in 2020*. Pew Research Center. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Barkbox [@barkbox]. (2021, Mar 23). My obsession with this @osotheakbash pic knows no bounds. [Meme]. Instagram. https://www.instagram.com/p/CMxe7SeD3Gx/

Barker, S. (2021, Mar 18). *Marketing with memes-How to use them to gain traction (updated March 2021).* Shane Baker. https://shanebarker.com/blog/marketing-memes/

Bazelon, E. (2020, June 15). *Restarting America Means People Will Die. So When Do We Do it?* The New York Times Magazine. https://www.nytimes.com/2020/04/10/magazine/coronavirus-economy-debate.html

BBC. (2020, May 4). *Coronavirus: Ghana's dancing pallbearers become Covid-19 meme* [Video]. https://www.bbc.com/news/av/world-africa-52503049

Beals, R. K. (2020, Mar 16). *Trump believes coronavirus will vanish with April temps experts are skeptical Warm weather alone is enough*. MarketWatch. https://www.marketwatch.com/story/trump-believes-coronavirus-will-vanish-with-april-temps-experts-are-skeptical-warm-weather-alone-is-enough-2020-03-12

Beskow, D., Kumar, S., & Carley, K. (2020). The evolution of political memes: Detecting and characterizing internet memes with multi-modal deep learning. *Information Processing & Management*, *57*(2). https://doi.org/10.1016/j.ipm.2019.102170

Bessi, A. & Ferrara, E. (2016, Nov 2). *Social bots distort the 2016 U.S. Presidential election online discussion*. First Monday. https://firstmonday.org/article/view/7090/5653

Betches [@betches]. (2021, May 28). Examination of content on account. Instagram. https://www.instagram.com/betches/

Page 2553 of 3957

Blaha, M. (2021). *5 vaping facts you need to know*. Johns Hopkins Medicine. https://www.hopkinsmedicine.org/health/wellness-and-prevention/5-truths-you-need-to-know-about-vaping

Bremmer, I. (2021, Feb 23). *The best global responses to COVID-19 pandemic, 1 year later*. Time. https://time.com/5851633/best-global-responses-covid-19/

Bowman, N.D. & Cohen, E. (2020). Mental shortcuts, emotion, and social rewards: The challenges of detecting and resisting fake news. In M. Zimdars & K. McLeod (Eds.). *Fake News: Understanding Media and Misinformation in the Digital Age* (pp. 224–233). The MIT Press.

Boulter, M. & Bolaji, L. (2020, Jan 23). *In the age of memes, how are young people getting their news?* PBS. https://www.pbs.org/newshour/nation/in-the-age-of-memes-how-are-young-people-getting-their-news

Burroughs, B. (2020). Fake memetics: political rhetoric and circulation in political campaigns. In M. Zimdars & K. McLeod (Eds.). *Fake News: Understanding Media and Misinformation in the Digital Age* (pp. 191–200). The MIT Press.

BW Online Bureau. (Jan 2020). *Influencer marketing company Buzzoka ventures into meme marketing.* Business World. http://bwdisrupt.businessworld.in/article/Influencer-Marketing-Company-Buzzoka-Ventures-into-Meme-Marketing-/21-01-2020-182468/

Calabresi, M. (2017, May 18). *Inside Russia's social media war on America*. TIME. https://time.com/4783932/inside-russia-social-media-war-america/

Carney, N. (2016). All lives matter, but so does race: Black Lives Matter and the evolving role of social media. *Humanity & Society*, *40*(3), 180-199. https://doi-org.libproxy.nps.edu/10.1177/0160597616643868

Clarke, P. (2020, Sep 4). *Americans looking to international travel for early 2021*. Travel Pulse. https://www.travelpulse.com/news/destinations/americans-looking-to-international-travel-for-early-2021.html

Center for Countering Digital Hate. (2021). *About*. https://www.counterhate.com/about-us

Center for Disease Control. (2021, April 19). *Health equity considerations and racial and ethnic minority groups.* https://www.cdc.gov/coronavirus/2019-ncov/community/health-equity/race-ethnicity.html

Chen, W., Lakshmanan, L., & Castillo, C. (2013). *Information and influence propagation in social networks* . Morgan & Claypool. https://doi.org/10.2200/S00527ED1V01Y201308DTM037

Cillizza, C. (2020, Feb 27). *Why 2020 is the 'meme election'* [Video]. CNN. https://www.youtube.com/watch?v=96xEjfstBY8

Page 2554 of 3957

Cole, S. (2018, June 12). *Researchers studied 160 million memes and found most of them come from two websites*. Vice. https://www.vice.com/en/article/zm884j/where-do-memes-come-from-researchers-studied-reddit-4chan

Corera, G. (2020, Oct 5). *U.S. election 2020: Who do Russia, China, and Iran want to win?* BBC News. https://www.bbc.com/news/election-us-2020-54293489

Edosomwan, S., Prakasan, S., Kouame, D., Watson, J., & Seymour, T. (2011). The history of social media and its impact on business. *The Journal of Applied Management and Entrepreneurship, 16*(3). http://www.minot.com/tom/SocialMedia.pdf

Etter, M., & Albu, O. (2021). Activists in the dark: Social media algorithms and collective action in two social movement organizations. *Organization (London, England)*, 28(1), 68–91. https://doi.org/10.1177/1350508420961532

Fabbri, T. (2020, Nov 2*). U.S. election 2020: The people behind the political memes you share.* BBC News. https://www.bbc.com/news/election-us-2020-54748453

File, T. & Mohanty, A. (2021, Jan 27). *95% of those vaccinated got or intend to get all required doses.* United States Census Bureau. https://www.census.gov/library/stories/2021/01/around-half-of-unvaccinated-americans-indicate-they-will-definitely-get-covid-19-vaccine.html

Gerber, T., & Zavisca, J. (2016). Does Russian propaganda work? *The Washington Quarterly, 39*(2), 79–98. https://doi.org/10.1080/0163660X.2016.1204398

Glucksman, M. (2017). The rise of social media influencer marketing on lifestyle branding: A case study of Lucie Fink. *Elon Journal of Undergraduate Research in Communications, 8*(2), p. 77-87. https://www.elon.edu/u/academics/communications/journal/wp-content/uploads/sites/153/2017/12/Fall2017Journal.pdf#page=77

Gorman, D. (2021, Mar 25). *How effective are ads on social media?* Global Web Index. https://blog.globalwebindex.com/trends/ads-on-social-media/

Graff, G. M. (2018, Oct 19). *Russian trolls are still playing both sides even with the Mueller probe.* Wired. https://www.wired.com/story/russia-indictment-twitter-facebook-play-both-sides/

Gruzd, A. & Haythornthwaite, C. (2013). Enabling community through social media. *Journal of Medical Internet Research, 15*(10). https://www.jmir.org/2013/10/e248/

He, Z., & Jiang, W. (2018). An evidential dynamical model to predict the interference effect of categorization on decision making results. *Knowledge-Based Systems, 150*, 139–149. https://doi.org/10.1016/j.knosys.2018.03.014

Heiskanen, B. (2017). Meme-ing electoral participation. *European Journal of American Studies, 12*(2). http://dx.doi.org.libproxy.nps.edu/10.4000/ejas.12158

Page 2555 of 3957

HOPE not hate. (2021, Mar). *State of hate 2021: Backlash, conspiracies & confrontation*. https://www.hopenothate.org.uk/wp-content/uploads/2021/03/state-of-hate-2021-final-2.pdf

Houck, S., Repke, M., & Conway, L. (2017). Understanding what makes terrorist groups' propaganda effective: An integrative complexity analysis of ISIL and Al Qaeda. *Journal of Policing, Intelligence and Counter Terrorism, 12*(2), 105–118. https://doi.org/10.1080/18335330.2017.1351032

The International News. (2021, Feb 16). *India's top bank latest brand to hop on to Pakistani influencer's #PawriHoriHai meme*. https://www.thenews.com.pk/latest/790939-indias-top-bank-latest-brand-to-hop-on-to-pakistani-influencers-pawrihorihai-meme

Isaac, P. (2020, Nov 7). *These 2020 U.S. presidential election memes will keep you laughing until inauguration day.* Cosmopolitan. https://www.cosmopolitan.com/politics/a34607531/best-2020-us-presidential-election-memes-tweets/

Jin, S., Muqaddam, A., & Ryu, E. (2019). Instafamous and social media influencer marketing. *Marketing Intelligence & Planning*, *37*(5), 567-579. https://doi.org/10.1108/MIP-09-2018-0375

Kao, J. & Li, M. S. (2020, Mar 26). *How China built a Twitter propaganda machine the let it loose on Coronavirus.* ProPublica. https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus

Klepper, D., Amiri, F., & Dupuy, B. (2021, Feb 15). *The superspreaders behind top COVID-19 conspiracy theories*. Los Angeles Times. https://www.latimes.com/world-nation/story/2021-02-15/the-superspreaders-behind-top-covid-19-conspiracy-theories

Kouzy, R., Abi Jaoude, J., Kraitem, A., El Alam, M., Karam, B., Adib, E., Zarka, J., Traboulsi, C., Akl, E., & Baddour, K. (2020). Coronavirus goes viral: Quantifying the COVID-19 misinformation epidemic on Twitter. *Curēus*, *12*(3), 7255. https://doi.org/10.7759/cureus.7255

Laub, P., Taimre, T., & Pollett, P. (2015). Hawkes Processes. *Cornell University arXiv*. https://arxiv.org/abs/1507.02822

Lee, H., Liang, C. Liao, S., & Chen, H. (2019). Analyzing the intention of consumer purchasing behaviors in relation to internet memes using VAB model. *Sustainability, 11*(20), 5549. https://doi.org/10.3390/su11205549

Lee, N. (2020, April 6). *Selfishness during a pandemic may have killed my father. It shouldn't have ended this way.* The Colorado Sun. https://coloradosun.com/2020/04/06/write-on-colorado-nicky-lee/

Page 2556 of 3957

Lewis, T. (2020, Oct 12). Eight persistent COVID-19 myths and why people believe them. Scientific American. https://www.scientificamerican.com/article/eight-persistent-covid-19-myths-and-why-people-believe-them/

Liu, J., McLaughlin, S., Lazaro, A., & Halpern-Felsher, B. (2020). What does it meme? A qualitative analysis of adolescents' perceptions of tobacco and marijuana messaging. *Public Health Reports (1974), 135*(5), 578–586. https://doi.org/10.1177/0033354920947399

Luo, C., Zheng, X., & Zeng, D. (2015). Inferring social influence and meme interaction with Hawkes processes. *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 135–137. https://doi.org/10.1109/ISI.2015.7165953

Lynas, M. (2020, April). *COVID: Top 10 current conspiracy theories.* Cornell Alliance for Science. https://allianceforscience.cornell.edu/blog/2020/04/covid-top-10-current-conspiracy-theories/

Mahan, L. (2020, Nov 9). *The story of election week 2020, as told by its memes.* InsideHook. https://www.insidehook.com/article/internet/election-week-2020-memes

Mammoser, G. (2018, Dec 9). *The FOMO is real: How social media increases depression and loneliness.* Healthline. https://www.healthline.com/health-news/social-media-use-increases-depression-and-loneliness

Mathew, J. (2018, July 30). *Understanding influencer marketing and why it is so effective*. Forbes. https://www.forbes.com/sites/theyec/2018/07/30/understanding-influencer-marketing-and-why-it-is-so-effective/?sh=1f6a076671a9

McLaughlin, E. (2020, Aug 9). *How George Floyd's death ignited a racial reckoning that shows no signs of slowing down.* CNN. https://www.cnn.com/2020/08/09/us/george-floyd-protests-different-why/index.html

McMinn, S. (2020, Mar 25). *Why Hong Kong students spreading racist coronavirus memes and blaming China are playing with fire*. South China Morning Post. https://www.scmp.com/comment/opinion/article/3076738/why-hong-kong-students-spreading-racist-coronavirus-memes-and

Meyers, S. L. & Mozur, P. (2019, Aug 13). *China is waging a disinformation war against Hong Kong protestors*. The New York Times. https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html

MediaKix. (2021). *Influencer Marketing Effectiveness: Key Survey Finds, Facts & Figures [Infographic].* https://mediakix.com/blog/influencer-marketing-effectiveness/#:~:text=80%25%20of%20marketers%20find%20influencer,better%20than%20other%20marketing%20channels.

Mina, A.X. (2019). *Memes to movements: How the world's most viral media is changing social protest and power*. Beacon Press.

Page 2557 of 3957

Mohsin, M. (2021, Feb 16). *10 Instagram Stats Every Marketer Should Know in 2021 [Infographic].* Oberlo. https://www.oberlo.com/blog/instagram-stats-every-marketer-should-know#:~:text=There%20are%201.074%20billion%20Instagram,of%2053%20minutes%20per%20day.

Mottola, M. (2020, Sep 29). *Seven types of engaging visual content for social media ads*. *Forbes*. https://www.forbes.com/sites/theyec/2020/09/29/seven-types-of-engaging-visual-content-for-social-media-ads/?sh=3cd7bdfa1a06

Naishadham, S., Johnson, C. K., & Marcelo, P. (2020, Aug 4). *'Too many people are selfish': As Americans resist COVID-19 restrictions, U.S. nears 5 million infections*. Chicago Tribune. https://www.chicagotribune.com/coronavirus/ct-nw-covid-19-updates-20200804-psj6rlmvvrhedaph4h2mpztalm-story.html

National Intelligence Council. (2021). *Global trends 2040: A more contested world*. https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf

National Post Staff. (2017, Nov 2). *'Hillary is a Satan': Ten ads that Russian trolls posted during the 206 U.S. election.* https://nationalpost.com/news/world/hillary-is-a-satan-ten-ads-that-russian-trolls-posted-during-the-2016-u-s-election

News18. (2021, Feb 15). *Netflix to Zomato, here's how brands are putting the 'Pawri' meme to market use*. https://www.news18.com/news/buzz/netflix-to-zomato-heres-how-brands-are-putting-the-pawri-meme-to-market-use-3435959.html

NewsGuard. (2021, Mar 29). *Newsguard launches "responsible advertising for news segments" to help brands stop funding misinformation.* 3BL CSR Wire. https://www.csrwire.com/press_releases/720336-newsguard-launches-responsible-advertising-news-segments-help-brands-stop

The New York Times [@nytimes]. (2021). Review of Tweets about COVID-19 pandemic. Twitter. https://twitter.com/nytimes?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

Nissen, M. (2013). Knowledge uniqueness. *Harnessing dynamic knowledge principles in the technology-driven world* (pp. 14–25). IGI Global. https://doi.org/10.4018/978-1-4666-4727-5.ch002

O'Brien, M., Moore, K., & McNicholas, F. (2020). Social media spread during COVID-19: the pros and cons of likes and shares. *Irish Medical Journal, 113*(4). https://www.irishpsychiatry.ie/wp-content/uploads/2020/04/Social-Media-Spread-During-Covid-19-The-Pros-and-Cons-of-Likes-and-Shares-IMJ-2020.pdf

Page 2558 of 3957

Ohlheiser, A. (2020, May 17). *Maybe it's time to retire the idea of "going viral."* MIT Technology Review. https://www.technologyreview.com/2020/05/17/1001809/maybe-its-time-to-retire-the-idea-of-going-viral/

Perrin, A. (2020, Oct 15). *23% of users in U.S. say social media led them to change views on an Issue; some cite Black Lives Matter*. Pew Research Center. https://www.pewresearch.org/fact-tank/2020/10/15/23-of-users-in-us-say-social-media-led-them-to-change-views-on-issue-some-cite-black-lives-matter/

Pfeiffer, D. (2020, Feb 18). *Wake up, Democrats! Memes matter in the race to 2020.* Wired. https://www.wired.com/story/opinion-wake-up-democrats-memes-matter-in-the-race-to-2020/

Pinsker, J. (2021, Feb 22). *The most likely timeline for life to return to normal*. The Atlantic. https://www.theatlantic.com/family/archive/2021/02/pandemic-daily-life-normal-summer-fall/618108/

Pitofsky, M. (2021, Feb 10). *Over 30 percent of Americans say they won't get COVID-19 vaccine: Poll.* The Hill. https://thehill.com/policy/healthcare/538198-over-30-percent-of-americans-say-they-wont-get-covid-19-vaccine-poll

Posetti, J. & Bontcheva, K. (2020, April 23). *Key themes and formats of the COVID-19 disinfodemic according to UN-ICFJ research.* ijnet. https://ijnet.org/en/story/key-themes-and-formats-covid-19-disinfodemic-according-un-icfj-research

Raaf, D. (2018, July 16). *These 3 brands are using viral memes to crush it on Instagram*. Medium. https://medium.com/@danraaf/these-3-brands-are-using-viral-memes-to-crush-it-on-instagram-ad38fc7ce82

Sarcasm_only [@sarcasm_only]. (2021, May 28). Examination of account content. Instagram. https://www.instagram.com/sarcasm_only/

Shepherd, M. (2021, Mar 17). *Small business marketing statistics and trends (2021).* Fundera. https://www.fundera.com/resources/small-business-marketing-statistics

Slimjim [@slimjim]. (2020, Dec 26). Slimyim. [Meme]. Instagram. https://www.instagram.com/p/CJRaYPrgylO/

Sprout Social. (2018). *Sprout social index*. https://media.sproutsocial.com/uploads/2019/04/Sprout-Social-Index-2018.pdf

Suciu, P. (2019, Oct 11). *More Americans are getting their news from social media.* Forbes. https://www.forbes.com/sites/petersuciu/2019/10/11/more-americans-are-getting-their-news-from-social-media/?sh=7c70ba303e17

Page 2559 of 3957

Timberg, C. & Dwoskin, E. (2018, Jul 6). *Twitter is sweeping out fake accounts like never before, putting user growth at risk.* The Washington Post. https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/

Twitter. (2021a, Mar 31). *About*. https://about.twitter.com/

Twitter. (2021b, Mar 31). *COVID-19 misleading information policy.* https://help.twitter.com/en/rules-and-policies/medical-misinformation-policy

Twitter. (2021c, May 31). *Healthy conversations.* https://about.twitter.com/en/our-priorities/healthy-conversations

U.S. Senate. (2019). *(U) Report of the Select Committee on Intelligence United States Senate on Russian active measures, campaigns, and interference in the 2016 U.S. election, volume 2: Russia's use of social media with additional views.* https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science (American Association for the Advancement of Science), 359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Wang, L. & Wood, B. (2011). An epidemiological approach to model the viral propagation of Memes. *Applied Mathematical Modelling, 35*, 5442–5447. https://www.sciencedirect.com/science/article/pii/S0307904X11002824#!

Wang, Z., & Busemeyer, J. (2016). Interference effects of categorization on decision making. *Cognition, 150*, 133–149. https://doi.org/10.1016/j.cognition.2016.01.019

Wardle, C. (2020). Journalism and the new information ecosystem: Responsibilities and challenges. In M. Zimdars & K. McLeod (Eds.). *Fake News: Understanding Media and Misinformation in the Digital Age* (pp. 71–85). The MIT Press.

Wardle, C. & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. *Council of Europe Report DGI (2017), 09.* https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Wardle, C. (2019). *First Draft's essential guide to understanding information disorder*. First Draft. https://firstdraftnews.org/wp-content/uploads/2019/10/Information_Disorder_Digital_AW.pdf?x76701

Warren, J. (2021, Jan 4). *This is how the Instagram algorithm works in 2021*. Later. https://later.com/blog/how-instagram-algorithm-works/

Weise, E. (2018, May 10). *Here's how Russian manipulators were able to target Facebook users*. USA Today. https://www.usatoday.com/story/tech/2018/05/10/how-russia-targeted-facebook-ads-disrupt-elections/596665002/

Page 2560 of 3957

Weitz, R. (2020). The Sino-Russian disinformation axis during the COVID-19 pandemic. *China Brief*, *20*(14). https://jamestown.org/program/the-sino-russian-disinformation-axis-during-the-covid-19-pandemic/

Wharton Business Daily. (2020, Aug 17). *How social media is shaping political campaigns*. Knowledge @Wharton. https://knowledge.wharton.upenn.edu/article/how-social-media-is-shaping-political-campaigns/

White House. (2021, April 151). *Fact Sheet: Imposing costs for harmful foreign activities by the Russian government*. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

WeRateDogs. (2021a, Feb 28). *WeRateDogs Shop*. https://weratedogs.com/collections/shop-all

Weratedogs [@weratedogs]. (2021b, May 31). Review of weratedogs Instagram. Instagram. https://www.instagram.com/weratedogs/?hl=en

WeRateDogs [@dog_rates]. (2021c, May 21). Review of WeRateDogs Twitter. Twitter. https://twitter.com/dog_rates?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

Wyrich, A. (2017, Nov 1). *Here are the Facebook ads Russia used in its 2016 election influence scheme.* Daily Dot. https://www.dailydot.com/debug/russia-facebook-ads-2016-election/

Zimdars, M. (2020). Introduction. In M. Zimdars & K. McLeod (Eds.). *Fake News: Understanding Media and Misinformation in the Digital Age* (pp. 1–11). The MIT Press.

Zitser, J. (2021, Mar 27). *Neo-Nazi groups are using Instagram to recruit young teenagers, experts warn. Memes are being used to entice them.* Insider. https://www.businessinsider.com/instagram-memes-used-recruit-young-people-to-nazi-groups-experts-2021-3

Page 2561 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2562 of 3957

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

Page 2563 of 3957

Naval Criminal Investigative Service
Office of Strategic Communications
Quantico, Va.

FOR IMMEDIATE RELEASE
RELEASE: 02-23-01
FEBRUARY 23, 2024

CONTACT: NCISPUBLICAFFAIRS@NCIS.NAVY.MIL

NCIS LEADS COUNTERINTELLIGENCE INVESTIGATION RELATING TO ESPIONAGE

The Naval Criminal Investigative Service (NCIS) is leading a counterintelligence investigation of U.S. Navy Chief Petty Officer Bryce Pedicini, assigned to USS HIGGINS (DDG 76), involving several violations of the Uniform Code of Military Justice relating to espionage.

NCIS Office of Special Projects and the NCIS Far East Field Office detained and questioned Pedicini on May 19, 2023, after being suspected of removing classified information from U.S. Navy secure spaces and passing them to a representative of a foreign government as early as November 2022. Pedicini was arrested by NCIS in May 2023 and placed into pre-trial confinement by his command. He is awaiting a General Court Martial in San Diego, Calif.

On Sept. 22, 2023, charges were preferred against Pedicini by U.S. Navy Region Legal Service Office Southwest for violations of:

- Article 103a (Espionage/Attempted Espionage)
- Article 134 (Communicating Defense Information)
- Article 92 (Failure to Obey a Lawful General Order)
- Article 80 (Attempted Violation of a Lawful General Order) of the Uniform Code of Military Justice

These charges include allegations that Pedicini delivered classified and national defense information to a representative of a foreign government with reason to believe it would be harmful to the United States or advantageous to the foreign nation.

A preliminary hearing officer found there was sufficient probable cause to believe Pedicini committed the above-listed violations and recommended additional charges pertaining to conspiracy and unauthorized access on Dec. 14, 2023. The Convening Authority, Commander,

Naval Surface Force, U.S. Pacific, referred charges to a general court martial on Feb. 13, 2024. A tentative trial date is scheduled for April 2024.

This investigation is part of the ongoing efforts by NCIS to prevent the exploitation of U.S. Navy personnel by foreign adversaries. As the primary investigative and counterintelligence arm of the Department of the Navy, NCIS ensures the continued advantage of the Department of Defense and the Navy over foreign adversaries by conducting complex counterintelligence investigations and other sensitive national security matters involving the Navy and Marine Corps.

###

Foreign Economic Espionage in Cyberspace

2018

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
NCSC
UNITED STATES OF AMERICA

Contents

Executive Summary • **1**

Scope Note • **2**

I. The Strategic Threat of Cyber Economic Espionage • **4**

II. Threats from Foreign Countries • **5**

China: Persistent Cyber Activities • **5**

Russia: A Sophisticated Adversary • **8**

Iran: An Increasing Cyber Threat • **9**

Targeted Technologies • **11**

III. Emerging Threats • **12**

Software Supply Chain Operations • **13**

Foreign Laws Could Enable Intellectual Property Theft • **13**

Foreign Technology Companies With Links to Host Governments • **14**

Annex – Decreasing the Prevalence of Economic or Industrial Espionage in Cyberspace • **15**

Executive Summary

In the 2011 report to Congress on *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, the Office of the National Counterintelligence Executive provided a baseline assessment of the many dangers facing the U.S. research, development, and manufacturing sectors when operating in cyberspace, the pervasive threats posed by foreign intelligence services and other threat actors, and the industries and technologies most likely at risk of espionage. The 2018 report provides additional insight into the most pervasive nation-state threats, and it includes a detailed breakout of the industrial sectors and technologies judged to be of highest interest to threat actors. It also discusses several potentially disruptive threat trends that warrant close attention.

This report focuses on the following issues

Foreign economic and industrial espionage against the United States continues to represent a significant threat to America's prosperity, security, and competitive advantage. Cyberspace remains a preferred operational domain for a wide range of industrial espionage threat actors, from adversarial nation-states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups. Next-generation technologies, such as Artificial Intelligence (AI) and the Internet-of-Things (IoT) will introduce new vulnerabilities to U.S. networks for which the cybersecurity community remains largely unprepared. Building an effective response will require understanding economic espionage as a worldwide, multi-vector threat to the integrity of the U.S. economy and global trade.

Foreign intelligence services—and threat actors working on their behalf—continue to represent the most persistent and pervasive cyber intelligence threat. China, Russia, and Iran stand out as three of the most capable and active cyber actors tied to economic espionage and the potential theft of U.S. trade secrets and proprietary information. Countries with closer ties to the United States also have conducted cyber espionage to obtain U.S. technology. Despite advances in cybersecurity, cyber espionage continues to offer threat actors a relatively low-cost, high-yield avenue of approach to a wide spectrum of intellectual property.

A range of potentially disruptive threat trends warrant attention. Software supply chain infiltration already threatens the critical infrastructure sector and is poised to threaten other sectors. Meanwhile, new foreign laws and increased risks posed by foreign technology companies due to their ties to host governments, may present U.S. companies with previously unforeseen threats.

Cyber economic espionage *is but one facet* of the much larger, global economic espionage challenge. We look forward to engaging in the larger public discourse on mitigating the national economic harm caused by these threats.

Scope Note

This report is submitted in compliance with the National Defense Authorization Act for Fiscal Year 2015, Section 1637, which requires that the President annually submit to Congress a report on foreign economic espionage and industrial espionage in cyberspace during the 12-month period preceding the submission of the report.

Definitions of Key Terms

For the purpose of this report, key terms were defined according to definitions provided in Section 1637 of the National Defense Authorization Act for Fiscal Year 2015.

Economic or Industrial Espionage means (a) stealing a trade secret or proprietary information or appropriating, taking, carrying away, or concealing, or by fraud, artifice, or deception obtaining, a trade secret or proprietary information without the authorization of the owner of the trade secret or proprietary information; (b) copying, duplicating, downloading, uploading, destroying, transmitting, delivering, sending, communicating, or conveying a trade secret or proprietary information without the authorization of the owner of the trade secret or proprietary information; or (c) knowingly receiving, buying, or possessing a trade secret or proprietary information that has been stolen or appropriated, obtained, or converted without the authorization of the owner of the trade secret or proprietary information.

Cyberspace means (a) the interdependent network of information technology infrastructures; and (b) includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Contributors

The National Counterintelligence and Security Center (NCSC) compiled this report, with close support from the Cyber Threat Intelligence Integration Center (CTIIC), and with input and coordination from many U.S. Government organizations, including the Central Intelligence Agency (CIA), Defense Cyber Crime Center (DC3), Defense Intelligence Agency (DIA), Defense Security Service (DSS), Department of Energy (DoE), Department of Defense (DoD), Department of Homeland Security (DHS), Department of State (DoS), Department of Treasury (Treasury), Federal Bureau of Investigation (FBI), National Cyber Investigative Joint Task Force (NCIJTF), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and Office of the Director of National Intelligence (ODNI).

Page 2570 of 3957

I. The Strategic Threat of Cyber Economic Espionage

Foreign economic and industrial espionage against the United States continues to represent a significant threat to America's prosperity, security, and competitive advantage. Cyberspace remains a preferred operational domain for a wide range of industrial espionage threat actors, from adversarial nation-states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups. Next-generation technologies such as Artificial Intelligence (AI) and the Internet-of-Things (IoT) will introduce new vulnerabilities to U.S. networks for which the cybersecurity community remains largely unprepared. Building an effective response demands understanding economic espionage as a worldwide, multi-vector threat to the integrity of the U.S. economy and global trade.

The United States remains a global center for research, development, and innovation across multiple high-technology sectors. Federal research institutions, universities, and corporations are regularly targeted by online actors seeking all manner of proprietary information and the overall long-term trend remains worrisome.

While next generation technologies will introduce a range of qualitative advances in data storage, analytics, and computational capacity, they also present potential vulnerabilities for which the cybersecurity community remains largely unprepared. The solidification of cloud computing over the past decade as a global information industry standard, coupled with the deployment of technologies such as AI and IoT, will introduce unforeseen vulnerabilities to U.S. networks.

- **Cloud networks and IoT infrastructure are rapidly expanding the global online operational space.** Threat actors have already demonstrated how cloud can be used as a platform for cyber exploitation. As IoT and AI applications expand to empower everything from "smart homes" to "smart cities", billions of potentially unsecured network nodes will create an incalculably larger exploitation space for cyber threat actors.

- **Lack of industry standardization during this pivotal first-generation deployment period will likely hamper the development of comprehensive security solutions in the near-term.**

- **Building an effective response demands understanding economic espionage as a worldwide, multi-vector threat to the integrity of both the U.S. economy and global trade.** Whereas cyberspace is a preferred operational domain for economic espionage, it is but one of many. Sophisticated threat actors, such as adversarial nation-states, combine cyber exploitation with supply chain operations, human recruitment, and the acquisition of knowledge by foreign students in U.S. universities, as part of a strategic technology acquisition program.

Page 2572 of 3957

II. Threats from Foreign Countries

Foreign intelligence services—and threat actors working on their behalf—continue to represent the most persistent and pervasive cyber intelligence threat. China, Russia, and Iran stand out as three of the most capable and active cyber actors tied to economic espionage and the potential theft of U.S. trade secrets and proprietary information. Countries with closer ties to the United States have also conducted cyber espionage to obtain U.S. technology. Despite advances in cybersecurity, cyber espionage continues to offer threat actors a relatively low-cost, high-yield avenue of approach to a wide spectrum of intellectual property.

We anticipate that China, Russia, and Iran will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace. All will almost certainly continue to deploy significant resources and a wide array of tactics to acquire intellectual property and proprietary information.

Countries with closer ties to the United States have conducted cyber espionage and other forms of intelligence collection to obtain U.S. technology, intellectual property, trade secrets, and proprietary information. U.S. allies or partners often take advantage of the access they enjoy to collect sensitive military and civilian technologies and to acquire know-how in priority sectors.

China: Persistent Cyber Activities

China has expansive efforts in place to acquire U.S. technology to include sensitive trade secrets and proprietary information. It continues to use cyber espionage to support its strategic development goals—science and technology advancement, military modernization, and economic policy objectives. China's cyberspace operations are part of a complex, multipronged technology development strategy that uses licit and illicit methods to achieve its goals. Chinese companies and individuals often acquire U.S. technology for commercial and scientific purposes. At the same time, the Chinese government seeks to enhance its collection of U.S. technology by enlisting the support of a broad range of actors spread throughout its government and industrial base.

Page 2573 of 3957

China's Strategic Goals

Non-Traditional Collectors	China uses individuals for whom science or business is their primary profession to target and acquire US technology.
Joint Ventures (JV)	China uses JVs to acquire technology and technical know-how.
Research partnerships	China actively seeks partnerships with government laboratories-such as the Department of Energy labs-to learn about and acquire specific technology, and the soft skills necessary to run such facilities.
Academic Collaborations	China uses collaborations and relationships with universities to acquire specific research and gain access to high-end research equipment. Its policies state it should exploit the openness of academia to fill China's strategic gaps.
S&T Investments	China has sustained, long-term state investments in its S&T infrastructure.
M&A	China seeks to buy companies that have technology, facilities and people. These sometimes end up as Committee on Foreign Investment in the United States (CFIUS) cases.
Front Companies	China uses front companies to obscure the hand of the Chinese government and acquire export controlled technology.
Talent Recruitment Programs	China uses its talent recruitment programs to find foreign experts to return to China and work on key strategic programs.
Intelligence Services	The Ministry of State Security (MSS), and military intelligence offices are used in China's technology acquisition efforts.
Legal and Regulatory Environment	China uses its laws and regulations to disadvantage foreign companies and advantage its own companies.

Page 2574 of 3957

The Intelligence Community and private sector security experts continue to identify ongoing Chinese cyber activity, although at lower volumes than existed before the bilateral September 2015 U.S.-China cyber commitments. Most Chinese cyber operations against U.S. private industry that have been detected are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. Examples of identified ongoing Chinese cyber activity include the following:

- According to several cyber intelligence companies, in 2017 the China-associated cyber espionage group APT10 continued widespread operations to target engineering, telecommunications, and aerospace industries. APT10 targeted companies across the globe, including the United States, using its exploitation of managed IT service providers as a means to conduct such operations.
- Cybersecurity researchers have found links between Chinese cyber actors and a back door in the popular CCleaner application that allowed the actors to target U.S. companies, including Google, Microsoft, Intel, and VMware.
- In November 2017, PricewaterhouseCoopers (PWC) reported that the China-based APT, known as KeyBoy, was shifting its focus to target Western organizations. According to PWC, the targeting likely was for corporate espionage purposes. KeyBoy previously focused on Asian targets, according to commercial cybersecurity reporting.
- According to FireEye, in 2017 TEMP.Periscope continued targeting the maritime industry as well as engineering-focused entities including research institutes, academic organizations, and private firms in the United States. FireEye has detected sharp increases in targeting in early 2018 as well.

Recent Unsealed U.S. Indictment With a Link to China

In November 2017, Wu Yingzhuo, Dong Hao and Xia Lei, Chinese nationals and residents of China, were charged with computer hacking, theft of trade secrets, conspiracy, and identity theft. These efforts were directed at U.S. and foreign employees and the computers of three corporations that were victims in the financial, engineering, and technology industries between 2011 and May 2017.

We believe that China will continue to be a threat to U.S. proprietary technology and intellectual property through cyber-enabled means or other methods. If this threat is not addressed, it could erode America's long-term competitive economic advantage.

Russia: A Sophisticated Adversary

The threat to U.S. technology from Russia will continue over the coming years as Moscow attempts to bolster an economy struggling with endemic corruption, state control, and a loss of talent departing for jobs abroad. Moscow's military modernization efforts also likely will be a motivating factor for Russia to steal U.S. intellectual property. An aggressive and capable collector of sensitive U.S. technologies, Russia uses cyberspace as one of many methods for obtaining the necessary know-how and technology to grow and modernize its economy. Other methods include the following:

- Use of Russian commercial and academic enterprises that interact with the West;
- Recruitment of Russian immigrants with advanced technical skills by the Russian intelligence services; and
- Russian intelligence penetration of public and private enterprises, which enable the government to obtain sensitive technical information from industry.

Russia uses cyber operations as an instrument of intelligence collection to inform its decision-making and benefit its economic interests. Experts contend that Russia needs to enact structural reforms, including economic diversification into sectors such as technology, to achieve the higher rate of gross domestic product growth publicly called for by Russian President Putin. In support of that goal, Russian intelligence services have conducted sophisticated and large-scale hacking operations to collect sensitive U.S. business and technology information. In addition, Moscow uses a range of other intelligence collection operations to steal valuable economic data:

- In 2016, the hacker "Eas7" confided to Western press that she had collaborated with the Russian Federal Security Service (FSB) on economic espionage missions. She estimated that "among the good hackers, at least half works (sic) for government structures," suggesting Moscow employs cyber criminals as a way to make such operations plausibly deniable.
- Moscow has used cyber operations to collect intellectual property data from U.S. energy, healthcare, and technology companies. For example, Russian Government hackers last year compromised dozens of U.S. energy firms, including their operational networks. This activity could be driven by multiple objectives, including collecting intelligence, developing accesses for disruptive purposes, and providing sensitive U.S. intellectual property to Russian companies.
- Since at least 2007, the Russian state-sponsored cyber program APT28 has routinely collected intelligence on defense and geopolitical issues, including those relating to the United States and Western Europe. Obtaining sensitive U.S. defense industry data could provide Moscow with economic (e.g. in foreign military sales) and security advantages as Russia continues to strengthen and modernize its military forces.

Page 2576 of 3957

Recent Unsealed U.S. Indictment with a Link to Russia

In March 2017, the United States Department of Justice indicted two FSB officials and their Russian cybercriminal conspirators on computer hacking and conspiracy charges related to the collection of emails of U.S. and European employees of transportation and financial services firms. The charges included conspiring to engage in economic espionage and theft of trade secrets.

We believe that Russia will continue to conduct aggressive cyber operations during the next year against the United States and its allies as part of a global intelligence collection program focused on furthering its security interests. Although cyber operations are just one element of Russia's multipronged approach to information collection, they give Russia's intelligence services a more agile and cost-efficient tool to accomplish Moscow's objectives. Indeed, Russian cyber actors are continuing to develop their cyber tradecraft—such as using open-source hacking tools that minimize forensic connections to Russia.

Iran: An Increasing Cyber Threat

Iranian cyber activities are often focused on Middle Eastern adversaries, such as Saudi Arabia and Israel; however, in 2017 Iran also targeted U.S. networks. A subset of this Iranian cyber activity aggressively targeted U.S. technologies with high value to the Iranian government. The loss of sensitive information and technologies not only presents a significant threat to U.S. national security. It also enables Tehran to develop advanced technologies to boost domestic economic growth, modernize its military forces, and increase its foreign sales. Examples of recent Iranian cyber activities include the following:

- The Iranian hacker group Rocket Kitten consistently targets U.S. defense firms, likely enabling Tehran to improve its already robust missile and space programs with proprietary and sensitive U.S. military technology.
- Iranian hackers target U.S. aerospace and civil aviation firms by using various website exploitation, spearphishing, credential harvesting, and social engineering techniques.
- The OilRig hacker group, which historically focuses on Saudi Arabia, has increased its targeting of U.S. financial institutions and information technology companies.
- The Iranian hacker group APT33 has targeted energy sector companies as part of Iran's national priorities for improving its petrochemical production and technology.
- Iranian hackers have targeted U.S. academic institutions, stealing valuable intellectual property and data.

Page 2577 of 3957

Recent Unsealed U.S. Indictments with a Link to Iran

In July 2017, Iranian nationals Mohammed Reza Rezakhah and Mohammed Saeed Ajily were charged with hacking into U.S. software companies, stealing their proprietary software, and selling the stolen software to Iranian universities, military and government entities, and other buyers outside of the United States.

In November 2017, Iranian national Behzad Mesri was charged with allegedly hacking HBO's corporate systems, stealing intellectual property and proprietary data, to include scripts and plot summaries for unaired episodes. Mesri had previously hacked computer systems for the Iranian military and has been a member of an Iran-based hacking group called the Turk Black Hat security team.

In March 2018, nine Iranian hackers associated with the Mabna Institute were charged with stealing intellectual property from more than 144 U.S. universities which spent approximately $3.4 billion to procure and access the data. The data was stolen at the behest of Iran's Islamic Revolutionary Guard Corps and used to benefit the government of Iran and other Iranian customers, including Iranian universities. Mabna Institute actors also targeted and compromised 36 U.S. businesses.

We believe that Iran will continue working to penetrate U.S. networks for economic or industrial espionage purposes. Iran's economy—still driven heavily by petroleum revenue—will depend on growth in nonoil industries and we expect Iran will continue to exploit cyberspace to gain advantages in these industries. Iran will remain committed to using its cyber capabilities to attain key economic goals, primarily by continuing to steal intellectual property, in an effort to narrow the science and technology gap between Iran and Western countries.

Page 2578 of 3957

Targeted Technologies

Although many aspects of U.S. economic activity and technology are of potential interest to foreign intelligence collectors, we judge that the highest interest is in the following areas:

Industry	Priority Sectors / Technologies	
Energy / Alternative Energy	• Advanced pressurized water reactor and high-temperature, gas-cooled nuclear power stations • Biofuels • Energy-efficient industries	• Oil, gas, and coalbed methane development, including fracking • Smart grids • Solar energy technology • Wind turbines
Biotechnology	• Advanced medical devices • Biomanufacturing and chemical manufacturing • Biomaterials	• Biopharmaceuticals • Genetically modified organisms • Infectious disease treatment • New vaccines and drugs
Defense Technology	• Aerospace & Aeronautic Systems • Armaments	• Marine Systems • Radar • Optics
Environmental Protection	• Batteries • Energy-efficient appliances • Green building materials	• Hybrid and electric cars • Waste management • Water/air pollution control
High-End Manufacturing	• 3D printing • Advanced robotics • Aircraft engines • Aviation maintenance and service sectors • Civilian aircraft • Electric motors • Foundational manufacturing equipment	• High-end computer numerically controlled machines • High-performance composite materials • High-performance sealing materials • Integrated circuit manufacturing equipment and assembly technology • Space infrastructure and exploration technology • Synthetic rubber
Information and Communications Technology	• Artificial intelligence • Big data analysis • Core electronics industries • E-commerce services • Foundational software products • High-end computer chips • Internet of Things	• Network equipment • Next-generation broadband wireless communications networks • Quantum computing and communications • Rare-earth materials

Page 2579 of 3957

III. Emerging Threats

A range of other potentially disruptive threats warrant attention. Software supply chain infiltration has already threatened the critical infrastructure sector and could threaten other sectors as well. Meanwhile, new foreign laws and increased risks posed by foreign technology companies due to their ties to host governments, may present U.S. companies with previously unforeseen threats.

Cyber threats will continue to evolve with technological advances in the global information environment. The following are emerging areas of concern that are likely to disrupt security procedures and expand the opportunities for collection of sensitive U.S. economic and technology information.

Software Supply Chain Operations

Last year represented a watershed in the reporting of software supply chain operations. In 2017, seven significant events were reported in the public domain compared to only four between 2014 and 2016. As the number of events grows, so too are the potential impacts. Hackers are clearly targeting software supply chains to achieve a range of potential effects to include cyber espionage, organizational disruption, or demonstrable financial impact:

- Floxif infected 2.2 million worldwide CCleaner customers with a backdoor. The hackers specifically targeted 18 companies and infected 40 computers to conduct espionage to gain access to Samsung, Sony, Asus, Intel, VMWare, O2, Singtel, Gauselmann, Dyn, Chunghwa and Fujitsu.

- Hackers corrupted software distributed by the South Korea-based firm Netsarang, which sells enterprise and network management tools. The backdoor enabled downloading of further malware or theft of information from hundreds of companies in energy, financial services, manufacturing, pharmaceuticals, telecommunications, and transportation industries.

- A tweaked version of M.E. Doc was infected with a backdoor to permit the delivery of software from the Ukrainian accounting firm a destructive payload disguised as ransomware. This attack, which was attributed to Russia, paralyzed networks worldwide, shutting down or affecting operations of banks, companies, transportation, and utilities. The cost of this attack to FedEx and Maersk was approximately $300 million each.

- A malware operation dubbed Kingslayer, targeted system administrator accounts associated with U.S. firms to steal credentials in order to breach the system and replace the legitimate application and updates with a malware version containing an embedded backdoor. Although it is not known which and how many firms were ultimately infected, at least one U.S. defense contractor was targeted and compromised.

Foreign Laws Could Enable Intellectual Property Theft

New and enhanced cyber, national security, and import laws in effect in foreign countries are posing an increasing risk to U.S. technology and propriety information. For example, in 2017, China and Russia aggressively enforced laws that bolstered their domestic companies at the expense of U.S. companies and also might allow their companies access to U.S. intellectual property and proprietary information.

In 2017, China put into effect a new cyber security law that restricts sales of foreign information and communication technology (ICT) and mandates that foreign companies submit ICT for government-administered national security reviews. The law also requires that firms operating in China store their data in China, and it requires government approval prior to transferring data outside China. The U.S. Chamber of Commerce has gone on record to explain that if a foreign company is forced to localize a valuable set of data or information in China, whether for research and development purposes or simply to conduct its business, it will have to assume a significant amount of risk. Its data or information may be misappropriated or misused, especially given the environment in China, where companies face significant legal and other uncertainties when they try to protect their data and information.

Required Steps for U.S. Companies to Do Business in China

1. Pass National Security Reviews for Technology and Services
2. Store All Data in China
3. Form Joint Venture to Open Data Center
4. Obtain Government Approval for Data Transfers
5. Buy Government-Approved Encryption and Virtual Private Networks (VPNs)

▶ China has Access to U.S. Intellectual Property and Proprietary Information

Page 2581 of 3957

Similarly, in recent years Russia has dramatically increased its demand for source code reviews for foreign technology being sold inside the country. Russia's Federal Security Service (FSB), associated with economic espionage missions in the past, serves as the authority charged with directing these source code reviews and approving the sale of technology products and services sold inside Russia.

High intelligence threat countries, such as China and Russia, could exploit these laws to significantly improve their access to the intellectual property of foreign companies operating in their countries and subsequently share this sensitive information with domestic firms.

Foreign Technology Companies with Links to Host Governments

Foreign information and communications technology companies are often subject to foreign state influence. This presents a risk to U.S. trade secrets and intellectual property. These companies provide valuable services that often require access to the physical and logical control points of the computers and networks they support. These unique accesses also present an opportunity for foreign countries to obtain sensitive proprietary information. Recent events underscore the potential risks posed by technology companies that have links to foreign governments with high threat intelligence services:

- Recent Chinese laws—including laws on national security and cybersecurity—provide Beijing a legal basis to compel technology companies operating in China to cooperate with Chinese security services.
- In September 2017, the Department of Homeland Security issued a directive to Federal departments and agencies to remove Kaspersky Lab products and services based on the information security risks posed by the company and its links to Russia.
- In December 2017, the Department of Justice made public an agreement with Netcracker Technology Corp. that resulted in the company agreeing that it would not store sensitive information and data from its U.S.-based technology clients in overseas locations, including most notably Russia.

Annex – Decreasing the Prevalence of Economic or Industrial Espionage in Cyberspace

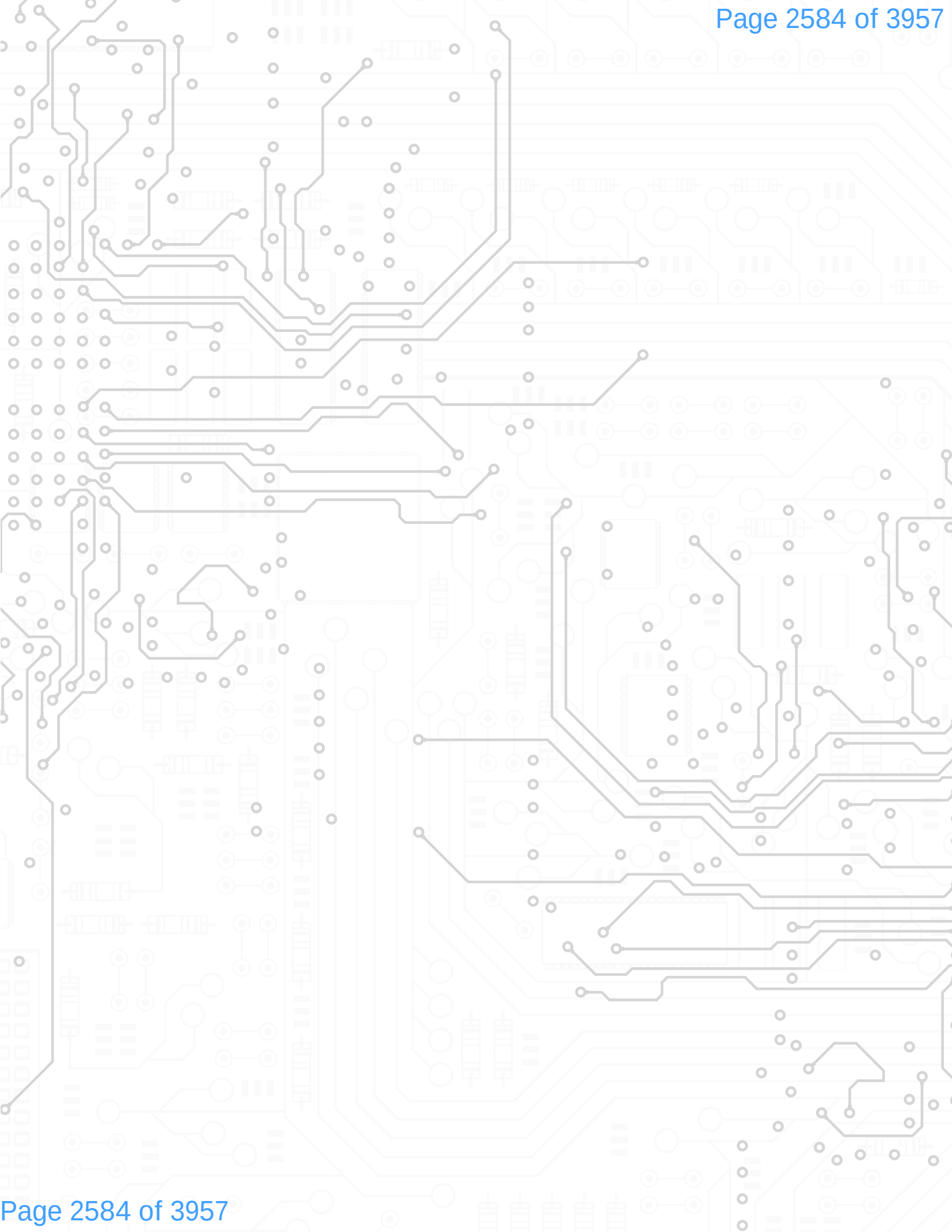
The U.S. Government (USG) continues to undertake numerous actions to counter economic espionage in cyberspace. Perhaps most evident are current USG efforts to protect critical infrastructure and other sensitive computer networks from malicious cyber activities. The USG also continues to work with the private sector to address science and technology gaps through cyber research and development as a way of mitigating the malicious activities of threat actors in cyberspace. The USG will continue to improve its efforts to disrupt, deny, exploit, or increase the costs of foreign cyber operations that are targeting the nation's most critical economic assets.

Examples of USG actions include the following:

- Sharing information about cyber threats, vulnerabilities, and other risks;
- Promoting best practices, risk assessments, and capability development;
- Improving our responses to cyber incidents;
- Building and driving the market towards a more secure cyber ecosystem; and
- Partnering with allies to address cyber issues.

The USG has the capability to impose costs on adversaries who engage in economic cyber espionage through various actions, including diplomatic, informational, military, law enforcement, and economic response. The details of many of these actions are too sensitive to discuss in this publication; however, we have provided a few general examples that illustrate the USG's response, such as:

- Public statements and attribution;
- Diplomatic demarches;
- Economic sanctions; and
- Law enforcement actions.



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Neurosecurity: Human Brain Electro-optical Signals as MASINT

by Dr. Matthew Canham and Dr. Ben D. Sawyer

INTRODUCTION

Applied neuroscience presently allows not only the scientific discovery-oriented probing of the inner workings of the mind, but increasingly the probing of individual minds toward gathering intelligence. Significant advances in neuroimaging, leveraging both active and passive electro-optical energy, can reveal specifics of information held in the mind even without cooperation (e.g., Lange et al., 2018; Sawyer et al., 2016a). The processes of the brain increasingly join many other energetic sources from which quantitative and qualitative data analysis may extract identifying features and other useful intelligence (Sawyer & Canham, 2019). Indeed, it is increasingly appropriate to discuss the human brain as a system which can be read from, written to, and the operations of which may therefore be collected for analysis or influenced (Sawyer & Canham, 2019). Indeed, we argue here that we are witnessing the end of the era in which human thought is generally accepted as an entirely private process, the starting point of an unquestionably remarkable transition. The collection of unintended emissions and byproducts toward intelligence fits well into the mold of Measurement and Signals Intelligence, and indeed Measurement and Signature Intelligence (both MASINT, Macartney, 2001), and so we believe this community within the Intelligence Community is well-suited to discuss these new realities of neurosecurity, as it helped shape many formative discussions surrounding cybersecurity. A MASINT perspective on biological, neural signatures comes with the need to discuss current capabilities, projected technological arc, practicalities, and potential abuses.

While these authors currently have no knowledge of remote monitoring of brain activity, multiple commercial entities are working toward this technology (Strickland, 2017) in various forms. Simultaneously, evidence of remote interference in normal brain functioning is in the news. Most recently, between December 2016 and October 2017, at least 21 employees stationed at the U.S. Embassy in Havana, Cuba, reported experiencing a constellation of symptoms usually associated with a concussion or traumatic brain injury (TBI). Eighteen of these employees reported a sudden onset of symptoms coinciding with an intense chirping or ringing sound similar to the Indies short-tailed cricket. Symptoms reported by employees included difficulty hearing, dizziness, headaches, cognitive difficulties, difficulties with balance, and intense brain pressure (Kirk, 2019). A clinical evaluation by researchers at the University of Pennsylvania found structural differences between exposed employees and healthy controls (Verma et al., 2019). While the clinical implications of this are currently unclear, it seems plausible that these employees were exposed to something that altered their neurological structures and cognitive functioning. The mystery continued to deepen in 2018 when an embassy employee stationed in Guangzhou, China, reported similar symptoms. While we stress that there is still considerable mystery surrounding these events, it does seem likely that these symptoms were (1) induced and (2) likely not the direct goal of whatever process produced the phenomenon. Initial examination of the victims suggests remote microwave energy, long known to affect temporal lobe function (Dyer, 2018). These phenomena provide potential evidence of the intentional targeting of neural architecture, potentially as an attack, potentially as a side effect to some other goal.

Less circumspect evidence also exists. Capability to monitor neural activity exists given direct physical proximity, and remote neural monitoring may be feasible. Recent advances have seen remote detection of other biosignals once considered only measurable from direct physical proximity. For example, NASA's Finding Individuals for Disaster and Emergency Response (FINDER) system uses low-power microwaves to detect heartbeats at great physical range (Liu et al., 2014). Core body temperature is now routinely monitored in crowds to identify individuals with infections (Ng, Kawb, & Chang, 2004). Moreover, two categories of neuroimaging technology are emerging with the promise to make remote brain access a near-term reality. Industry groups like Facebook and Open Water are working to advance near-infrared and holographic techniques for monitoring neural blood flow patterns in real time (Open Water, 2018).

Page 2586 of 3957

Meanwhile, Neuralink, Kernel, and others are working to connect the electrical activity of the brain to intermediary electrodes, and then to the Internet. The success of either of these technologies, neuroimaging at range or Internet-connected electroencephalography, will open a new universe of possibilities for the realms of MASINT, SIGINT, and HUMINT alike.

CURRENT STATE OF THE ART

Before diving into the world of neuroimaging, we offer a brief introduction into what is currently known about how the brain functions. We begin with the neuron, the basic building block of the neural network that is our brain. A basic decision-making system, it takes in input from upstream neurons through receptors known as dendrites and, once a certain threshold of these signals is met, "fires" an action potential which travels down the long synapse to the synaptic gap which separates one neuron from another. Here, chemical signals take over, propagating further action potentials downstream to other neurons in spreading cascades of activity and activation. The process is a foundation for complex patterns of information being aggregated and processed. For example, while the earliest neurons to process visual information might only detect the presence or absence of an edge, neurons further downstream in visual cortex will aggregate the presence of an edge in a specific orientation or relative position and recognize this as the letter "K." Further downstream, neurons will respond more vigorously to the letter "K" when it is placed at the beginning of a word as opposed to the middle or end. In this way, information is aggregated and processed into meaningful coherence.

While there is still debate surrounding the validity of brain area specialization, and growing evidence for "network" approaches to understanding activity, at a coarse level, brain regions appear to be functionally specialized for different activities. Understanding this differential specialization allows for a limited, but growing, degree of reverse engineering of brain processes. A great deal of cognitive processing occurs in the neocortex, the outermost layer of the brain. Here, four "lobes," anatomical brain regions, have been linked by research to functional specializations (see Figure 1, Miller & Cummings, 2017). The occipital lobe, or visual cortex, is where much of visual processing takes place. The parietal lobe handles spatial awareness and somatosensory processes which feed the brain's sense of bodily positioning and stimulation. For example, tickling the hands or feet with a feather would activate somatosensory processing, which would occur primarily in the frontal parietal lobe. The temporal lobe also sits just forward of the occipital lobe and below the parietal lobe, usually just above one's ear. The temporal lobe (aka the auditory cortex) processes sound and often handles long-term memory processing as well. Finally, the frontal lobe is responsible for fine motor functioning, and actions known as executive functions: deliberate decision-making, inhibitory control, attention, and working memory. If you are intensely concentrating on a task, then there is a high likelihood that you are recruiting much of your frontal lobe's prefrontal cortex. This final example is especially significant from a MASINT perspective: it has been suggested that when deliberately trying to deceive someone, the deceiver relies on his/her frontal lobe to a greater degree than does someone who is not attempting to be deceptive (Zeki et al., 2004). There is greater activation in the prefrontal cortex because the individual must inhibit the true version events and must hold two versions active simultaneously (Ofen et al., 2016). Although there is still much debate on the validity of this assertion, as an example it illustrates how neural processing might be utilized in an intelligence-gathering capacity.

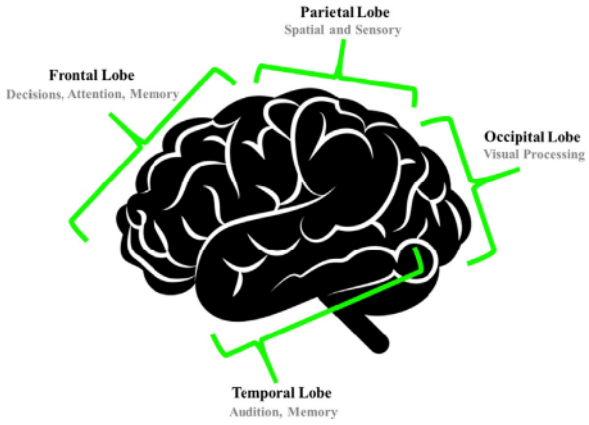


Figure 1: The neocortex or surface of the brain, disproportionately responsible for cognitive processing, is currently conceptualized as divided into functional regions. As with technical and social systems, useful MASINT consideration of these areas is in terms of intelligence and potential influence. Increasingly, it is possible to collect electro-optical energy emitted by the brain and, leveraging temporal and spatial dimensions, decode meaning and so acquire useful intelligence. Influence is also possible, and devices which project electrical force into the brain can disrupt or modify brain processes.

Detectable Signals – A discussion about neuro-imagining should first make the distinction between structural and functional imaging. Structural imaging provides a highly detailed static image of the neuro-

Page 2587 of 3957

anatomical structures of an individual. When the researchers from the University of Pennsylvania examined the embassy employees and found differences in whole brain white matter, this difference was found through the analysis of static structural images (Verma et al., 2019). In contrast, functional imagery tends to be coarser but provides a dynamic series of snapshots that provide insight into the neural activity of an individual. While both techniques have relevance to MASINT applications, functional imaging will be the topic of focus here. Within the universe of functional imaging there are currently two types of signals, blood flow and electrical activity, that are detected to derive neural functioning.

Blood Flow Signals – When neurons are active, these cells consume sugar and oxygen and therefore require replenishment. This replenishment transpires through a process known as hemodynamic response. Termed a blood-oxygen-level-dependent (BOLD) signal, this difference between oxygenated and deoxygenated blood is detectable through various means such as magnetic manipulation or using infrared spectrum light. Examining this signal using magnetism usually involves a technology known as functional Magnetic Resonance Imaging (fMRI). fMRI technology witnessed an upshot in usage within brain research beginning in the early 1990s because it was considerably less intrusive than comparable imaging technologies available at the time. A major drawback in fMRI as a MASINT technique is the need to immobilize a subject and capture imagery over a long time period (from 45 minutes to a few hours), while secured to a table and loaded into a magnetic resonance tube. Movement during imaging is highly detrimental, meaning that only extremely compliant individuals can be imaged. Finally, high tesla (a measurement of magnetism strength) equipment capable of high spatial and temporal resolution imaging is extremely expensive and often requires a dedicated staff, making this technology largely confined to use within a dedicated laboratory. These inconveniences notwithstanding, several researchers have proposed methods of employing fMRI as a means of deception detection (Ganis et al., 2003; Kozel et al., 2005; Monteleone et al., 2009; Ganis et al., 2011). Continuing advances in the miniaturization of this technology suggest this could eventually be an approach moved out of the laboratory and into the field (see, for example, Cooley et al., 2015).

Other emerging techniques such as functional Near Infrared Spectroscopy (fNIRS) offer a window into more near-term workable solutions. Cheap, low-power, and portable, fNIRS utilizes the near infrared spectrum light to detect the BOLD signal. In the 700-900nm spectral range, bodily tissues are mostly transparent, allowing maximal detectability of the relative difference between oxygenated and deoxygenated hemoglobin. fNIRS utilizes a combination of infrared light emitters and receivers to parse out the BOLD signal through differences in infrared light intensity. These differences in light intensity can then be interpreted to detect and localize BOLD signals from specific brain regions to infer localized activity. One of the major advantages of fNIRS over fMRI from a MASINT perspective is the ease of use, and portability of these devices. Indeed, the technology is routinely held up as an excellent match for the demands of brain machine interface and field research (respective reviews are Naseer & Hong, 2015 and Quaresima and Ferrari, 2019). It is currently unclear what the ultimate detectable range using the infrared spectrum will be, but at present these signals are detected using a sensor cap worn by the subject which directly contacts the skin. This portability and ease of use would potentially allow for modern deployment in the debriefing of HUMINT assets by handlers or operational psychologists.

Electrical Activity Signals – While neuroimaging techniques dependent upon blood flow offer high spatial resolution and the capability of localizing neural activity, they lack the capability of detecting activity with a high temporal resolution because there is an inherent lag in the reuptake of oxygenated hemoglobin into active neural regions. This delay means that events which happen very quickly, such as visual recognition, can be missed by techniques reliant on BOLD signal. In these situations, techniques that detect electrical activity offer an advantage over those that detect signals related to blood flow. Electrical detection techniques have very high temporal resolution (on the order of milliseconds), but because electrical fields are distorted by the scalp, they lack the spatial resolution that blood flow-based imaging techniques have. Therefore, researchers often combine these techniques when studying neuro phenomena.

Techniques measuring electrical activity include deep brain electrodes, Electrocorticography (ECoG), and Electroencephalography (EEG), listed from most to least invasive. Brain-contact techniques utilize small probes (approximately 5 im thick) to directly connect to neurons to detect activity (Muthuswamy, 2012), and involve opening the skull to access the cortex. ECoG is somewhat less invasive, involving electrodes that rest upon the dura, a thin sheet of enervated tissue which contains the cerebrospinal fluid and the brain. Non-invasive techniques such as EEG detect voltage potential fluctuations deriving from the action potential activity within the neurons of the brain. Such measured "potentials" can be measured longitudinally over time, or measured relative to specific events, an approach which can identify specific patterns of brain activity known as event-related potentials (ERP). This connection between

Page 2588 of 3957

outside events and brain activity is an excellent strategy to reverse engineer (to a limited degree) the brain activity as it relates to a specific stimulus. One of the most studied ERPs, the "P300" wave, is a distinctive positive fluctuation that occurs approximately 300 milliseconds after visual recognition of a stimulus. The P300 has therefore been proposed as a deception detection technique in "guilty knowledge tests." A subject wearing an EEG would, in such a test, be presented with visual stimuli in succession, and an amplified P300 of what occurred directly after any image recognized, and without the awareness or conscious control of the subject. Many other potentially useful ERPs exist, in the context of MASINT, and include error-related negativity (ERN, see Sawyer et al., 2016b), the P3 (see Rosenfeld et al., 1991), and ERN composite signals such as the multifaceted electroencephalographic response (MERMER, see Farwell & Smith, 2001), to name but a few. Indeed, while the present literature is focused upon individual signatures and their functional meeting, the overarching message here from a MASINT perspective is that electrical signals collected incidentally from brain activity can be used to provide actionable intelligence.

Directing Input into the Brain – Thus far our discussion has centered around reading activity from the brain, but electromagnetic energy can also be effectively used to input information into the brain. A delicate system, the brain can be influenced or disrupted by relatively small amounts of kinetic or electrical energy, and indeed is susceptible to informational patterns (Sawyer et al., 2016a; Sawyer & Hancock, 2018) Transcranial Magnetic Stimulation (TMS) is one such technology, and uses magnetic energy directed toward the neocortex either to excite or to suppress the underlying neural region. For example, an individual who has their visual cortex (occipital lobe, see Figure 1) may experience loss or aberration of vision. TMS has been used for decades in both clinical and research contexts. Recent applications of this technology are striking: for example, a research group at the University of Washington (Jiang et al., 2019) employed TMS as part of an "artificial telepathy" apparatus. In this experiment, two subjects (the senders) watched the orientation of Tetris-like pieces and focused on whether the piece should be rotated to align its placement. A third subject (the receiver), located in a different room and unable to see the pieces, was tasked with deciding whether to rotate the piece. The receiver performed well above chance (~81% accuracy) in deciding whether the piece needed to be rotated, based completely upon the signal he received from the senders. This suggests that beyond collecting actionable intelligence, there are presently ever-increasing opportunities for near engineering, potentially for influence or projecting force.

BRAIN MACHINE INTERFACES INTRODUCE NEW ATTACK SURFACES

Significant progress has been made in recent years in the development of both invasive and non-invasive Brain-Machine Interfaces (BMIs), allowing operators to communicate directly with machinery (computers, robotics, cars, artificial limbs, etc.) using only their thoughts (Roelfsema et al., 2018). A quick patent search reveals that over 3,800 patents were filed for such technology in 2018 (Google Patents, 2019). The intimate connection between the operator's brain and the controlled device opens an entirely new dimension of attack surfaces to be exploited by cyber threat actors. Information security primarily rests upon three pillars: Confidentiality (preventing unauthorized disclosure of information), Integrity (preventing unauthorized modification of information), and Availability (maintaining access to information), the so-called CIA Triangle (Wiley, 2008). Within the context of neuro-security a breach of Confidentiality could potentially allow unprecedented access to an individual's most private data, his/her thoughts. A breach of Integrity would mean that an attacker could inject commands into a neuro-device, or alternatively send false feedback to the brain from the device. A failure of Availability would prevent a user from being able to control the device or receive data from it. The failures of any of these pillars might seem to be purely within the realm of science fiction; however, proof of concept attacks have already been demonstrated for each.

Reaching into the uncooperative individual's mind to retrieve, or influence, information is increasingly a reality. Lange et al. (2018) were able to recover partial Personal Identification Numbers (PINs) from subjects' EEG (electroencephalogram) signal. Other research (Roelfsema et al., 2018) has demonstrated the ability to infer the words or concepts that an individual is thinking of, from EEG signals. Without the proper security, individuals using BMIs relying on similar signal processing would be subject to having their private thoughts exposed. Perhaps more disconcerting than breaching Confidentiality is a breach of Integrity; such a breach was demonstrated by Cusack et al., 2017 in a highly controlled environment. In this study, researchers conducted a Man-In-The-Middle attack against a BMI and a toy car and were able to intercept thought-based commands from the user's BMI and inject modified commands. In this case they substituted the command "turn left" with "turn right." If such an attack were launched against an artificial limb or a wheelchair (both of which can now be controlled with similar technology), an attacker could easily cause death or serious physical injury either the user or those around them. In a similar vein, Cusack et al. (2017) describe a simple modification to their integrity-focused attack of flooding the BMI connection with meaningless packets to disrupt the control channel and thereby deny the operator

Page 2589 of 3957

access to the controlled device. This type of attack, properly timed, could lead to equally destructive results if the downstream device is the artificial limb or wheelchair mentioned above.

FUTURE DIRECTIONS AND NEUROSECURITY CONCERNS

The current state of the art in neuroimaging requires that sensors be placed in very close proximity to a subject's cranium, a state of affairs that many other energetic MASINT sources once shared. Could technology be someday (or presently) capable of detecting neural signals from a distance? While the signal detection difficulties of such a system are great, it is within the realm of possibility. Even such a technology with very limited range would have serious implications for the Intelligence Community, and open the door to covert neuro-surveillance. A few inches might allow an apparatus to be embedded in surfaces, such as seating. A few meters would allow for neuro-surveillance of an interview at a border crossing. More range comes with more interesting, and concerning, implications.

What about individuals who choose to use technology to project their neural information outward? Neuralink, and other industry actors, have this possibility as a direct piece of their value proposition. The idea of computer network-connected brains mirrors that of other computer network-connected sensors: surveillance becomes implicit in return for convenience. Indeed, it may be useful to consider the fact that surveillance capabilities of a covert microphone and a present generation household smart speaker are functionally very little. Covert or overt monitoring of neural activity holds many parallel possibilities, and Biafra mentioned remote neuroimaging is joined by technologies which will intentionally transmit neural information over the Internet, or other networks. It is extremely likely that industry and state actors, in the absence of legislative restraint, will find reason and avenues to collect and leverage such data. The rights of individuals to their own personal neural information, when transported through computer networks, is likely in the process of being decided presently by society and the courts, as rights to personal electronic information are a likely precedent.

Input, as discussed above, is another fascinating dimension of networked neural implants. The ideas are not radical, and indeed Apple and Nucleus, manufacturer of cochlear implants, recently made iOS the operating system connecting to more human implants than any other. These technologies join other apps which can be used to connect to a variety of human implants. In cochlear implants, for example, the intended mode of input is digital audio signals: it is better to listen to your phone call when beamed directly to your implant them through a microphone facing the phone speaker. However, these devices offer opportunities for MASINT, and for influence. Indeed, just as personal information and computer networks can be used for both surveillance and influence, it may be possible to manipulate overtly or covertly a target through an active neural, sensory nerves, or peripheral nervous system connection.

Consider a concerted effort to expose a subject to positive or negative stimulation in response to specific actions. Such a campaign would certainly result in some level of conditioning. We can, for example, imagine creating incentives not to enter a geo-fenced location, or not to leave one. Threat actors with the goal of rendering a target ineffective in their current occupation might leverage a cochlear implant to arrange for painful, annoying, disturbing, or other negative stimulus to be inflicted whenever the target entered their office. They could also simply degrade the quality of the function of the device. Because cochlear implants connect to the Internet through iPhones, this could be accomplished through the malicious employment of code. Note that such an attack would leverage intelligence about use location from the phone, and use the same phone to send negative stimuli to the target through the cochlear implants. Of course, cochlear implants in the United States presently all have removable external units, and could simply be removed. Submitting to deafness in order to remove the stimuli a denial in its own right, it is worth considering that such a scheme would work on other implants, each with its own uncomfortable set of possibilities.

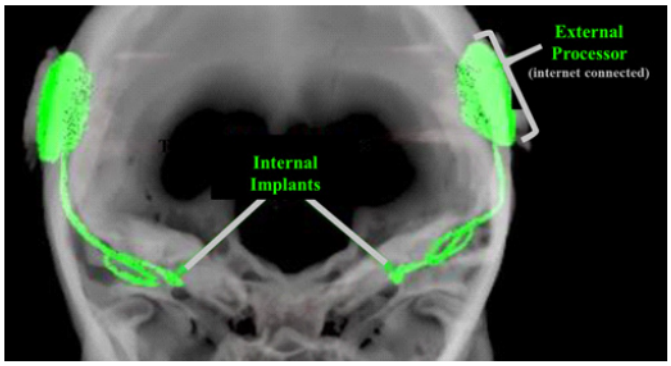


Figure 2: Modern cochlear implants are now compatible with Apple's iOS, which has therefore become a new and widely available attack surface for individuals with this type of sensory nerve-connected prosthesis. Neurosecurity questions exist regarding which central, sensory, or peripheral nervous system-connected devices will soon also be Internet-connected, and whether these have input or output capabilities.

The implications of direct and potential remote neuroimaging are, course, not limited to intelligence, nor to influence, nor to negative outcomes. Neuroimaging, especially remotely,

Page 2590 of 3957

might prove a particularly robust new form of biometrics, through the recording of an individual's neural responses to specific stimuli, using amenable ERPs, for example. The possibilities for industry, health, and human computer interface are monumental. Interpersonal communication might be revolutionized, or at least improved. However, we believe that this hopeful narrative must be tempered with understanding of the implications to individual and aggregate security. Major questions exist, and at present there are no answers.

OPEN QUESTIONS AND CONCERNS SURROUNDING NEUROIMAGING AS A MASINT SOURCE

In sum, applied neuroscience techniques previously reserved for experts probing scientific questions are now increasingly amenable to MASINT. There are presently multiple scenarios in which intelligence can be gathered through passive monitoring of the electro-optical signals concurrent with brain activity (blood flow and neural discharge patterns), and in the near future such access may become available at greater physical distance. These opportunities are joined by rapid advancements in understanding of the functional organization and temporal signaling of the brain, coupled with rapid advancement in occupational power and machine learning technique quite familiar to the MASINT community. The result is the beginning of an era in which neural information, and the machinations of the human brain, are joining many other systems previously made amenable to MASINT information-gathering approaches. Indeed, the impacts of these combined advances are undoubtedly fueling scattered conversation and innovation in the public and classified spheres of many countries. While some outcomes will be undeniably positive, we feel that there are strong signs that a more focused conversation needs to be held.

Recently, several U.S. embassy workers stationed at Guangzhou, China, have reported symptoms like those reported by U.S. embassy workers stationed in Cuba. Again, there is much controversy surrounding these reports. One widely held assumption is that these are in fact the result of some type of "neuro-attack." Perplexing problems now arise. How could such an attack be detected? Every time your brain forms a new memory (which happens constantly), your brain changes in subtle and poorly understood ways. This constant change makes baselining incredibly challenging, and there remains some question as to whether this is even possible. Moreover, it seems likely that an "input"-based technology, as may be the cause, would be infinitely more detectable than a technology monitoring output. It seems evident that neuroimaging technology holds great potential for MASINT, and for this reason alone there is the likelihood that state-sponsored intelligence services will attempt to employ this technology as an intelligence-gathering technique. The high likelihood of this experimentation, and the relatively feasible nature of creating such a technology, should compel more research to be conducted on a variety of related neurosecurity topics.

It seems evident that neuroimaging technology holds great potential for MASINT, and for this reason alone there is the likelihood that state-sponsored intelligence services will attempt to employ this technology as an intelligence-gathering technique.

Beyond the fundamental question of whether neural tissue is amenable to gathering intelligence, or a likely target for projecting force, fundamental forensic questions which should be addressed by such a line of research are as follows:

How do we ensure neurosecurity? Just as cybersecurity was once poorly understood, so now is neurosecurity. We must understand which approaches are real threats, what their limitations are, and develop understanding as to how our own state, industry, and greater public population can be protected. We must also begin a dialogue in scientific, legislative, and public spheres to address how best to integrate these coming realities into our society. How do we safeguard freedom and security when the information between our ears is no longer inherently our own?

How do we detect attacks? In terms of information-gathering attacks, neurosecurity is likely to suffer from many of the same challenges as cybersecurity; by definition, a well-executed attack need leave no trace (see Hancock, Hancock & Sawyer, 2015). In terms of influence, the more difficult question is one of trust. What is possible in terms of influence, and how can we detect it? Indeed, this is the challenge of cyber-compromised computer systems which serve new masters, or have their cycles turned toward threat actor goals. How do we know when an individual has been attacked? One of the greatest challenges in the "Havana Syndrome" has been establishing whether something in fact occurred. Subjectively, patient reports align very closely (sudden onset, hearing a high-pitched chirping or ringing, difficulty concentrating and maintaining balance), but there is thus far no way to establish exposure conclusively.

Is it possible to develop a baseline? In cybersecurity, understanding of the original state of the system is vital for understanding whether an intrusion has occurred, and how the system is compromised. If a method for detecting a

Page 2591 of 3957

neuroattack is developed, it will likely involve establishing an analogous neural baselining. The clinical evaluation of Havana Syndrome victims by researchers at the University of Pennsylvania found structural differences between exposed employees and healthy controls. Specifically, structural imaging indicated significantly decreased levels of whole brain white matter, differences in regional gray and white matter volumes, cerebellar microstructural integrity, and functional connectivity in the visuospatial and auditory subnetworks (Verma et al., 2019). While this study found differences between the exposed population and healthy controls, it was unable to demonstrate differences within patients before and after the time of exposure because there was no baseline created prior to their deployment. Another limitation of this study was that it focused on the structural aspects of the patients' neural architectures, but not their cognitive functioning. Baselining to detect a neuro-attack will likely necessitate a cognitive functioning component, perhaps involving rapid response to various stimuli. Developing a baseline of cognitive functioning will likely utilize neuroimaging, for example EEG to measure patient responses to stimuli over time. One of the greatest challenges to this will be understanding whether such baselining is even possible. The brain is incredibly plastic and changes constantly. In fact, every new memory formed causes changes within the brain. An unanswered question is what does "normal" change look like compared to "abnormal" change, and can these differences be detected? If they can be detected, is EEG the right technique, and are EEG responses to stimuli consistent over time? The few answers that presently exist come from vastly different domains in the neurosecurity threat to come.

CONCLUSION: TOWARD A MASINT UNDERSTANDING OF THE BRAIN

MASINT has existed for long enough that the community has witnessed many energetic signals moving from non-useful to pivotal. We here predict that the energetic emissions of the human brain will follow that pattern. Understanding the time frame of that change is difficult. It may take the entirety of our coming careers. It may have already happened. The cause of the Havana Syndrome remains a mystery at the time of this writing. It is also unclear whether Havana Syndrome is specifically the result of a neuro-weapon, or something entirely different. It does, however, provide the opportunity for a timely thought experiment, as the world will witness the effects of neuro-weapons in the foreseeable future. It is critical that tools and techniques be developed to detect the effects of these weapons, and to guard against them. We believe that the framework of MASINT, and the broader Intelligence Community which has such implicit interest in these ongoing developments, is an excellent place to begin this critical work.

References

Cooley, C. Z., Stockmann, J. P., Armstrong, B. D., Sarracanie, M., Lev, M. H., Rosen, M. S., & Wald, L. L. (2015). Two dimensional imaging in a lightweight portable MRI scanner without gradient coils. *Magnetic Resonance in Medicine*, *73*(2), 872-883.

Cusack, B., Sundararajan, K., & Khaleghparast, R. (2017). Neurosecurity for brainware devices.

Dyer, O. (2018). Microwave weapon caused syndrome in diplomats in Cuba, US medical team believes. *Bmj*, 362, k3848-k3848.

Farwell, L. A., & Smith, S. S. (2001). Using brain MERMER testing to detect knowledge despite efforts to conceal. *Journal of Forensic Science*, 46(1), 135-143.

Ganis, G., Kosslyn, S. M., Stose, S., Thompson, W. L., & Yurgelun-Todd, D. A. (2003). Neural correlates of different types of deception: An fMRI investigation. Cerebral cortex, 13(8), 830-836.

Ganis, G., Rosenfeld, J. P., Meixner, J., Kievit, R. A., & Schendan, H. E. (2011). Lying in the scanner: covert countermeasures disrupt deception detection by functional magnetic resonance imaging. *Neuroimage*, 55(1), 312-319.

Google Patents, (2019). Retrieved from https://patents.google.com.

Hancock, P. A., Hancock, G. and Sawyer, B. D., 2015, Cybernomics and the implications of cyber-deception. *The Ergonomist*, 537, 12-14.

Jiang, L., Stocco, A., Losey, D. M., Abernethy, J. A., Prat, C. S., & Rao, R. P. (2019). BrainNet: a multi-person brain-to-brain interface for direct collaboration between brains. *Scientific Reports*, 9(1), 6115.

Kozel, F. A., Johnson, K. A., Mu, Q., Grenesko, E. L., Laken, S. J., & George, M. S. (2005). Detecting deception using functional magnetic resonance imaging. *Biological Psychiatry*, 58(8), 605-613.

Lange, J., Massart, C., Mouraux, A., & Standaert, F. X. (2018). Side-channel attacks against the human brain: The PIN code case study (extended version). *Brain Informatics*, 5(2), 12.

Liu, L., Liu, Z., Xie, H., Barrowes, B., & Bagtzoglou, A. C. (2014). Numerical simulation of UWB impulse radar vital sign detection at an earthquake disaster site. *Ad Hoc Networks*, 13, 34-41.

Macartney, J. D. (2001). John, how should we explain MASINT? *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, 170-171.

Miller, B. L., & Cummings, J. L. (eds.). (2017). *The human frontal lobes: Functions and disorders*. Guilford Publications.

Page 2592 of 3957

Monteleone, G. T., Phan, K. L., Nusbaum, H. C., Fitzgerald, D., Irick, J. S., Fienberg, S. E., & Cacioppo, J. T. (2009). Detection of deception using fMRI: better than chance, but well below perfection. *Social Neuroscience*, 4(6), 528-538.

Muthuswamy, J., Sridharan, A., & Okandan, M. (2016). MEMS Neural Probes. *Encyclopedia of Nanotechnology*, 1993-2009.

Naseer, N., & Hong, K. S. (2015). fNIRS-based brain-computer interfaces: a review. *Frontiers in Human Neuroscience*, 9, 3.

Ng, E. Y., Kawb, G. J. L., & Chang, W. M. (2004). Analysis of IR thermal imager for mass blind fever screening. *Microvascular Research*, 68(2), 104-109.

Ofen, N., Whitfield-Gabrieli, S., Chai, X. J., Schwarzlose, R. F., & Gabrieli, J. D. (2016). Neural correlates of deception: Lying about past events and personal beliefs. Social cognitive and affective neuroscience, 12(1), 116-127.

Open Water (2018). At https://www.openwater.cc/technology.

Poulsen K. (29 March 2008). Hackers assault epilepsy patients via computer. Retrieved 23 September 2019 from https://www.wired.com/2008/03/hackers-assault-epilepsy-patients-via-computer/.

Quaresima, V., & Ferrari, M. (2019). Functional near-infrared spectroscopy (fNIRS) for assessing cerebral cortex function during human behavior in natural/social situations: a concise review. *Organizational Research Methods*, 22(1), 46-68.

Roelfsema, P. R., Denys, D., & Klink, P. C. (2018). Mind reading and writing: the future of neurotechnology. *Trends in cognitive sciences*.

Rosenfeld, J. P., Angell, A., Johnson, M., & Qian, J. H. (1991). An ERP based, control question lie detector analog: Algorithms for discriminating effects within individuals' average waveforms. *Psychophysiology*, 28(3), 319-335.

Sawyer, B. D., & Canham, M., (2019) Neurosecurity: Infosec meets Brain-machine Interface. *B-Sides Las Vegas 2019*. Video at https://t.co/dGIJD9UIH4?amp=1.

Sawyer, B. D., Finomore, V. S., Funke, G., Warm, J. S., Matthews, G and Hancock, P. A., 2016a, Cyber vigilance: The human factor. *American Intelligence Journal*, 32(2), 157-165.

Sawyer, B. D., Karwowski, W., Xanthopoulos, P. and Hancock, P. A., (2016b), Detection of error-related negativity in complex visual stimuli: A new neuroergonomic arrow in the practitioner's quiver. *Ergonomics*, 1-7.

Strickland, E. (2017). Silicon valley's latest craze: Brain tech [News]. *IEEE Spectrum*, 54(7), 8-9.

Tosini, G., Ferguson, I., & Tsubota, K. (2016). Effects of blue light on the circadian system and eye physiology. *Molecular Vision*, 22, 61-68.

Wiley, J. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd edition, 239-274.

Yazdani, P. (2017). *Assessing seizure susceptibility using visual psychophysical tests* (doctoral dissertation, Newcastle University).

Dr. Matthew Canham, a psychologist and neuroscientist, is Research Professor of Cybersecurity for the Institute of Simulation and Training at the University of Central Florida in Orlando. His PhD degree in Cognition, Perception, and Cognitive Neuroscience is from the University of California, Santa Barbara. His research focuses on the human aspects of privacy and cybersecurity. Previously, Dr. Canham was a Supervisory Special Agent with the FBI, where he served in the field performing investigations of cyber-breaches, intellectual property theft, and other federal violations. Later, as manager of the Emerging Technologies Program with the Operational Technology Division based in Quantico, VA, he co-authored the FBI briefing for the incoming U.S. Presidential Cabinet on "Technology Based Threats to Law Enforcement in the 21st Century" and provided subject matter expertise to the FBI's Cyber Behavioral Analysis.

Dr. Ben D. Sawyer is Assistant Professor within Industrial Engineering and Management Systems at the University of Central Florida, and Director of the Laboratory for Autonomy-Brain Exchange (LabX). His PhD degree in Applied Experimental Psychology and MS in Industrial Engineering are from the University of Central Florida. At the Massachusetts Institute of Technology, he leveraged biosignals, big data, and machine learning to engineer models of human performance and behavior for the use of machine counterparts. At the Air Force Research Laboratory 711th Human Performance Wing's Applied Neuroscience and BATMAN Divisions, he built mathematical models of human performance for special operations, including cyber operations. His present research, and laboratory, seek to accelerate information transfer between human and autonomy. Dr. Sawyer's design recommendations are leveraged by Fortune 500 companies. His work has been covered by Forbes, *Reuters, Fast Company, and the BBC, and published in leading scientific journals.*

Page 2593 of 3957

An official website of the United States government Here's how you know

PRESS RELEASE

Former U.S. Military Pilot Admits Acting as Paid Agent of China and Lying on National Security Background Forms

Thursday, June 23, 2022

Share

For Immediate Release
Office of Public Affairs

A former U.S. Army helicopter pilot-turned-civilian-contractor pleaded guilty in federal court today, admitting that he acted as an unregistered agent of China and accepted thousands of dollars from representatives of the Chinese government to provide aviation-related information from his defense-contractor employers. He also pleaded guilty to making related false statements during national security background checks.

Shapour Moinian, 67, of San Diego, served in the Army in the United States, Germany, and South Korea from approximately 1977 through 2000. After his service, Moinian worked for various cleared defense contractors in the United States – including in San Diego – as well as the Department of Defense. "Cleared" is a term that indicates a contractor is permitted to work on projects that involve classified information.

According to his plea agreement, while Moinian was working for a cleared defense contractor, or CDC, on various aviation projects used by the U.S. military and U.S. intelligence agencies, he was contacted by an individual in China who claimed to be working for a technical recruiting company. This person offered Moinian the opportunity to consult for the aviation industry in China.

"Moinian was a paid agent of the Chinese government who sold American aviation-related technology," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "The Department of Justice has no tolerance for those who help foreign governments break the law to undermine American competitiveness and innovation."

"This defendant took the aviation materials of his American employers and sold them to China," said U.S. Attorney Randy Grossman for the Southern District of California. "This conduct was an outrageous breach of trust by a former member of the U.S. military. The United States will aggressively investigate and prosecute anyone who works at the direction of foreign governments to steal American technology and intellectual property."

"The People's Republic of China remains determined to acquire our information and technology. In this case, we witnessed a former U.S. Government employee acting as an agent of the government of China and Chinese intelligence officers' extensive use of social media to identify willing targets," said Assistant Director Alan E. Kohler Jr. of the FBI's of the Counterintelligence Division. "The FBI is committed not only to leveraging risk and consequences upon the defendant, but also to confronting the behavior and policies of the Chinese government that threaten our national security and freedom."

"The defendant admitted to being an unregistered agent of a foreign power, lying on his background check paperwork to obtain his security clearance, knowingly providing proprietary information to people controlled by the Chinese government, and willingly receiving payments from them. This is another example of how the Chinese government enhances its defense capabilities through the illicit exploitation of U.S. technology," said Special Agent in Charge Stacey Moy of the FBI's San Diego Field Office. "When someone holds a security clearance, they know what information should be reported to security officials. In this case, the defendant betrayed his sacred oath, knew his actions were wrong, and subsequently lied about it. The FBI and our partners on the Counterintelligence Task Force will pursue anyone who abuses their placement and access to obtain proprietary information on behalf of a foreign government. I specifically want to thank the Naval Criminal Investigative Service (NCIS) for their continued partnership on this case."

"Mr. Moinian sold information to the Chinese government, and lied repeatedly to cover up his crimes," said Special Agent in Charge Michelle Kramer of the NCIS Office of Special Projects. "Now he is being held to account for his actions. NCIS and our partners remain unwavering in our commitment to protecting the U.S. military and rooting out criminality that threatens the superiority of the U.S. warfighter."

In March of 2017, Moinian travelled to Hong Kong where he met with this purported recruiter and agreed to provide information and materials related to multiple types of aircraft designed and/or manufactured in the United States in exchange for money. Moinian accepted approximately $7,000-$10,000 in United States currency during that meeting. According to his plea agreement, at this meeting and at all subsequent meetings, Moinian knew that these individuals were employed by or directed by the government of the People's Republic of China.

Upon returning to the United States, Moinian began gathering aviation-related materials, which included transferring material from a CDC to a thumb drive. In September 2017, the defendant traveled overseas and, during a stopover at the Shanghai airport, met with Chinese government officials and provided aviation-related materials on a thumb drive, including proprietary information from a CDC. Thereafter, Moinian arranged for payment for this information through the South Korean bank account of his stepdaughter. Moinian told his stepdaughter that these funds were payment for his consulting work overseas and instructed her to transfer the funds to him in multiple transactions.

Moinian also received a cell phone and other equipment from these individuals to communicate with them and aid in the electronic transfer of materials and information.

At the end of March 2018, Moinian traveled to Bali and met with these same individuals again. Later that year, he began working at another CDC. During this timeframe, the same individuals in China transferred thousands of dollars into the South Korean bank account of Moinian's stepdaughter, who subsequently wired the funds to Moinian in multiple transactions.

In August 2019, Moinian traveled again to Hong Kong and met with these same individuals where he was again paid approximately $22,000 in cash for his services. Moinian and his wife smuggled this cash back into the United States.

According to his plea agreement, Moinian also admitted that he lied on his government background questionnaires in July 2017 and March 2020, when he falsely stated that did not have any close or continuing contacts with foreign nationals and that no foreign national had offered him a job.

At sentencing, Moinian faces a maximum penalty of 10 years in prison and fine up to $250,000 for acting as an agent of a foreign government, and up to five years and a $250,000 fine for the false statements count. Sentencing is scheduled for Aug. 29.

This case was investigated by the FBI and the NCIS and is being prosecuted by the U.S. Attorney's Office for the Southern District of California and the Department of Justice's National Security Division.

Updated June 23, 2022

Topics

COUNTERINTELLIGENCE | NATIONAL SECURITY

Components

Federal Bureau of Investigation (FBI) | National Security Division (NSD) | USAO - California, Southern

Press Release Number: 22-660

Related Content

PRESS RELEASE

Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea

The Justice Department unsealed charges, seizures, and other court-authorized actions to disrupt the illicit revenue generation efforts of the Democratic People's Republic of Korea (DPRK or North Korea).

May 16, 2024

PRESS RELEASE

Justice Department Announces Arrest, Premises Search, and Seizures of Multiple Website Domains to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea

The Justice Department today announced a series of coordinated and court-authorized actions to disrupt the illicit revenue generation efforts of Democratic People's Republic of Korea (DPRK) information technology (IT) workers.

May 16, 2024

PRESS RELEASE

Maryland Woman Pleads Guilty to Conspiring to Destroy the Baltimore Region Power Grid

Sarah Beth Clendaniel, 36, of Catonsville, Maryland, pleaded guilty today to conspiring to damage or destroy electrical facilities in Maryland.

May 14, 2024

Office of Public Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Office of Public Affairs Direct Line
202-514-2007

Department of Justice Main Switchboard
202-514-2000

Signup for Email Updates
Social Media

Page 2594 of 3957

News

All News
Blogs
Photo Galleries
Podcasts
Press Releases
Speeches
Videos

Archived News

Para Noticias en Español

PRESS RELEASE

Maryland Nuclear Engineer and Wife Sentenced for Espionage-Related Offenses

Wednesday, November 9, 2022

Share

For Immediate Release
Office of Public Affairs

A Maryland man and his wife were sentenced today for conspiracy to communicate Restricted Data related to the design of nuclear-powered warships.

Jonathan Toebbe, 44, of Annapolis, was sentenced today to 232 months, over 19 years, of incarceration. His wife, Diana Toebbe, 46, was sentenced to 262 months, more than 21 years, of incarceration. The Toebbes pleaded guilty to the conspiracy in August 2022.

"The Toebbes conspired to sell restricted defense information that would place the lives of our men and women in uniform and the security of the United States at risk," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "The Department of Justice remains committed to protecting U.S. defense technology."

"If not for the remarkable efforts of FBI agents, the sensitive data stolen by Mr. Toebbe could have ended up in the hands of an adversary of the United States and put the safety of our military and our nation at risk," said U.S. Attorney William J. Ihlenfeld II for the Northern District of West Virginia. "The FBI keeps American citizens safe from enemies both foreign and domestic and this case is an excellent reminder of their important work."

"These actions are a betrayal of trust, not only to the U.S. Government, but also to the American people," said Assistant Director Alan E. Kohler Jr. of the FBI's Counterintelligence Division. "All U.S. Government employees swear to support and defend the Constitution of the United States, and with that oath comes the obligation to protect sensitive information. Those entrusted with such grave responsibility must be held accountable if they violate their oath and betray their country. The investigation which led to today's sentencing is a reminder that the FBI and our partners will continue to doggedly pursue those who betray their sworn oath and those who aid them."

"The Toebbes were willing to compromise the security of the nation by selling information related to naval nuclear propulsion systems, they are now being held accountable for their actions," said Special Agent in Charge Mike Nordwall of the FBI Pittsburgh Field Office. "The FBI and our federal partners have an unwavering commitment to protect U.S. secrets and will continue to aggressively investigate and expose espionage activities conducted on U.S. soil."

"Naval nuclear engineer Jonathan Toebbe was entrusted with our nation's critical secrets and, along with his wife Diana Toebbe, put the security of our country at risk for financial gain," said U.S. Attorney Cindy Chung for the Western District of Pennsylvania. "Their serious criminal conduct betrayed and endangered the Department of the Navy's loyal and selfless service members. The seriousness of the offense in this case cannot be overstated."

"The Toebbes betrayed the American people and put our national security at significant risk when they selfishly attempted to sell highly sensitive information related to nuclear-powered warships for their own financial benefit," said Special Agent in Charge Brice Miller of the Naval Criminal Investigative Service (NCIS) Office of Special Projects. "As the law enforcement arm of the Department of the Navy responsible for preventing terrorism, reducing crime, and protecting secrets, NCIS remains committed to protecting vital information and technology that ensures the superiority of the U.S. Navy and Marine Corps."

According to court documents, at the time of his arrest, Jonathan Toebbe was an employee of the Department of the Navy who served as a nuclear engineer and was assigned to the Naval Nuclear Propulsion Program, also known as Naval Reactors. He held an active national security clearance through the Department of Defense, giving him access to "Restricted Data" within the meaning of the Atomic Energy Act. Restricted Data concerns design, manufacture or utilization of atomic weapons, or production of Special Nuclear Material (SNM), or use of SNM in the production of energy – such as naval reactors. Jonathan Toebbe worked with and had access to information concerning naval nuclear propulsion including information related to military sensitive design elements, operating parameters and performance characteristics of the reactors for nuclear powered warships.

According to court documents, Jonathan Toebbe sent a package to a foreign government, listing a return address in Pittsburgh, Pennsylvania, containing a sample of Restricted Data and instructions for establishing a covert relationship to purchase additional Restricted Data. Jonathan Toebbe began corresponding via encrypted email with an individual whom he believed to be a representative of the foreign government. The individual was really an undercover FBI agent. Jonathan Toebbe continued this correspondence for several months, which led to an agreement to sell Restricted Data in exchange for thousands of dollars in cryptocurrency.

On June 8, 2021, the undercover agent sent $10,000 in cryptocurrency to Jonathan Toebbe as "good faith" payment. Shortly afterwards, on June 26, Jonathan Toebbe serviced a dead drop by placing an SD card, which was concealed within half a peanut butter sandwich and contained military sensitive design elements relating to submarine nuclear reactors, at a pre-arranged location. After retrieving the SD card, the undercover agent sent Jonathan Toebbe a $20,000 cryptocurrency payment. In return, Jonathan Toebbe emailed the undercover agent a decryption key for the SD Card. A review of the SD card revealed that it contained Restricted Data related to submarine nuclear reactors. On Aug. 28, 2021, Jonathan Toebbe made another "dead drop" of an SD card in eastern Virginia, this time concealing the card in a chewing gum package. After making a payment to Jonathan Toebbe of $70,000 in cryptocurrency, the FBI received a decryption key for the card. It, too, contained Restricted Data related to submarine nuclear reactors. The FBI arrested Jonathan Toebbe and his wife on Oct. 9, 2021 after he placed yet another SD card at a pre-arranged "dead drop" at a second location in West Virginia.

The FBI and NCIS are investigating the case.

Trial Attorneys Matthew J. McKenzie and S. Derek Shugert of the National Security Division's Counterintelligence and Export Control Section, Assistant U.S. Attorneys Jarod J. Douglas and Lara Omps-Botteicher for the Northern District of West Virginia and Special Assistant U.S. Attorney Jessica Lieber Smolar for the Western District of Pennsylvania prosecuted the case.

Updated November 9, 2022

Topics

COUNTERINTELLIGENCE | NATIONAL SECURITY

Components

Federal Bureau of Investigation (FBI) | National Security Division (NSD) | USAO - West Virginia, Northern

Press Release Number: 22-1207

Related Content

PRESS RELEASE

Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea

The Justice Department unsealed charges, seizures, and other court-authorized actions to disrupt the illicit revenue generation efforts of the Democratic People's Republic of Korea (DPRK or North Korea).

May 16, 2024

PRESS RELEASE

Justice Department Announces Arrest, Premises Search, and Seizures of Multiple Website Domains to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea

The Justice Department today announced a series of coordinated and court-authorized actions to disrupt the illicit revenue generation efforts of Democratic People's Republic of Korea (DPRK) information technology (IT) workers.

May 16, 2024

PRESS RELEASE

Maryland Woman Pleads Guilty to Conspiring to Destroy the Baltimore Region Power Grid

Sarah Beth Clendaniel, 36, of Catonsville, Maryland, pleaded guilty today to conspiring to damage or destroy electrical facilities in Maryland.

May 14, 2024

Office of Public Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Office of Public Affairs Direct Line
202-514-2007

Department of Justice Main Switchboard
202-514-2000

Signup for Email Updates
Social Media

News

All News
Blogs
Photo Galleries
Podcasts
Press Releases
Speeches
Videos

Archived News

Para Noticias en Español

PRESS RELEASE

U.S. Government Contractor Arrested on Espionage Charges

Thursday, September 21, 2023

Share

For Immediate Release
Office of Public Affairs

IT Help Desk Technician Charged with Transferring Classified Materials to a Foreign Government

A U.S. government contractor was arrested on Aug. 24 based on espionage charges in a complaint unsealed today. Abraham Teklu Lemma, 50, a naturalized U.S. citizen of Ethiopian descent, of Silver Spring, Maryland, is charged with delivering national defense information to aid a foreign government, conspiracy to deliver national defense information to aid a foreign government, and the willful retention of national defense information.

According to the criminal complaint, between on or about Dec. 19, 2022, and Aug. 7, 2023, Lemma copied classified information from intelligence reports and deleted the classification markings from them. Lemma then removed the information, which was classified as SECRET and TOP SECRET, from secure facilities at the Department of State. This material related to a specific country and/or geographic region. Lemma accessed, copied, removed, and retained this information without authorization.

According to the charging documents, Lemma used an encrypted application to transmit classified national defense information to a foreign government official associated with a foreign country's intelligence service. In these communications, Lemma expressed an interest and willingness to assist the foreign government official by providing information. In one communication, the foreign official stated, "[i]t's time to continue ur support." Lemma responded, "Roger that!" In other chats, the foreign official tasked Lemma to focus on information related to particular subjects, and Lemma responded "[a]bsolutely, I have been focusing on that all this week . . . ." As alleged in the criminal complaint, the classified national defense information Lemma transferred to the foreign official included satellite imagery and other information regarding military activities in the foreign country and region.

The two espionage charges carry a potential penalty of death or any term of years up to life in prison, and the willful retention charge carries a maximum penalty of 10 years in prison. A federal judge will determine any sentence based on the U.S. Sentencing Guidelines and other statutory factors.

The FBI's Washington Field Office, the State Department's Diplomatic Security Service, and the Justice Department's Office of the Inspector General are investigating the case.

Assistant U.S. Attorneys Tejpal Chawla and Alexandra Hughes for the District of Columbia and Trial Attorneys Heather Schmidt and Kathryn DeMarco of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

A criminal complaint is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Lemma complaint Lemma affidavit

Updated September 21, 2023

Topics

COUNTERINTELLIGENCE | NATIONAL SECURITY

Components

Federal Bureau of Investigation (FBI) | National Security Division (NSD) | USAO - District of Columbia

Press Release Number: 23-1,038

Related Content

PRESS RELEASE

Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea

The Justice Department unsealed charges, seizures, and other court-authorized actions to disrupt the illicit revenue generation efforts of the Democratic People's Republic of Korea (DPRK or North Korea).

May 16, 2024

PRESS RELEASE

Justice Department Announces Arrest, Premises Search, and Seizures of Multiple Website Domains to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea

The Justice Department today announced a series of coordinated and court-authorized actions to disrupt the illicit revenue generation efforts of Democratic People's Republic of Korea (DPRK) information technology (IT) workers.

May 16, 2024

PRESS RELEASE

Maryland Woman Pleads Guilty to Conspiring to Destroy the Baltimore Region Power Grid

Sarah Beth Clendaniel, 36, of Catonsville, Maryland, pleaded guilty today to conspiring to damage or destroy electrical facilities in Maryland.

May 14, 2024

Office of Public Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Office of Public Affairs Direct Line
202-514-2007

Department of Justice Main Switchboard
202-514-2000

Signup for Email Updates
Social Media

An official website of the United States government Here's how you know

PRESS RELEASE

U.S. Navy Sailor Sentenced to 27 Months in Prison for Transmitting Sensitive U.S. Military Information to Chinese Intelligence

Monday, January 8, 2024

Share

For Immediate Release
Office of Public Affairs

A U.S. Navy service member was sentenced today to 27 months in prison and ordered to pay a $5,500 fine for transmitting sensitive U.S. military information to an intelligence officer from the People's Republic of China (PRC) in exchange for bribery payments.

According to court documents, Petty Officer Wenheng Zhao, 26, aka Thomas Zhao, of Monterey Park, California, pleaded guilty in October 2023 to one count of conspiring with the intelligence officer and one count of receiving a bribe.

"Mr. Zhao betrayed his solemn oath to defend his country and endangered those who serve in the U.S. military," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "Today, he is being held to account for those crimes. The Justice Department is committed to combatting the Chinese government's efforts to undermine our nation's security and holding accountable those who violate our laws as part of those efforts."

"Zhao betrayed his country and disgraced himself when he accepted bribes from an intelligence officer with the People's Republic of China," said U.S. Attorney Martin Estrada for the Central District of California. "As a result, he has now been removed from the military and will serve time in federal prison. Today's sentence shows that my office will swiftly act to root out and punish those who seek to undermine our nation's security."

"Make no mistake, the PRC is engaged in an aggressive effort to undermine the national security of the U.S. and its partners," said Executive Assistant Director Larissa L. Knapp of the FBI's National Security Branch. "Zhao chose to betray the oath he took to our country and put others at risk by providing sensitive U.S. information to a PRC intelligence official. The Chinese Communist Party has repeatedly shown it will freely break any law or norm to achieve a perceived intelligence advantage. Today's sentencing demonstrates, yet again, the inability of China's Intelligence Services to prevent the FBI and our vital partners from apprehending and prosecuting the spies China recruits."

"Mr. Zhao betrayed his oath to the United States and deserves to be held fully accountable for accepting bribes in exchange for transmitting sensitive U.S. military information to an intelligence officer from the People's Republic of China," said Acting Special Agent in Charge Angel Cruz of the Naval Criminal Investigative Service (NCIS) Office of Special Projects. "NCIS will continue to leverage its unique law enforcement and counterintelligence authorities to vigorously pursue those who attempt to compromise our national security information. We are grateful to the FBI and Department of Justice for their substantial assistance to this lengthy investigation and greatly appreciate our continued partnership."

Zhao, who worked at Naval Base Ventura County in Port Hueneme and held a U.S. security clearance, engaged in a corrupt scheme to collect and transmit sensitive U.S. military information to the intelligence officer in violation of his official duties.

Between August 2021 and at least May 2023, Zhao received at least $14,866 in at least 14 separate bribe payments from the intelligence officer. In exchange for the illicit payments, Zhao secretly collected and transmitted to the intelligence officer sensitive, non-public information regarding U.S. Navy operational security, military trainings and exercises, and critical infrastructure. Zhao entered restricted military and naval installations to collect and record this information.

Zhao transmitted plans for a large-scale maritime training exercise in the Pacific theatre, operational orders and electrical diagrams and blueprints for a Ground/Air Task Oriented Radar system located in Okinawa, Japan.

He used sophisticated encrypted communication methods to transmit the information. He also destroyed evidence and concealed his relationship with the intelligence officer. Zhao's conduct violated his official duties to protect such information and the oath he swore to protect the United States.

The FBI Los Angeles Field Office's Counterintelligence and Cyber Division and NCIS conducted the investigation. IRS-Criminal Investigation provided substantial assistance.

Assistant U.S. Attorneys Annamartine Salick, Sarah Gerdes, Christine Ro and Kathrynne Seiden for the Central District of California prosecuted the case. Assistant U.S. Attorney Ryan Waters for the Central District of California and Trial Attorney Adam Barry of the National Security Division's Counterintelligence and Export Control Section provided valuable assistance.

Updated January 8, 2024

Topics

COUNTERING NATION-STATE THREATS | COUNTERINTELLIGENCE | NATIONAL SECURITY

Components

Federal Bureau of Investigation (FBI) | National Security Division (NSD) | USAO - California, Central

Press Release Number: 24-20

Related Content

PRESS RELEASE

Justice Department Announces Arrest, Premises Search, and Seizures of Multiple Website Domains to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea

The Justice Department today announced a series of coordinated and court-authorized actions to disrupt the illicit revenue generation efforts of Democratic People's Republic of Korea (DPRK) information technology (IT) workers.

May 16, 2024

PRESS RELEASE

Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea

The Justice Department unsealed charges, seizures, and other court-authorized actions to disrupt the illicit revenue generation efforts of the Democratic People's Republic of Korea (DPRK or North Korea).

May 16, 2024

PRESS RELEASE

Maryland Woman Pleads Guilty to Conspiring to Destroy the Baltimore Region Power Grid

Sarah Beth Clendaniel, 36, of Catonsville, Maryland, pleaded guilty today to conspiring to damage or destroy electrical facilities in Maryland.

May 14, 2024

Office of Public Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Office of Public Affairs Direct Line
202-514-2007

Department of Justice Main Switchboard
202-514-2000

Signup for Email Updates
Social Media

Page 2598 of 3957

PRESS RELEASE

U.S. Navy Service Member Pleads Guilty to Transmitting Sensitive U.S. Military Information to Chinese Intelligence Officer

Tuesday, October 10, 2023

Share

For Immediate Release
Office of Public Affairs

A U.S. Navy service member pleaded guilty today to federal felony offenses and admitted he transmitted sensitive U.S. military information to an intelligence officer from the People's Republic of China (PRC) in exchange for bribery payments.

Petty Officer Wenheng Zhao, 26, aka Thomas Zhao, of Monterey Park, California, pleaded guilty to conspiring with the intelligence officer and receiving a bribe.

Zhao, who worked at Naval Base Ventura County in Port Hueneme and held a U.S. security clearance, admitted he engaged in a corrupt scheme to collect and transmit sensitive U.S. military information to the intelligence officer in violation of his official duties.

"The intelligence services of the People's Republic of China actively target clearance holders across the military, seeking to entice them with money to provide sensitive government information," said Assistant Attorney General for National Security Matthew G. Olsen. "When contacted by his co-conspirator, rather than reporting it to the Navy, the defendant chose greed over protecting the national security of the United States. He is now being held accountable for his crimes. To others tempted to put personal profit ahead of patriotic duty, know that we are committed to identifying you and bringing you to justice."

"Protecting our country's national security is of the utmost importance," said Executive Assistant Director Larissa L. Knapp of the FBI's National Security Branch. "Zhao's guilty plea is an acknowledgement of the betrayal in selling sensitive military information to the Government of China. The FBI reminds all government officials to remain vigilant in reporting potential recruitment efforts by foreign actors, and we remain committed to standing with our partners to protect the U.S. from threats to our national security."

Between August 2021 and at least May 2023, Zhao admitted receiving at least $14,866 in at least 14 separate bribes from the intelligence officer. In exchange for the illicit payments, Zhao surreptitiously collected and transmitted to the intelligence officer sensitive, non-public information regarding U.S. Navy operational security, military trainings and exercises and critical infrastructure. Zhao admitted he entered restricted military and naval installations to collect and record this information.

Zhao specifically admitted to transmitting plans for a large-scale maritime training exercise in the Pacific theatre, operational orders, and electrical diagrams and blueprints for a Ground/Air Task Oriented Radar system located in Okinawa, Japan.

Zhao further admitted to using sophisticated encrypted communication methods to transmit the information, destroying evidence and concealing his relationship with the intelligence officer. Zhao's conduct violated his official duties to protect such information and the oath he swore to protect the United States.

"Officer Zhao betrayed his country and the men and women of the U.S. Navy by accepting bribes from a foreign adversary," said U.S. Attorney Martin Estrada for the Central District of California. "While he and the PRC officer he served took great pains to conceal their corrupt scheme, investigators were vigilant in uncovering this shameful plot. Today's resolution, requiring Zhao to plead guilty to all charges against him, shows that we will act swiftly and decisively to protect our nation from those who seek to undermine our security."

"The Naval Criminal Investigative Service (NCIS) would like to once again thank our partners at the FBI and Department of Justice for their continued assistance in bringing this case to a quick resolution," said Acting Special Agent in Charge Angel Cruz of the NCIS Office of Special Projects. "The swift action by the Department of Justice in prosecuting this case should serve as a warning to anyone who attempt to compromise the Department of the Navy's sensitive information or the security of our warfighters. If you or someone you know has knowledge of a potential compromise of sensitive military information, please contact your nearest NCIS or FBI office."

Zhao pleaded guilty before U.S. District Judge R. Gary Klausner. Sentencing is scheduled for Jan. 8, 2024. As a result of today's guilty plea, Zhao faces a statutory maximum penalty of 20 years in prison - five years for the conspiracy count and 15 years for the bribery charge. Zhao has been in custody since his arrest on Aug. 3.

The FBI Los Angeles Field Office's Counterintelligence and Cyber Division and NCIS conducted the investigation. IRS-Criminal Investigation provided substantial assistance.

Assistant U.S. Attorneys Annamartine Salick, Sarah Gerdes, Christine Ro and Kathrynne Seiden for the Central District of California and Trial Attorney Adam Barry of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case, with assistance from Ryan Waters of the Asset Forfeiture Section.

Updated October 10, 2023

Topics

COUNTERING NATION-STATE THREATS | COUNTERINTELLIGENCE | NATIONAL SECURITY

Components

Federal Bureau of Investigation (FBI) | National Security Division (NSD) | USAO-California, Central

Press Release Number: 23-1,117

Related Content

PRESS RELEASE

Justice Department Announces Arrest, Premises Search, and Seizures of Multiple Website Domains to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea

The Justice Department today announced a series of coordinated and court-authorized actions to disrupt the illicit revenue generation efforts of Democratic People's Republic of Korea (DPRK) information technology (IT) workers.

May 16, 2024

PRESS RELEASE

Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea

The Justice Department unsealed charges, seizures, and other court-authorized actions to disrupt the illicit revenue generation efforts of the Democratic People's Republic of Korea (DPRK or North Korea).

May 16, 2024

PRESS RELEASE

Maryland Woman Pleads Guilty to Conspiring to Destroy the Baltimore Region Power Grid

Sarah Beth Clendaniel, 36, of Catonsville, Maryland, pleaded guilty today to conspiring to damage or destroy electrical facilities in Maryland.

May 14, 2024

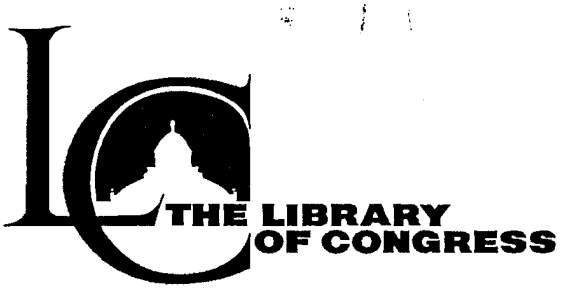
Office of Public Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Office of Public Affairs Direct Line
202-514-2007

Department of Justice Main Switchboard
202-514-2000

Signup for Email Updates
Social Media

Page 2599 of 3957



AN OVERVIEW OF

PSYCHOLOGICAL OPERATIONS (PSYOP)

Prepared by:
Federal Research Division
Library of Congress
Washington, DC 20540
October 1989
Analyst: Glenn Curtis

19951222 023

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget. Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	October 1989	Final

4. TITLE AND SUBTITLE

An Overview of Psychological Operations (PSYOP)

5. FUNDING NUMBERS

6. AUTHOR(S)

Glenn Curtis

DTIC ELECTE DEC 27 1995 S F D

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Federal Research Division
Library of Congress
Washington, DC 20540-5220

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

Prepared under an Interagency Agreement

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This study examines the theory and application of psychological operations (PSYOP), with particular emphasis on contemporary military applications. Substantial historical and theoretical background is supplied, with detailed analysis of case studies. Current PSYOP applications by the United States and the Soviet Union are emphasized and include descriptions of their respective PSYOP capabilities, organizations, and goals.

14. SUBJECT TERMS

Psychological operations
United States
Soviet Union

15. NUMBER OF PAGES

36

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18
298-102

DTIC QUALITY INSPECTED 1

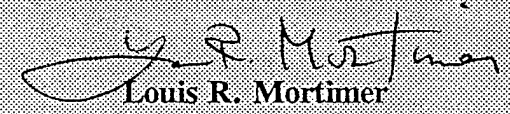
Page 2601 of 3957

Dear Reader:

This product was prepared by the staff of the *Federal Research Division* of the *Library of Congress* under an interagency agreement with the sponsoring United States Government agency.

The Federal Research Division is the Library of Congress's primary fee-for-service research unit. At the request of Executive and Judicial branch agencies of the United States Government and on a cost-recovery basis, the Division prepares studies and reports, chronologies, bibliographies, foreign-language abstracts, and other tailored products in hard-copy and electronic media. The subjects researched include the broad spectrum of social sciences, physical sciences, and the humanities.

For additional information on obtaining the research and analytical services of the Federal Research Division, please call 202/707-9905, fax 202/707-9920), via Internet frd@mail.loc.gov, or write to *Marketing Coordinator, Federal Research Division, Library of Congress, Washington, DC 20540-5220.*



Louis R. Mortimer
Chief
Federal Research Division
Library of Congress
Washington, DC 20540-5220

CONTENTS

		Page
1.	INTRODUCTION AND DEFINITIONS	1
2.	PSYOP APPLICATIONS IN HISTORY	10
3.	SOVIET PSYOP	14
4.	UNITED STATES PSYOP	21
5.	CONCLUSIONS	32
6.	ENDNOTES	34

Accesion For
NTIS CRA&I ☑
DTIC TAB ☐
Unannounced ☐
Justification .....
By .....
Distribution /
Availability Codes
Dist | Avail and / or Special
A-1

OUTLINE

1. INTRODUCTION AND DEFINITIONS

   A. Definitions of PSYOP, official and unofficial
   B. Expansion of scope in the twentieth century
   C. New concepts: disinformation, active measures
   D. Propaganda
   E. How the mechanisms of PSYOP work, with examples
   F. New applications--low-intensity conflict, unconventional warfare
   G. Domestic applications--rallying public support

2. PSYOP APPLICATIONS IN HISTORY

   A. Judith and Holophernes
   B. Ghengis Khan
   C. American Revolution propaganda
   D. World War I and the beginning of PSYOP expansion
   E. Nazi propaganda
   F. The postwar situation

3. SOVIET PSYOP

   A. Philosophical base
   B. General methodology of the Soviet PSYOP approach
   C. The Soviets PSYOP machinery
      1. International Department
      2. Propaganda Department
      3. KGB
   D. Active measures and how they work--examples
   E. Soviet propaganda failures
   F The program under Gorbachev
      1. New approaches
      2. Old approaches continued

4. UNITED STATES PSYOP

   A. The contemporary environment
   B. Historical background, beginning with World War II
   C. The U.S. PSYOP record
   D. Needs for improvement in current policy

5. CONCLUSIONS

6. ENDNOTES

1. INTRODUCTION AND DEFINITIONS

"To subdue the enemy without fighting is the acme of skill."--
Sun Tzu, 4th century B.C.

Psychological operations, or PSYOP, is a form of political and military activity that is understood and defined in a number of different ways. The definition upon which current peacetime U.S. PSYOP policy is based was established in Department of Defense Directive S-3321.1, Overt Psychological Operations Conducted by the Military Services in Peacetime and in Contingencies Short of Declared War (1984). That definition states that Psychological Operations are "planned political, economic, military, and ideological activities directed toward foreign countries, organizations, and individuals in order to create emotions, attitudes, understandings, beliefs, or behavior favorable to the achievement of U.S. political and military objectives." The DoD directive was formulated to establish standard guidelines for all aspects of PSYOP (planning, programming, execution, control) conducted by agencies of the U.S. Department of Defense in non-wartime conditions. But PSYOP also includes a number of other activities that fall under strategic military and political policy. Activities of that type are defined in Joint Chiefs of Staff Publication 1 as: "planned psychological activities in peace and war, which normally pursue objectives to gain the support and cooperation of friendly and neutral countries and to reduce the will and the capacity of hostile or potentially hostile countries to wage war." The latter definition reflects the expansion in scope that has occurred in PSYOP in the last fifty years. In the modern world, the scope of PSYOP is wider than ever

Page 2605 of 3957

before, even though the basic concepts continue as they have existed for thousands of years. Reflecting this expansion, PSYOP expert Fred W. Walker notes, "We might consider the term persuasive communications to mean the same thing as psychological operations."[1] Another expert, William Daugherty, prescribes an even broader field: "PSYOP is communication and therefore covers the entire field of human action."[2] In the present political-military meaning of the term, PSYOP is a multi-stage process that uses a combination of non-coercive devices to gain influence over the actions and attitudes of a targeted group without resorting to the use of force. The first stage of the process is defining the target, the second is finding methods or agents to influence the target's perception of reality, and the third is the output of the message through selected channels. In this process, the most critical element is credibility--to retain the attention of the audience, the audience must be convinced it is receiving information that is reliable and pertinent to its interests. If the audience detects contradictions or falsehoods, credibility is lost--for a particular operation, and perhaps for future operations as well. Therefore, the cardinal motto for all PSYOP applications is "Truth is the best PSYOP." The advantage of using PSYOP has remained the same throughout its history: if an opponent's attitude can be influenced favorably, his physical resistance will diminish. This means that, when used in combination with other military or political operations, PSYOP acts as a force multiplier, enhancing the effect of those operations on the target.

The term "psychological operations" was first used in reference to surrender messages (messages offering humane treatment for enemy

Page 2606 of 3957

personnel ceasing to resist U.S. forces) sent to the Japanese mainland in 1945. From World War I until the 1960s, "psychological warfare" was the umbrella term in common use. In the 1960s, it was recognized that much more was included in the modern concept than warfare in the conventional sense, so PSYOP became the umbrella term. Psychological warfare, or PSYWAR, remains part of the PSYOP concept. It refers to activity seeking to influence the attitudes and actions of hostile foreign groups in support of national objectives in wartime.[3] Psychological warfare is thus the type of psychological operation most closely connected with military actions: before and during engagement, to minimize the enemy will to fight, and afterwards, to underscore the impact of his losses and the hopelessness of his situation. Military actions themselves (the dropping of the atomic bomb, as an extreme example) may play a psychological role beyond their military impact, because the demonstrated ability to inflict harm has a psychological effect on the potential victim.

In the twentieth century, PSYOP applications have been broadened by the intense ideologies and systems of mass communications that have supported them since World War I. Particularly since the 1930s, the connection of PSYOP with ideology and mass communication has made it a constant strategic element of international politics. Communism and Fascism have used PSYOP in new ways, still considered unethical by much of the world, and forced the opponents of their ideologies to rethink their PSYOP procedures accordingly. The concepts of "disinformation" and "active measures" have been added to the

Page 2607 of 3957

international PSYOP vocabulary, and the definition of "propaganda" has been expanded in this process.

Disinformation, translated from the Russian term dezinformatsiya, has been defined as "any government-sponsored communication in which deliberately misleading information is passed to targeted individuals, groups, or governments with the purpose of influencing foreign elite or public opinion." Disinformation differs from propaganda because the latter does not necessarily involve deceiving a target group, and because disinformation always has a specific foreign target.[4] "Active measures" is a translation of an umbrella Soviet term, aktivnyye meropriyatiya. It has come into English usage because our term "covert activities" does not cover the enormous breadth of activities and participants included in the Soviet concept. In addition to using conventional covert operations, active measures seek to acquire influence over an opponent's attitudes through the media, economic leverage, front organizations, and other seemingly innocent overt agencies with covert sponsorship.[5] The goal of active measures can be summarized as political influence and disruption on an international scale, to achieve a specific result. Both disinformation and active measures are weapons in what Communist dogma sees as peacetime psychological warfare. That warfare is an extension of the international military goals of the Communist movement. Those weapons will be discussed more fully in the Soviet PSYOP section of this survey. But it is important to note that these types of PSYOP have been added only to the Soviet arsenal. While the U.S. must respond effectively to them, it remains committed to the principle of truth in all information programs.

Page 2608 of 3957

"Propaganda" is a broad term that means management of collective attitudes through communications and symbols, for the purpose of promoting or damaging a cause.[6] Among its non-PSYOP applications are commercial advertising, political campaigning, and religious exhortation. (The term was invented by the Roman Catholic Church in its seventeenth-century campaigns against Protestantism.) But in the contemporary public understanding, those aspects have been over-shadowed by the widespread political uses of propaganda in the twentieth century. Although the term had become associated with untruth, propaganda in the PSYOP context must contain large amounts of true information, because of the primary requirement that the audience believe the message. By convention, PSYOP propaganda is divided into three types: white, gray, and black. White propaganda originates from a correctly identified source, black from a completely misidentified source; the source of gray propaganda is masked by transmission through a "front" agency that is nominally independent of the actual source. "Symbolic propaganda" uses action rather than words to produce its effect. The most dramatic example of symbolic propaganda was the use of the atomic bomb in World War II to physically demonstrate the hopelessness of the Japanese position. Several years later, the first Soviet nuclear test sent a symbolic message that had a strong psychological effect on the West.

PSYOP relies heavily on correct evaluation and exploitation of the target's "capacity for self-deception."[7] What is this "capacity for self-deception," and how is it exploited? Approaches differ according to specific conditions, because target groups vary widely. Examples of such

Page 2609 of 3957

target groups are military enemies, political rivals, indigenous populations in guerrilla and counterinsurgency operations, and domestic populations whose support is needed for military or political campaigns. Every identifiable group, society, and nation has a unique set of needs and goals, as well as a uniquely shaped group psychology. The needs and goals may be long- or short-term, military or political, real or imaginary. To cite two extreme examples, the group psychology may be shared by a small group in a short-term, tactical situation (such as a military unit occupying foreign territory), or by several nations in a semi-permanent, strategic situation (such as a group of nations strategically located between two superpowers). Between those extremes are many combinations of needs and goals. If a psychological operation is done properly, the perceptions formed by the target group can be slanted in a particular direction without immediate challenge and actions or attitudes changed accordingly. Psychological operations thus can reduce the risk and expense of coercive action. Such operations are especially useful to groups such as guerrilla forces whose capacity for coercive action is limited. PSYOPs is not to be confused with military deception, which causes an enemy to take inappropriate action by misleading his assessment of positions or intentions.

For the operating side, the immediate target is a weak point of an ultimate target, a place where psychological advantage can be gained and used as a weapon in the longer term. How would this work in the two examples given above? For an occupying force, the points of psychological vulnerability might be distance from home and prolonged exposure to an uncomfortable cultural environment. In such a case, if

Page 2610 of 3957

the opponent's intelligence reveals discontent within the force, a psychological operation might use communications media to convince group members of the loneliness and pointlessness of their venture, and to offer easy surrender conditions. If such a message penetrates without effective challenge, it blunts the effectiveness of the occupation. This approach might be accompanied by terrorists acts that "emphasize" the alienation of the occupiers.

In the international example, smaller nations are subjected to constant superpower propaganda. The Soviet Union uses overt and covert measures in campaigns to split smaller countries from the United States and move them toward a neutral position. In Europe such efforts exploit the substantial public and official desire for peace and security, doubts about American resolve to defend Europe, and fears of nuclear war. A campaign of this sort continues over many years and is woven into the fabric of superpower foreign policy.

In modern times nations increasingly understand the need for propaganda to justify their positions to both domestic and foreign audiences. In peacetime and in protracted war, PSYOP procedures now are integrated with and parallel to measures of military preparedness. Key factors in their success are accurate evaluation of adversary psychology, secrecy, and the output of information that is consistent and credible.

A PSYOP application of particular current value is in insurgency and counterinsurgency activity in what is called "low-intensity conflict" (LIC). Geographically confined to the Third World, LIC PSYOP now is often used in confrontations of client groups of larger powers such as

Page 2611 of 3957

Soviet Union, China, and the United States. Such confrontations occur most often in areas with weak governments, poorly developed or unbalanced economies, and valuable natural resources or strategic location.[8] In recent years, El Salvador, Cambodia, and Afghanistan have been the sites of major superpower insurgency-counterinsurgency efforts. The U.S. has been on both sides of such campaigns, aiding counterinsurgency in El Salvador and the Philippines, insurgency in Nicaragua and Angola. Because guerrilla warfare relies heavily on psychological impact to complement sheer force, successful counterinsurgency must use PSYOP effectively to defeat such campaigns. Victory goes to the side that best understands and exploits the psychology of the indigenous population that is the main source of support for the guerrillas. As insurgency and counterinsurgency have developed, important PSYOP tools are community relations programs, public information, and civic action programs carried out by military personnel in the areas in dispute. Insurgency PSYOP is not limited to proxy confrontations between the United States and Soviet camps. The Ayatollah Khomeini conducted a very effective insurgency against the Iranian government. Exploiting religious fervor and dissatisfaction with the government, the exiled Khomeini smuggled large numbers of tape cassettes into Iran, spreading propaganda to stir revolutionary feeling and build a movement from an initially small number of followers.[9] In this case, no effective counterinsurgency campaign was mounted, and the government fell.

In the contemporary world, unconventional warfare is the rule, not the exception. Given that fact, PSYOP has become a military tool of

greater importance than it was in the "classic" model. This is because the element of psychology is present in all forms and levels of combat, even when some conventional aspects of doctrine become less relevant. When the clear boundaries of open combat disappear and civilian populations become an integral part of every confrontation, PSYOP no longer is a specialized, sinister weapon that can be disregarded because it does not yield spectacular results. Proper PSYOP procedure is often a critical guarantee of success; solid PSYOP approaches to an indigenous population can hold territory with minimal expense or loss of life. But under such circumstances, the PSYOP weapons must be as familiar as any other weapon to all military personnel, because it is they who carry out PSYOP in their everyday contact with the population. In places such as El Salvador, the psychological relationship between military personnel and the civilian population is a prime determinant of the government's success against guerrillas; in this case, U.S. advisers are training the host nation's forces in PSYOP applications. A key word is "integration" of PSYOP into the framework of conventional military doctrine.

Another important application of PSYOP is to rally a domestic population behind a political or military cause. In wartime all nations, whatever their political system, must inspire willing sacrifice by their people. All U.S. war efforts, from the American Revolution to Vietnam, have required extensive "selling." As Korea and Vietnam showed, the complex psychology of a democracy is not always receptive to such campaigns. In such cases, targeted propaganda is the most important tool, but covert active measures have also been useful for totalitarian governments in combating uncooperative internal elements.

Page 2613 of 3957

The historical examples that follow will show the variety of goals, methods, agents, and target groups that have been included in psychological operations of the past. In the sections that follow, discussion of past and current Soviet PSYOP will show how that nation has refined and expanded the entire field to meet the ideological requirements of the Leninist state. And discussion of United States PSYOP, past and present, will focus on the response to Soviet PSYOP campaigns from World War II to the present, in what has become the most massive PSYOP battle in history.

2. PSYOP APPLICATIONS IN HISTORY

The Art of War, a treatise written by the Chinese military thinker Sun Tzu in the fourth century B.C., advocates the idea that an army of superior numbers can be "made not to fight." This idea was in use even before that time. An early example is the slaying of Holophernes, leader of an Assyrian force invading ancient Israel, by the Israelite Judith. Knowing that enemy troop morale depended heavily on the single figure of the commander, Judith gained the confidence of Holophernes, beheaded him, and carried the head back to her people. The symbolism of the missing head and the lost command figure totally demoralized the Assyrians, who were easily routed in spite of vastly superior numbers. The story appears in the apocryphal Biblical Book of Judith; its historical accuracy is unproven, but it remains a good example of assessing the enemy's psychological weak point and using a powerful psychological symbol to bolster the morale of one's own forces.[10]

Page 2614 of 3957

In another example, Ghengis Khan is credited with leading huge hordes of savage horsemen across Russia and into Europe. The size of his armies was exaggerated by agents planted in advance of the army and by rumor and other forms of propaganda. To supplement his PSYOP activities, Ghengis Khan also used rapid troop maneuver to confirm the illusion of invincible numbers. Because the Mongols created an image of total, barbaric domination, target groups never believed they were the victims of astute psychological warfare. Once the image had spread, the Mongols had created a permanent weakness in enemy psychology, and thus gained a military advantage wherever the Mongol reputation was known.[11]

In another instance, during the American Revolution the rebels distributed propaganda leaflets that invited Hessian mercenaries and British common soldiers to desert. One such leaflet provided two short, contrasting lists: the negatives of life in the British Army and the advantages of deserting and settling permanently in America. Promises of leniency and surrender passes have become a staple of battlefield PSYOP. In the Revolutionary War application, the direct appeal exploited the mentality of the occupying force, class differences between officers and enlisted men, and nationality differences between the British and their German mercenaries. Thousands of troops heeded the appeal and never returned to Europe. At the same time, domestic loyalist opposition was muffled by anti-British propaganda in the newspapers of the thirteen colonies.[12]

A qualitative change occurred in PSYOP about l900, when communications became much faster and more inclusive. For the first time, entire nations could be targeted in a psychological operation by

Page 2615 of 3957

print, radio, and film. These media provided direct, reliable transmission of propaganda messages to anyone within sight or earshot. The new media were first used widely in World War I; the British used them to spread rumors of German atrocities, including cannibalism.[13] Because the British had already developed a more sophisticated print and communications system than the Germans, they mounted a propaganda campaign that the Germans could not overcome. The British diplomatic service was also more adept at public diplomacy than its German equivalent. The British used German propaganda ineptitude to their advantage by simply disseminating many undiplomatic German statements, without change or comment; the difference in PSYOP skill between the two sides was enough to make the message clear that the Germans were uncivilized, arrogant "Huns" (a term used by the Kaiser himself for his army). German morale was deflated by having bombastic public statements made into ammunition for the enemy. This propaganda defeat was an important incentive for better performance by German propagandists in the next war.

Because of the expanded scale on which it was used, PSYOP is considered by historians as a crucial factor in the Allied victory in World War I. The Creel Committee, the first specialized U.S. agency for wartime propaganda, succeeded in building domestic support for a war that was not popular initially; it also was the model for later U.S. publicity and propaganda agencies. And the very presence of the U.S. in the war, after long neutrality, had great psychological as well as the military impact. Early in 1917, Germany began sinking all ships approaching Britain, in order to starve the British into surrender. The

Page 2616 of 3957

Germans assumed that Britain would surrender before the U.S. could retaliate for its sunken ships by entering the war on Britain's side; when the error of this gamble became obvious, German morale fell. The German General Ludendorff named allied PSYOP the most important factor in German morale decline.

Before and during World War II, the Nazis used a propaganda machine aimed first at domestic opinion, then at world opinion. The basic psychological assumption of that machine was that public opinion is formed by symbols and images, not rational thought. If the correct symbols were presented with enough force, the public would follow. The theory worked because the audiences chosen were prone to self-deception about certain emotional topics. The charismatic figure of Adolph Hitler provided the ultimate symbol of renewed power to a nation humiliated by the results of World War I. The propaganda machine of Joseph Goebbels convinced Germans and many audiences elsewhere that Communists and Jews were the enemies; that only Fascism could provide protection from them; and that the advance of Fascism was both just and inevitable.[14] The worldwide desire for peace provided a psychological weak point that prevented rational evaluation of these messages; British and United States opposition was delayed until Europe had been conquered piecemeal. By that stage, Germany had developed effective print and broadcast media. A much older form of propaganda dissemination, the mass rally, was also used very profitably. The Germans also made extensive use of "black propaganda" and subversive pro-Nazi groups and agents in occupied territory.

Page 2617 of 3957

After World War II, the Soviet Union raised peacetime PSYOP to new levels of sophistication as the Cold War broke out. And, as new international political conditions developed, tactical military PSYOP began to play a new role. These activities will be the subject of the following sections.

3. SOVIET PSYOP

Like other aspects of Soviet policy, the Soviet theory of psychological operations is based on the teachings of Lenin. The central concept (which sharply differentiates Soviet from United States approaches to the subject) is that the Soviet Union is in a state of undeclared war with capitalist world--a war that will not end until world Communist domination is achieved. Given the magnitude of the goal, moral constraints have had much less influence on Soviet PSYOP than on those of the United States and other countries. In the words of covert operations specialist Chapman Pincher, for the Soviet Union "politics is the continuation of war by other means."[15] On the peacetime strategic level, politics is the main arena of Soviet PSYOP. However, this approach was not invented by the Bolsheviks in 1917; it was used sporadically for centuries by the Russian tsars in domestic and foreign relations, but it has been codified and intensified in the last seven decades. Soviet PSYOP is by far the most intensive, complex and consistent peacetime campaign of its type ever launched. The Soviet political system backs its PSYOP policy with whatever resources are necessary to achieve its goals.

Page 2618 of 3957

Soviet PSYOP campaigns are a tightly integrated combination of conventional devices, influential "legitimate" institutions such as the diplomatic corps and the press, and covert activities. On the level of open propaganda, the goal is to "out-talk" the adversary, establishing terms of international dialogue favorable to the Soviet Union. This process is constant, aimed at wearing down the West and convincing other listeners that the Soviet position is valid. A favorite message in the Soviet arsenal says that it is the West that is on the psychological offensive: with an insatiable ideological drive, imperialism uses all possible psychological means to undermine the progressive development of other nations toward the ideal, inevitable Communist order. Furthermore, Dmitri Volkogonov, the leading Soviet PSYOP theoretician, says that the imperialist powers invented psychological warfare to maintain world domination.[16] Briefly stated, his view is that imperialist PSYOP seeks to divide the communist world, disorient its people politically, and falsely portray the Soviet Union as the main threat to world peace. Volkogonov attributes virtually all the known Soviet active measures methodology to the United States and its imperialist allies. To the extent that this idea is believed around the world, Soviet PSYOP succeeds in putting the debate into its terms.

Three departments of the Soviet government supervise active measures and propaganda activities. The International Department of the Communist Party of the Soviet Union provides liaison with nonruling Communist parties and front organizations abroad, directs their active measures, and apportions responsibility for various types of activity. This department also suggests new measures to advance the international

Page 2619 of 3957

policies of the ruling Politburo. Overall foreign policy is often affected by activities of the International Department (I.D.), which has no equivalent in Western governments.[17] The functions of this agency appear to have been expanded and refined in recent years, especially after the abolishment of the party's International Information Department. A key figure in this development was Anatoli Dobrynin, former Ambassador to the U.S. and head of the I.D. until late 1988. The latter was in charge of the overall propaganda apparatus until l986, when that function was split between the I.D. and a second major agency, the Propaganda Department. The latter now runs all domestic and foreign propaganda efforts. Its level of sophistication rose especially fast under Aleksandr Yakovlev, who until reassigned late in l988 was an effective domestic and international spokesman for the Gorbachev reforms.[18] The third propaganda agency is the KGB, or Committee for State Security, which handles espionage and disinformation activities at home and abroad. The disinformation mission aims mainly at destabilizing and misleading the NATO alliance and Japan, while concealing actual Soviet policy aims. In addition to the three major agencies, the Ministry of Foreign Affairs has broad responsibility for the overt Soviet press and foreign cultural relations--which in the Soviet system are closely coordinated with less "legitimate" PSYOP functions.

Although government reform has changed some of the structure of this system, there is evidence that even more resources are now allocated to PSYOP activities. History has shown that active measures are emphasized in times of improved relations with the West because targets become more vulnerable in such times.[19]

Page 2620 of 3957

Favorite covert devices of Soviet active measures are forged documents and planted media stories, surfacing in forms that erode the position of the ultimate target. Often, forged United States and NATO documents are used to show that the West is intent on aggression in Europe or the Third World. Active measures aim to divide the target group (most often NATO) by intensifying latent hostilities within it. Germany is a favorite target for such divisive methods because the Nazi past remains a psychological weak point for all of Europe. Print and broadcast media are nearly always used to achieve maximum dissemination of a message. The procedure is to identify a potentially sympathetic audience with political influence (for example, the leftist West German Green Party and the Labor Party in Great Britain), and tailor the message for maximum favor with that audience.[20] In recent years, this tailoring includes maximum exposure of the terms perestroika (restructuring) and glasnost (openness), which for the Western audience indicate that hoped-for Soviet internal reforms are taking place and Cold War tension is easing. Debate flourishes on the actuality of those reforms, but there is no doubt that the terminology used to describe them has been quite successful in exploiting a Western psychological preoccupation.

A variety of agencies--from individual covert agents to client nations--carry out Soviet psychological operations. In the Third World, Cuba is an especially active agent, working on Soviet operations and independently. A major front organization for Soviet operations is the Helsinki-based World Peace Council. That organization, indirectly controlled by the Communist Party of the Soviet Union, plays a major role in stirring anti-NATO feeling in Europe. Political influence

Page 2621 of 3957

operations are a special type of active measure, using personal contacts to advance a Soviet position in foreign decisionmaking institutions. These contacts range from foreign figures (diplomats, journalists, scientists) to KGB agents "planted" in positions of influence.[21] Because the Soviet Union is the initiator, it has been able to choose its "battlefields," where chances of achieving psychological influence are greatest and opponents can be put on the defensive. In target countries, such campaigns exploit weak points such as ethnic rivalries, distrust of existing social or government systems, and class antagonism. And active measures are always used in conjunction with other devices to advance Soviet foreign policy goals.

A few examples of Soviet active measures will demonstrate their goals and methods. In 1976, a testament of Zhou En-lai surfaced in a prominent Japanese newspaper. The document spoke against the Cultural Revolution in China and advocated closer relations with the Soviet Union. It had been placed by the KGB office in Tokyo.[22] In another instance, the KGB created a pamphlet, entitled CIA Insider, purported to be a listing of CIA agents and press outlets all over the world. The pamphlet, released in Switzerland, attempted to show the pervasive CIA influence in the Western press; it is an example of the "upside-down" black propaganda ploy of attributing Soviet PSYOP methods to Western nations.[23] And in the early 1960s, a long series of items planted in the European press ruined the political career of Franz-Josef Strauss, a staunch advocate of United States armaments in West Germany. Strauss was painted as a warmonger seeking revenge on the Soviet Union for the results of World War II.[24] In another example, in 1979, Radio Ba Yi

Page 2622 of 3957

began broadcasting into China from the Soviet Far East. Its positions on domestic, diplomatic and military issues aimed initially at discrediting Deng Xiaoping, who was also attacked directly by the station. The Soviet Union acknowledged no role in the broadcasts, which supported all Soviet positions and advocate closer Sino-Soviet relations.[25] In the recent Soviet effort for better relations with China, the station was shut down.

The Soviet Union has also found itself on the negative side of PSYOP activities. When it invaded Afghanistan, counterinsurgency efforts failed to win over the indigenous population, and the occupying force became demoralized by guerrilla psychological warfare. And in l983 the Soviet Union shot down a Korean civilian airliner, causing an uproar in world opinion. The Soviets tried to turn press attention "upside-down" by claiming that the United States had provoked the incident--but Soviet statements were poorly coordinated and contradictory, and they failed to win the battle of world opinion.[26] The obvious fabrications and confusion in the propaganda line violated the basic principle that information used in PSYOP must be believable to the target group.

Historically, Soviet active measures have had several weaknesses. The Soviet ideology of atheism and Communism is unattractive to many audiences, so it must be concealed or glossed over in many cases. Acts such as the Afghan invasion have eroded trust in the Soviet Union as defender of Third-World liberty. And many forgeries and press placements have been poorly executed and very obvious.[27]

Most experts on the Soviet Union agree that in recent years the sophistication of Soviet propaganda and active measures has grown, and some of their weaknesses have been eliminated. First, the Soviet Union

Page 2623 of 3957

now has a charismatic leader in the person of Mikhail Gorbachev. This is a weapon the Soviets have never had before. Gorbachev is able to send direct, credible messages to world leaders and use international media to propagate a view of the Soviet Union as a reformed, peace-loving, and benign nation. Like Roosevelt, he has cultivated a personal image of honest and moral humanity that has universal appeal. Following the cardinal principle of PSYOP, that all messages be based in truth, Gorbachev's messages utilize the actual liberalization of internal and external Soviet policy (highlighting such events as removal of Soviet tanks from Hungary and the liberation of Andrei Sakharov) to maximum effect in shaping the new image. Arms control proposals, slipshod and obviously insincere under previous regimes, now impress even Western skeptics with their scope and consistency. Gorbachev has also shown wisdom in choosing and shaping his messages to target audiences, alternating between firmness and conciliation. At the same time, there is strong evidence of continued commitment to Lenin's principle of all-out political war as an extension of military struggle in peacetime. A 1988 report of the United States Information Agency lists major active-measures "black" programs begun after Gorbachev came to power. Among the messages widely disseminated by these programs: the AIDS virus was created in an American laboratory for germ warfare; the United States developed a weapon that kills only non-whites; Latin American babies are butchered and sold to U.S. distributors for use in medical transplants; and the CIA murdered Swedish Prime Minister Olaf Palme. While such messages have not changed substantially since earlier years, the approach of more subtle, "gray" programs has changed. Soviet-controlled

Page 2624 of 3957

international peace groups now seek a broader appeal by softening their rhetoric; other Soviet-influenced groups now seek wide contact with Westerners, to subtly convince them that Soviet positions are just; and the Soviets now sponsor many international peace forums, including respected professional figures, to enhance their peace-loving image. All these efforts complement the statements and actions of Gorbachev, whose programs of glasnost and perestroika seem committed to greater Soviet openness and nonmilitary programs.[28]

In summary, the Soviet Union is by far the largest practitioner of PSYOP in the world. PSYOP has been an integral part of its foreign and domestic policy since the Bolshevik Revolution. In organizational structure and function, Soviet psychological operations overlap the more conventional functions of government and diplomatic institutions. Because PSYOP is still viewed as another version of military struggle, coordination of tactical military doctrine with long-term strategic-international goals remains especially close and consistent.

4. UNITED STATES PSYOP

In the "age of communications," all nations must find ways to "explain themselves" to the rest of the world, and to their domestic populations. The more international obligations the nation has, the more vital is the process of sending messages that create desirable psychological responses in their recipients. As described in the previous section, the United States faces a sustained, multilevel Soviet PSYOP

Page 2625 of 3957

campaign. The campaign aims to discredit the United States and its allies in the view of the world and of their own populations.

Since mass communications became a PSYOP tool, the United States has been involved in several wars requiring domestic and international justification of its position versus adversaries such as the Germans, the Japanese, the Koreans and Chinese, and the Viet Cong. In each conflict, large-scale tactical PSYOP machinery also went into motion. Generally, such efforts have been a response to the initiative of an opponent; neither strategic nor tactical PSYOP apparatus has been at adequate strength before the threat appeared. And since World War II, moral and bureaucratic questions have interfered with coordination of PSYOP programs. As the definition of the word "war" becomes less clear, domestic perceptions of military and political goals become more vulnerable to psychological targeting by adversaries. This was seen most dramatically in Vietnam, but it also applies to current low-intensity conflict situations.

In World War II, a very effective PSYOP weapon of the United States was the charismatic leadership of Franklin Roosevelt, whose inspirational radio broadcasts were admired by Joseph Goebbels, Hitler's propaganda chief.[28] The United States created two major agencies for PSYOP activities in the war: the Office of War Information (OWI, for domestic and foreign propaganda), and the Office of Strategic Services (OSS, among whose functions was direction of military PSYOP). The OWI consolidated a number of information agencies that existed before the war. Wartime urgency did not prevent friction between the two agencies, congressional interference, and diffusion of PSYOP and

propaganda decisionmaking among theater commanders of the Army and Navy--factors that hindered PSYOP missions in many cases.[29] But the propaganda of the OWI was marked by careful evaluation of target psychology, appropriate messages, and effective delivery. For example, the OWI aimed surrender appeals at the psychological vulnerabilities of fanatical Japanese soldiers, inducing large numbers to surrender in spite of a military code that seemingly precluded such behavior.[30] Although the United States PSYOP effort in World War II was somewhat cumbersome and disorganized, there were enough instances of such astute targeting to overcome the head start that the Axis powers had gained in propaganda.[31]

After the war, the word "propaganda" was associated in the United States with Fascism and Communism, the systems that had "reinvented" the device for their ideological advancement. The American public did not consider propaganda an activity to be pursued in peacetime by the leader of the free world. There followed a period of indecision about the role of PSYOP in peacetime, and most wartime PSYOP units were disbanded shortly after the war ended. When the Korean War began, only one operational psychological warfare troop unit existed. As in the previous war, a strong PSYOP effort was eventually mounted in Korea, offering mainly radio, loudspeaker, and leaflet support of conventional ground troops. But complaints of weak support often came from the PSYOP units at the front.[32] The Korean War was the stimulus for formation in 1951 of the Office of the Chief of Psychological Warfare (the first centralized agency for PSYOP) and the Psychological Warfare Center at Fort Bragg in 1952. The former no longer exists, but the

Page 2627 of 3957

latter is now the center of PSYOP training and research for all the Armed Forces. In 1953 the United States Information Agency (USIA) was created for international dissemination of information.

In general, withdrawal from PSYOP activity after World War II was slowed by the realization that the Soviet Union was now a formidable enemy in the Cold War. This realization was based on two ideas: that the world does not automatically understand or approve of the United States; and that the Soviet Union is ready and able to exploit doubts about the morality and motives of the United States, in numerous overt and covert ways. An initial reaction to this situation was creation of the Central Intelligence Agency in I946, with authority for covert psychological and political activities. The size and scope of this organization grew very fast during the Korean War.[33]

Beginning about 1960, Communist expansionist doctrine has sought to exploit "wars of liberation" and insurgencies in areas previously under European colonial control. Soviet propaganda has portrayed the Soviet Union as defender of oppressed peoples, and the United States as an exploiting imperialist.[34] To meet this potent psychological gambit of guerrilla war, U.S. PSYOP applications in influencing the Third World and conducting unconventional warfare have become increasingly important in recent years.

How successful has the United States been in meeting postwar PSYOP challenges? The record has been mixed. A number of systemic differences prevent United States PSYOP from ever being the all-pervasive, centralized extension of foreign policy that it is for the Soviet Union. In the United States, all information cannot be officially

Page 2628 of 3957

controlled; secrecy is difficult even in the most critical cases; and decisionmaking always involves a number of conflicting views. The Soviet Ministry of Foreign Affairs is mobilized for propaganda activities that the United States State Department could never undertake. Likewise, no American institution has the total control exercised by the Communist Party of the Soviet Union.

The Vietnam War was the most recent large-scale PSYOP campaign of the United States. As in Korea, the main tactical devices were loudspeakers, leaflets, and radio. The Chien-Hoi (Open Arms) amnesty program stressed the strength of the South Vietnamese Army and the hopelessness of the Viet Cong position. In many respects, this massive effort fell short on both strategic and tactical levels: the first when domestic and international doubts about legitimacy were not met by United States official information, the second when PSYOP and military operations failed to complement each other, and the enemy was able to exploit the psychological vulnerabilities of both United States troops and the indigenous population of Vietnam.

However, a number of post-Korea United States psychological operations have been successful. In 1965, American troops invaded the Dominican Republic to quell what was believed to be the first stage of a Castro-type revolution. During the American presence, liaison between military and civilian PSYOP groups was quite successful in supporting the military and political aims of the occupation.[35] According to verbal reports of participants, leaflets became such a valuable source of information that they were eagerly purchased in the capital city of Santo Domingo. In the Vietnam War, the Civilian Operations and Revolutionary

Page 2629 of 3957

Development Support centralized and focused counterinsurgency targeting of indigenous populations in some areas.[36] The Joint U.S. Public Affairs Office (JUSPAO), founded to integrate public information and PSYOP functions in Vietnam, achieved a number of successes. CounterPSYOPs activity in Europe in the early 1980s ensured timely installation of intermediate-range missiles, despite an intensive Soviet psychological campaign to exploit European peace and antinuclear groups. And in the Grenada invasion of 1983, U.S. amnesty messages and rewards substantially reduced the opposing force.

After Vietnam, overall budgetary support for PSYOP declined. Army PSYOP units in Okinawa, Panama, and Germany were disbanded. This left the 4th Psychological Operations Group (consisting of four battalions in l988) at Ft. Bragg as the only active-duty unit in the United States Armed Forces with an exclusively PSYOP mission.[37] A National Guard unit remained in the Air Force and support units remained in the Navy, but Ft. Bragg became the source of PSYOP support for all types of military operations. If medium- and high-intensity conflict should break out, support would come from a reserve PSYOP unit trained at Ft. Bragg. In peacetime, the active-duty unit builds the research base for future readiness, and it has the mission of PSYOP support for low-intensity conflicts and peacetime overt activities.[38] Because the latter type of support has growing potential for application, a number of leading PSYOP authorities have agreed that United States capability needs to be expanded, and that PSYOP expertise should be integrated into standard U.S. military training. This group includes Alfred Paddock, formerly commander of the 4th Psychological Operations Group and director of

Page 2630 of 3957

psychological operations in the Pentagon; Melvin Kriesel and Michael Totten, former commanders of the 4th Psychological Operations Group; and Sam Sarkesian, professor of political science and former chairman of the Inter-University Seminar on Armed Forces and Society.[39]

Since the Reagan Administration put additional emphasis on information as one of the elements of national power, overt psychological operations in peacetime have been increased. These psychological operations have included training and advice to indigenous forces allied with the United States, surveys and assessments leading to actual operations, miscellaneous support to host nation PSYOP programs, and other overt PSYOP projects. Typical of PSYOP support to host nation programs is the long-term program created for El Salvador. One trainer is assigned to the U.S. military group in the capital, San Salvador, to coordinate all U.S. PSYOP programs in the country. Over the years the U.S. PSYOP contribution has resulted in significant change not only in the PSYOP practices of the El Salvadoran Armed Forces, but also in their general approach to insurgency, including an increased respect for human rights.

Programs similar to the El Salvadoran project exist worldwide, as established by DoD Directive S-3321.1. This directive requires every Unified and Specified Commander-in-Chief to conduct overt psychological operations in peacetime as appropriate to the military mission.

Overt psychological operations are coordinated with the State Department and require Country Team approval for each operation. The operations are coordinated with the United States Information Agency (USIA) to prevent dissemination of conflicting information. DoD

Page 2631 of 3957

operations attempt to fill the informational niches not filled by other agencies, dealing with subjects and areas of primary DoD concern but of secondary importance to the other information agencies.

At the strategic level, covert psychological activities are centralized in the Central Intelligence Agency, the latitude of whose operations has varied with the degree of oversight exercised by Congress. Meanwhile, overt propaganda is less centralized, and it is isolated from covert activity. In the I980s, the United States has sought to bolster programs of cultural relations and positive image-making abroad. "Public diplomacy" has been used much more aggressively to correct the record about United States intentions and in counterattacking Soviet and Cuban propaganda. In I983 a Special Planning Group was formed, including representatives from all government agencies having propaganda functions. The goal of this group was to centralize the public diplomacy effort and put forth a coherent, positive international image. The USIA has been instrumental in several specific improvements: coordinating United States explanations of Central American policy; ensuring INF installation in Europe; and increasing the budget for cultural relations and propaganda.[40] An interagency committee for public diplomacy, first used in the INF European campaign, continues low-key, behind-the-scenes coordination of policy statements and explanations.

But policy agencies still lack coordination with public diplomacy efforts; agency roles in PSYOP are not well defined; and the United States has often found itself in a reactive position in international situations requiring PSYOP applications. Because of agency

Page 2632 of 3957

compartmentalization, messages often lack the crucial element of credibility because they are contradictory. And, in the words of Army intelligence officer and scholar John Oseth, there is an "American suspicion of the tools of psychological manipulation,"[41] which insulates American institutions from association with such activities. On the military side, this takes the form of suspicion toward peacetime support of elite, special-purpose groups, such as those that would be given exclusively PSYOP missions.

A number of separate United States agencies now disseminate propaganda worldwide. The United States Information Agency runs the Voice of America and various cultural and information programs abroad. The Board for International Broadcasting runs Radio Free Europe and Radio Liberty, which broadcast into the Soviet bloc. And the Central Intelligence Agency continues its administration of covert PSYOP and counterPSYOPs activities abroad. DoD peacetime overt PSYOP activities have joined these groups in disseminating international information. Like the USIA, DoD disseminates international information only to foreign groups overseas.

As a result of governmental recognition of PSYOP deficiencies, in 1985 the Secretary of Defense promulgated a Master Plan to revitalize PSYOP. This plan reviewed the considerable inadequacies of PSYOP at that time, and recommended remedies for each item. Responsibility for DoD policy was given to the Under Secretary of Defense for Policy, which in turn created a Directorate for Psychological Operations assigned to the Deputy Under Secretary for Policy. This directorate was to be responsible for PSYOP policy and monitor response to the Master Plan.

Page 2633 of 3957

The active duty PSYOP group was fully manned for the first time in years, and modernized equipment of all types replaced the Korean War-vintage radios, presses, and loudspeakers of the PSYOP units. PSYOP education and training were greatly improved, with a new Army functional area code assigned for PSYOP officers, and an enlisted military specialty was created. New awareness and staff training courses were created, to provide officers and enlisted personnel to meet a new demand for competent staff personnel. PSYOP staffs at all levels were created and strengthened, and they were moved out from under control of special operations staffs. The PSYOP Worldwatch Program was created, as a new, proactive body at the Joint Staff level, monitoring daily intelligence and open-source traffic for situations in which PSYOP input is appropriate. Similar bodies were created at the Unified and Specified Commands, adding a new element of proactive PSYOP to replace the traditional U.S. reactive posture. The Secretary of Defense assigned PSYOP forces to the newly created United States Special Operations Command, giving a four-star proponent for PSYOP and establishing a new support structure for Unified and Specified Command psychological operations across the spectrum of conflict. Heightened preparedness for wartime, contingency situations, low-intensity conflict, and peacetime operations resulted from the changes initiated from the Master Plan. By 1989, the response to the Master Plan had so changed the PSYOP environment that a new plan, was needed to accommodate the progress made since 1985. Because of the nature of PSYOP, these peacetime programs provide the most realistic training for PSYOP personnel. The overall effect of this PSYOP renaissance has not yet been calculated,

but many successes in peacetime and low-intensity conflict have already been ascribed to it.

In conclusion, the United States has practiced psychological operations in the twentieth century when such measures were a military or diplomatic necessity, but there has been great reluctance to organize and maintain units with PSYOP capability during peacetime. When the "rules of the game" changed after World War II, awareness of the value of PSYOP gradually increased, and a number of organizations were given distinct functions such as covert activities and distribution of cultural information. But no overall, permanent coordination structure has appeared to maximize the PSYOP potential of each organization as needed, either on the tactical-military or the strategic-international level.

On the tactical level, United States military PSYOP staffing has been low, and military personnel are not widely trained in the goals and methods of psychological operations. Writers commenting on this situation have pointed out that the potential requirement of United States PSYOP aid to counterinsurgency in the Third World seems to be increasing, without appropriate improvement in readiness. Although efforts were made periodically toward a comprehensive U.S. tactical PSYOP doctrine, the policy has been to approach each case individually after it arises, with no overall philosophical context.[42] The most recent of those efforts, the DoD Master Plan, has focused greater attention and resources on the subject.

Page 2635 of 3957

5. CONCLUSIONS

The time-honored principles of PSYOP retain exactly the same basic value as they have always had: as a force multiplier that complements military operations by lessening the determination of the target to resist. But since the days of Genghis Khan the definition of PSYOP has come to include a much broader range of activities and methods: from organized campaigns using leaflets and speakers in conventional tactical combat, to official statements by national leaders aimed at an international audience, to the everyday interaction of non-specialized military personnel with a host population. In spite of expanded application, the basic principles still apply: the message must be credible, meaning that it must be based in truth; it must be chosen and shaped to create a positive impression on the target audience; and it must be integrated into the overall military or political program of which it is part.

Contemporary PSYOP is practiced by many countries and agencies, in many circumstances, for a variety of goals. For the Soviet Union, it is a standard part of foreign policy, an accepted method of achieving national goals. For the U.S. it retains a negative connotation, both in political and military usage, although its utility has been proven in many situations. Consistency and coordination have been missing even in U.S. wartime PSYOP. For other nations involved in low-intensity or unconventional warfare as sponsors or participants, PSYOP has become an invaluable tool in gaining the support of segments of a population. For this reason, U.S. PSYOP support of allied nations, and effective

Page 2636 of 3957

PSYOP approaches to neutral nations, has become a vital part of the U.S. program of protecting or influencing those countries.

All of this occurs in a world where: the chief potential military opponent has a dynamic, sophisticated, multilevel PSYOP apparatus; conventional military operations are increasingly costly, while PSYOP remains relatively inexpensive; and the shadow of nuclear war puts most world conflicts into vague, quasimilitary forms. Under these conditions the psychology of conflict assumes a primary role, one that must be understood by every military commander.

Page 2637 of 3957

ENDNOTES

1. Fred W. Walker, "Truth Is the Best Propaganda: A Study in Military Psychological Operations." National Guard, October 1987, p. 27.

2. American Institutes for Research in the Behavioral Sciences, The Art and Science of Psychological Operations: Case Studies of Military Applications, vol. 1. (Washington: Department of the Army, 1976), p. 17.

3. United States Joint Chiefs of Staff. Dictionary of Military and Associated Terms. (Washington: GPO, 1984), p. 293.

4. United States Department of State. Contemporary Soviet Propaganda and Disinformation--A Conference Report. (Washington: Department of State, 1987), p. iii.

5. United States Congress, 97th. 2d Session. House. Permanent Select Committee on Intelligence. "Soviet Active Measures." Hearings, July l982, p. 32.

6. Oliver Thomson. Mass Persuasion in History. (Edinburgh: Paul Harris, l977), p. 3.

7. Jock Haswell. The Tangled Web--The Art of Tactical and Strategic Deception. (Wendover, England: J. Goodchild, 1975), p. 59.

8. Frank Barnett, B. Hugh Tovar, and Richard H. Shultz, eds. Special Operations in United States Strategy. (Washington: National Defense University Press, 1984), p. 20.

9. The Art and Science of Psychological Operations, p. 5.

10. Haswell, pp. 9-20.

11. Linebarger, pp. 14-16.

12. Linebarger, p. 21.

13. James M. Read, Atrocity Propaganda 1914-1919. (New Haven: Yale University Press, 1941), p. 159.

14. Linebarger, p. 81.

15. Chapman Pincher, The Secret Offensive. (New York: St. Martin's Press, 1985), p. 2.

16. D.A. Volkogonov, The Psychological War. (Moscow: Progress, 1986), p. 37.

Page 2638 of 3957

17. United States Congress, pp. 34-35.

18. Bill Keller, "Moscow's Other Mastermind." New York Times Magazine, February 19, 1989, pp. 31-33.

19. Fred W. Walker, "Recent Changes in the Soviet Propaganda Machine." Journal of Defense and Diplomacy, May l988, pp. 47-50.

20. United States Congress, pp. 31-35.

21. United States Congress, pp. 39-43.

22. United States Congress, p. 87.

23. United States Congress, p. 170.

24. Pincher, pp. 60-61.

25. David Hertzberg, "Soviet Sponsored Clandestine Radio," in Joseph S. Gordon, ed., Psychological Operations--The Soviet Challenge. (Boulder, Colorado: Westview Press, l988), pp. 67-69.

26. Peter Kenez, "The Lesson of 007," in Gordon, pp. 77-85.

27. United States Information Agency. Committee to Oppose Soviet Active Measures. Soviet Active Measures in the Era of Glasnost: Prepared at the request of the U.S. House of Representatives, Committee on Appropriations. Washington, DC: USIA, 1988.

28. United States Congress, p. 49.

29. Charles Roetter, The Art of Psychological Warfare 1914-1945. (New York: Stein and Day, 1974), p. 128.

30. Roetter, pp. 130-131.

31. Roetter, pp. 136-137.

32. Linebarger, pp. 93-98.

33. Alfred H. Paddock, Jr., U.S. Army Special Warfare--Its Origins. (Washington: National Defense University Press, 1982), p. 100.

34. Paddock, p. 41.

35. Maurice A.J. Tugwell, "Soviet Propaganda in the Third World," in Gordon, p. 47.

36. Ron D. McLaurin, ed., Military Propaganda: Psychological Warfare and Operations. (New York: Praeger, 1982), pp. 282-285.

37. Barnett, Tovar, and Shultz, pp. 218-219.

Page 2639 of 3957

38. Barnett, Tovar, and Shultz, p. 237.

39. Alfred H. Paddock, "Military Psychological Operations and U.S. Strategy," in Gordon, pp. 145-164; Michael W. Totten, "U.S. Army Psychological Operations and the Army Reserve," in Gordon, pp. 188-209; and Sam C. Sarkesian, "Organizational Strategy and Low Intensity Conflicts, in Barnett, Tovar, and Shultz, pp. 261-289.

40. Paddock, in Gordon, pp. 146-148.

41. John M. Oseth, "Public Diplomacy and US Foreign Policy," in Gordon, p. 139.

42. Joseph Miranda. "Political Warfare: Can the West Survive?" Journal of Social, Political and Economic Studies, Spring 1985, p. 7.

Page 2640 of 3957

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COMPREHENSIVE DEFENSE: PSYCHOLOGICAL RESILIENCE IN MONGOLIA

by

Bayasgalan Lkhagvasuren

March 2022

Thesis Advisor: Douglas A. Borer
Co-Advisor: Shannon C. Houck

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
COMPREHENSIVE DEFENSE: PSYCHOLOGICAL RESILIENCE IN MONGOLIA

5. FUNDING NUMBERS

6. AUTHOR(S) Bayasgalan Lkhagvasuren

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Mongolia is bordered by two powerful nations that are vying for greater influence on the global stage. As a relatively smaller, democratic nation vulnerable to influence from these prominent neighbors, Mongolia faces increasing challenges in governance. One of the primary challenges is maintaining Mongolian independence, which requires national resilience and resistance in the face of external influence. Specifically, it requires psychological resilience in all sectors and all layers of society as a critical component for comprehensive defense. Mongolian national defense policies have relied on conventional military forces for decades, but those policies do not include the psychological preparation and involvement of the Mongolian population. This thesis looks to Nordic countries and Taiwan for insight. Norway, Finland, and Sweden maintain a comprehensive defense, or "total defense," approach that systematically invests in social and psychological resilience. This thesis asks, How can Mongolia achieve similar levels of national resilience? To address this question, this research uses NATO's comprehensive defense model as a framework to explore lines of effort Mongolia can invest in to enhance social and psychological resilience across all areas of society through education, information, and inclusion. Furthermore, the study makes recommendations on how to begin implementing programs to develop Mongolia's psychological resilience using existing resources.

14. SUBJECT TERMS
comprehensive defense, psychological resilience, whole-of-society, education, information, inclusion, social media

15. NUMBER OF PAGES
69

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Page 2643 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2644 of 3957

Approved for public release. Distribution is unlimited.

COMPREHENSIVE DEFENSE: PSYCHOLOGICAL RESILIENCE IN MONGOLIA

Bayasgalan Lkhagvasuren
Lieutenant Colonel, Mongolian Armed Forces
MMAS, The U.S. Army Command and General Staff College, 2018

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2022

Approved by: Douglas A. Borer
Advisor

Shannon C. Houck
Co-Advisor

Carter Malkasian
Chair, Department of Defense Analysis

Page 2645 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2646 of 3957

ABSTRACT

Mongolia is bordered by two powerful nations that are vying for greater influence on the global stage. As a relatively smaller, democratic nation vulnerable to influence from these prominent neighbors, Mongolia faces increasing challenges in governance. One of the primary challenges is maintaining Mongolian independence, which requires national resilience and resistance in the face of external influence. Specifically, it requires psychological resilience in all sectors and all layers of society as a critical component for comprehensive defense. Mongolian national defense policies have relied on conventional military forces for decades, but those policies do not include the psychological preparation and involvement of the Mongolian population. This thesis looks to Nordic countries and Taiwan for insight. Norway, Finland, and Sweden maintain a comprehensive defense, or "total defense," approach that systematically invests in social and psychological resilience. This thesis asks, How can Mongolia achieve similar levels of national resilience? To address this question, this research uses NATO's comprehensive defense model as a framework to explore lines of effort Mongolia can invest in to enhance social and psychological resilience across all areas of society through education, information, and inclusion. Furthermore, the study makes recommendations on how to begin implementing programs to develop Mongolia's psychological resilience using existing resources.

Page 2647 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2648 of 3957

TABLE OF CONTENTS

I. INTRODUCTION....1

II. THE LITERATURE REVIEW AND APPROACH....5
A. BRIEF OVERVIEW OF THE LITERATURE AND SIMILAR CASES....5
B. APPROACH....8

III. EDUCATION....11
A. YOUTH....12
B. GOVERNMENT ENTITIES....14
C. PRIVATE AND CIVIC SECTORS....16
D. MILITARY AND LAW ENFORCEMENT AGENCIES....20

IV. INFORMATION....21
A. SOCIAL MEDIA VULNERABILITIES....21
B. EXISTING POLITICAL DEBATES....23
C. PRESS....24
D. COUNTERMEASURES AND MONGOLIAN EXPOSURES....26
E. CIVIC-GOVERNMENT PARTNERSHIP ON INFORMATION....27

V. SOCIAL INCLUSION FOR YOUNG PEOPLE....29
A. WHAT IS SOCIAL INCLUSION?....29
B. WHY IS IT IMPORTANT?....29
C. WHAT ARE THE CURRENT EFFORTS?....30
1. National Identity and Shared National Values....31
2. National Language and Script....33
3. Mongolia and Nomadic Lifestyles....35

VI. CONCLUSION AND RECOMMENDATIONS....37
A. RECOMMENDATIONS....39
B. AREAS FOR FURTHER STUDY....43

LIST OF REFERENCES....45

INITIAL DISTRIBUTION LIST....53

Page 2649 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Example of Misinformation, a Fake Picture of Mongolian Allegedly Victimized in South Korea in 2021. 23

Figure 2. Flood and Storm Warning Information Distribution 40

Figure 3. Integrated Layered Defense 44

Page 2651 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CDH	*Comprehensive Defense Handbook*
CITA	Communication and Information technology Authority
LDF	Local Defense Forces
MFC	Mongolian Fact-Checking Center
MPP	Mongolian People's Party
NAMEM	National Agency of Meteorology and Environmental Monitoring
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Agency
OSCE	Organization for Security and Cooperation in Europe
PRC	People's Republic of China
ROC	Resistance Operating Concept
UNESCO	United Nations Educational, Scientific and Cultural Organization

Page 2653 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my sincere appreciation and deepest gratitude to my thesis advisors, Douglas A. Borer and Shannon C. Houck. Their valuable expertise and timely feedback helped me accomplish my objectives on time. They deserve my special thanks for their time, patience, helpful critiques, and comments.

I wish to express my special acknowledgment to Mr. Michael Stevens, Mrs. Julia McClenon, and Mr. Robert J. Shumaker for their support and recommendations, and for opening doors. Without the mentorship and support, this thesis would not have been completed.

Most of all, my greatest appreciation goes to my family (Batsaikhan Bolor, Yalaltbayar Misheel, and Margad Bayasgalan) for their gracious and kind support. This thesis and my educational experience at the Naval Postgraduate School would not have been possible without their support and reassurance. For that, I am everlastingly grateful.

Page 2655 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2656 of 3957

I. INTRODUCTION

> Conquering the world on horseback is easy; it is dismounting and governing that is hard.
>
> —Genghis Khan

Mongolia is bordered by powerful nations that are vying for greater influence on the global stage. As a relatively smaller, democratic nation vulnerable to influence from these prominent neighboring countries, Mongolia faces increasing challenges in governance. One of the primary challenges is maintaining Mongolian independence, which requires national resilience and resistance in the face of external influence. Throughout history many countries have faced similar dilemmas. When faced by potentially threatening neighbors often smaller states will band together in alliances, but also seek to strengthen their internal capacity to maintain independence. Such is the contemporary case in Europe, where the concept of "comprehensive defense" underscores European efforts at resilience and resistance.

The *NATO Comprehensive Defense Handbook* (CDH) defines comprehensive defense as "an official Government strategy, which encompasses a whole-of-society approach to protecting the nation against potential threats,"[1] the purpose of which is "developing the capability and willingness of all members of society to directly contribute to their safety, security and natural right to self-determination."[2] The core pillars of comprehensive defense include: social and psychological, economic and essential services, military, cyber, civil, and internal and border security. As part of the whole-of-society approach, Mongolia must pursue lines of effort within each of these pillars. Consistent with that overall goal, this research focuses specifically on social and psychological resilience.

---

[1] NATO Special Operations Headquarters, *NATO Comprehensive Defense Handbook*, Vol. 1. (Shape, Belgium: Quartier General, 2020), 15.

[2] NATO Special Operations Headquarters, 15.

Page 2657 of 3957

Mongolian national defense policies have relied on conventional military forces for decades, but those policies do not include the psychological preparation and involvement of the Mongolian population. Smaller nations in other parts of the world face similar challenges and in response have invested in comprehensive defense efforts. Nordic countries and Taiwan in particular offer important insights that might be useful for Mongolia. Nordic states' (Norway, Finland, and Sweden) comprehensive defense or "total defense" approach systematically invests in social and psychological resilience. Psychological resilience involves "developing and maintaining the will, resolve, and determination to overcome a national crisis and defend the nation … [as] an element of national pride and mutual respect which contributes to the strength and commitment to overcome a crisis and the faith that it will be overcome."[3] Nordic countries have seen success in this domain. For example, in a Gallup Poll in 2015, 74% of Finns said they would fight for their country, which was the highest percentage in Europe.[4] Moreover, according to a 2018 annual opinion poll, the most recent, by the non-governmental organization (NGO) "People and Defence," 81% of Norwegians support a military defense in the event of an attack, 79% want to retain conscription, and 72% are willing to participate in defense to the extent that they are capable.[5]

How could Mongolia achieve similar levels of national resilience? To examine this question, this research uses NATO's comprehensive defense model as a framework to explore lines of effort Mongolia can invest in to enhance social and psychological resilience across all areas of society through three lines of effort: (1) education, (2) information, and (3) inclusion. This research is focused on national defense, but it is by no means designed to only inform the Mongolian Ministry of Defense (MOD). Successful comprehensive defense planning requires a whole of government approach,

---

[3] Otto Fiala, *Resistance Operating Concept*, 1st ed. (Stockholm, Sweden: Swedish Defence University, 2019), 3.

[4] "WIN/Gallup International's Global Survey Shows Three in Five Willing to Fight for Their Country," Center for Public and Political Studies, May 7, 2015, https://www.gallup-international.bg/en/33483/win-gallup-internationals-global-survey-shows-three-in-five-willing-to-fight-for-their-country/.

[5] James Kenneth Wither, "Back to the Future? Nordic Total Defense Concepts," *Defense Studies* 20, no. 1 (January 2020): 67, https://www.tandfonline.com/doi/full/10.1080/14702436.2020.1718498.

one that requires an MOD involvement, but can only succeed if all elements of Mongolian governmental and civil society are involved.

Page 2659 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2660 of 3957

II. THE LITERATURE REVIEW AND APPROACH

> One must learn by doing the thing, for though you think you know it, you have no certainty until you try.
>
> —Sophocles, 400 B.C.

A. BRIEF OVERVIEW OF THE LITERATURE AND SIMILAR CASES

Historically, small nations have struggled to deter and resist aggressive superpowers. However, sometimes the weak and small have defeated the strong and large. Ivan Arreguín-Toft, a U.S. Army electronic warfare and signals intelligence veteran and University of Chicago PhD, argues that when large states attack with a "direct strategic approach and small states defend with an indirect strategy such as preplanned resistance, the weaker actor tends to win."[6] Defending against superpower nations like Russia and China, however, small nations would be likely to repeat the outcome of the Russia-Georgia War in 2008, which seemed to demonstrate that a minor country cannot stand up to a superpower in a conventional war. "The defeat of the Georgian Armed Forces, fighting alone against the superior Russian military, was a warning signal to other small nations, not just in eastern Europe, but around the world."[7] Arreguin-Toft would argue that Georgia lost because it attempted to fight the superior Russian force with conventional military means: a "direct approach." It might have fared better by taking an "indirect approach" that would have included guerrilla warfare.

In the article "The August 2008 War in Georgia: From Ethnic Conflict to Border Wars," Vicken Cheterian identifies that "Great powers' military and economic interests did not always work together with the UN [United Nations] and OSCE [Organization for Security and Cooperation in Europe] diplomatic solutions."[8] Cheterian illuminates three

---

[6] Ivan Arregun-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict" *International Security*, Vol. 26, No. 1 (Summer 2001), 105.

[7] Bayasgalan Lkhagvasuren, "Book Review: Resistance Operating Concept," *Small Wars Journal* (June 2021), https://smallwarsjournal.com/jrnl/art/book-review-resistance-operating-concept.

[8] Vicken Cheterian, "The August 2008 War in Georgia: From Ethnic Conflict to Border Wars," *Central Asian Survey* (July 2009): 165, https://doi.org/10.1080/02634930903056768.

Page 2661 of 3957

things those small nations need to understand in the modern world. These include (1) never provoke superpowers in a conventional way; (2) never depend on external supports; and (3) without civilian support "total defense" will be useless. Margus Kuul, of the Estonian Defense Force, establishes that "a strategy which combines civil resistance strategy and unconventional military action can be an effective component of a total defense capacity."[9] This means not only that Mongolian military personnel need to learn comprehensive defense policies, but the strategic decision-makers also need to understand the "total defense" concept and its key factors.

Since 2018, two important documents on irregular warfare have been published that highlight the need for improved understanding of comprehensive defense or total defense strategies as a means of national deterrence. The first is the *Resistance Operating Concept* (ROC) published by the Swedish Defense University.[10] The ROC is important to Mongolian comprehensive defense strategies because it serves as a master text for a whole-of-government approach to national self-defense. The second document is the *NATO Comprehensive Defense Handbook*, mentioned earlier[11] Volumes I and II of NATO's CDH are also important to understanding and developing comprehensive defense strategies. The CDH recommends a whole-of-society comprehensive defense and deterrence approach to small nations, and it contains a full training spectrum for asymmetric defense components. Both volumes create greater awareness about psychological resilience concepts and implementation of the key tenets of preparing for comprehensive defense.

The literature used for this research on psychological resilience as a comprehensive defense focuses not only on the ROC and NATO handbook, but also on related case studies about psychological resilience in the policies of Nordic states and Taiwan. With the exception of Denmark, the Nordic states (Norway, Finland, and Sweden) and Taiwan maintain conscription of their personnel , as does Mongolia. One of

---

[9] Margus Kuul, "Civil Resistance: An Essential Element of a Total Defense Strategy" (master's thesis, Naval Postgraduate School, 2014), 106, https://calhoun.nps.edu/handle/10945/42667.

[10] Fiala, Resistance Operating Concept, 13.

[11] NATO Special Operations Headquarters, *NATO Comprehensive Defense Handbook*, 3.

Page 2662 of 3957

the significant advantages of conscription is that it guarantees an adequate number of reserves in the military. Also, it boosts the national pride of most citizens. The Nordic states have incorporated psychological resilience into their strategy since 2014, and they are disclosing their national best practices with NATO countries. In terms of psychological resilience, the Finnish government defines it as "the ability of individuals, communities, society and the nation to withstand the pressures arising from crisis situations and to recover from their impacts."[12] This definition has demonstrated that Finnish national defense policies consider psychological resilience a crucial element. Finnish people believe "their country's strong public education system, long history of balancing Russia, and a comprehensive government strategy allow it to deflect coordinated propaganda and disinformation."[13] Meanwhile, the Sweden Defense Commission has proposed an "inquiry into psychological defence against propaganda and disinformation and distributed an information pamphlet to all households."[14]

In addition to the European countries discussed, Israel, Singapore, and Taiwan are practicing comprehensive defense policies successfully. The Republic of China (Taiwan), which is considered a nation, often depends on economic trade and shares (maritime) borders with the People's Republic of China (PRC), just as Mongolia does in East Asia. Beijing has been practicing economic sanctions in the last years in order to influence the Taiwanese government and business sectors. But Taiwan shows a positive example of social resilience on this matter. President Tsai Ing-wen's diversification strategy and alternative investment options for the economy resulted in "the general public becoming more aware of the downsides of dependence on bilateral trade and cautionary sentiment towards China's assertiveness."[15]

---

[12] Yhteiskunnan Turvallisuus, *Security Strategy for Society*, Finnish Government Resolution (Helsinki, Finland: The Security Committee, November 2017), 22. https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

[13] Reid Standish, "Why Is Finland Able to Fend off Putin's Information War?," *Foreign Policy* (March 2017), https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.

[14] Wither, "Back to the Future? Nordic Total Defense Concepts," 66.

[15] Christina Lai, "More than Carrots and Sticks: Economic Statecraft and Coercion in China–Taiwan Relations from 2000 to 2019," *Politics* (February 2021): 12, https://doi.org/10.1177/0263395720962654.

B. APPROACH

Most Mongolian national defense documents primarily focus on physical resilience; therefore, further research is needed to examine how small states can prepare and train their civil societies for psychological resilience as a pillar for a whole-of-society defense. While decision makers enhance Mongolian defense forces' readiness, they fail to persuade the Mongolian private and civilian sectors to participate as a component of asymmetric warfare. Namely, the existing defense strategy omits the potential for participation by civilian sectors as a practical strategic alternative that could strengthen Mongolian deterrence capacity.

To fill these gaps, thesis explores how CDH would look in the development of the Mongolian psychological resilience. The study therefore focuses on three lines of effort: (1) education, (2) information, and (3) inclusion. First, this thesis identifies education programs promoting the whole-of-society approach to the Mongolian population, including the public, private, and civilian sectors for enhancing their resilience capabilities. Second, the research explores information programs (e.g., digital literacy) that help ensure society is accurately informed about current conditions or trends that may affect national safety or security. This is a critical problem. According to January 2021 estimates, there are 2.60 million social media users in Mongolia.[16] Linda Sanchez, U.S. special rapporteur to NATO's Committee on Democracy and Security, highlights that "disinformation and propaganda contribute to heightening the polarization of societies and increasing dissatisfaction with democracy."[17] Many Mongolians understand that disinformation and propaganda are used and yet citizens receive and believe widely disseminated false and misleading narratives from domestic and external ill-intentioned actors. For instance, the people who have no basic facts about internet security are targeted by cybercriminal groups. According to local security authorities, "Police in the Mongolian capital of Ulaanbaatar have apprehended 800 Chinese citizens and confiscated

[16] Simon Kemp, "Digital 2021: Mongolia," Datareportal, accessed October 17, 2021, https://datareportal.com/reports/digital-2021-mongolia.

[17] Linda Sanchez, Bolstering the Democracy Resilience of the Alliance Against Disinformation and Propaganda," Preliminary Draft Special Report to NATO Committee on the Civil Dimension of Security (Brussels, Belgium: NATO Parliamentary Assembly, March 2021), 1.

Page 2664 of 3957

hundreds of computers and mobile phone SIM cards as part of an investigation into a cybercrime ring."[18] Therefore, this thesis further identifies the Mongolian population's social media vulnerabilities, including existing political debates and social grievances, and external threats facing the nation (e.g., weaponized information and other psychological tools used to influence Mongolia). Understanding the information environment in Mongolia will inform ways for developing an underlying social resilience. Third, this thesis examines ways Mongolia can foster inclusion across all sectors of society. Inclusion, or group belongingness, is "a fundamental human"[19] need, and satisfying this need as a valued Mongolian citizen has benefits beyond fulfilling the individual's need to belong—it also strengthens the group itself by creating members that "strongly identify with the group's values and goals."[20] Many initiatives that promote societal inclusion overlap with the education and information lines of effort (e.g., bridging the digital divide; teaching Mongolian language, history, and traditions), but research suggests some additional avenues. Some of these include "inclusive leadership styles"[21] and the use of national narratives that promote unity and strength. Arie Kruglanski, distinguished social psychology professor at the University of Maryland, College Park, suggests governments should create opportunities for citizens to pursue "significance-bestowing occupations" and "create organizations such as the Peace Corps and Doctors Without Borders that take advantage of young people's desire to be idealistic and to do something for their country."[22]

Finally, this thesis emphasizes the role of partner nations in supporting Mongolian national psychological resilience and future recommendations for Mongolians on psychological resilience. To this end, in recent years the Mongolian government has been

---

[18] "Mongolia Arrests 800 Chinese Citizens in Cybercrime Probe," Reuters, 2019, https://www.reuters.com/article/us-mongolia-crime-china-idUSKBN1XA0NW.

[19] Roy. F. Baumeister and Mark. R. Leary, "The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation," *Psychological Bulletin* 117, no. 3 (1995): 497.

[20] H. Tajfel and J.C. Turner, The Social Identity Theory of Intergroup Behavior, Political Psychology: Key Readings (Chicago: Hall Publishers, 1986), 14.

[21] Lynn M. Shore and Beth G. Chung, "Inclusive Leadership: How Leaders Sustain or Discourage Work Group Inclusion," SAGE Publishing (May 2021), DOI: 10.1177/1059601121999580.

[22] Zara Greenbaum, "5 Questions for Arie W. Kruglanski," American Psychological Association, April 2018, www.apa.org/monitor/2019/04/conversation-kruglanski#.

pursuing what is known as the "Third Neighbor Policy." This multi-lateral approach seeks to build effective ties with actors in states that do not physically border on Mongolia. It is believed that doing so will help further stabilize Mongolia.

Page 2666 of 3957

III. EDUCATION

> Education is the basic tool for the development of consciousness and the reconstitution of society.
>
> —Mahatma Gandhi

According to the NATO handbook, "national resilience begins with the individual."[23] Therefore, enhancing individual resilience is one of the challenging objectives for any country regarding comprehensive defense policies. Mongolian defense law declares "the basis of Mongolian defense policy is based on participation of government entities and all citizens."[24] Also, the law itself describes the Government of Mongolia as being tasked to train all citizens, as well as government entities, and non-governmental agencies to defend the nation. In this way, the existing defense policy is remarkably conventionally militarized, and the law does not include a psychological defense policy or stipulation for programs against disinformation, misinformation, fake news, and propaganda.[25]

This vulnerability is not without consequence. Indeed, Mongolia has been a "testing space" for misinformation and disinformation for other nations. According to an article in *Poynter*, Battsetseg Enkhtaivan, lead fact-checker of the Mongolian Fact-Checking Center, and her family encountered misinformation stating that "COVID-19 vaccines were just experimental Chinese treatments being tested on Mongolians without proper safety checks."[26] After hearing that misinformation her mother and sisters refused to get vaccinated, and they got sick with COVID-19. The article goes further by explaining that although "the practice and impacts of misinformation are not new to

---

[23] NATO Special Operations Headquarters, 25.

[24] "Батлан хамгаалах тухай" Монгол Улсын хууль, [Defense Law], The State Great Khural - Parliament of Mongolia, October 06, 2016, https://legalinfo.mn/mn/detail/12122.

[25] Sanchez, Bolstering the Democracy Resilience of the Alliance Against Disinformation and Propaganda, 2.

[26] Harrison Mantas, "The Mongolian Fact Checking Center Fights Misinformation in a Country where the Word Doesn't Exist," *Poynter,* August 2021, https://www.poynter.org/fact-checking/2021/the-mongolian-fact-check-center-fights-misinformation-in-a-country-where-the-word-doesnt-exist/.

Page 2667 of 3957

Mongolia, the concept can be difficult to translate for everyday people."[27] It is just one of the latest examples of misinformation in Mongolia, and it demonstrates that Mongolian social resilience has not fully developed. Part of the solution requires digital literacy education across all sectors of society.

Just as the NATO CDH outlined that the relevant learning audiences are divided into four groups, this thesis also proposes four groups of audiences within Mongolia: 1) youth; 2) government entities; 3) private and civic sectors; and 4) military and law enforcement agencies. These audience groups are described in the following sections.

A. YOUTH

The Mongolian population trends younger. As of 2019, "the proportion of children, adolescents and young adults was 35 percent."[28] As the future of Mongolia, the youth's social and psychological resilience education is a crucial part of comprehensive defense policy. Research suggests "Mongolian youth spend an average of 5–6 hours every day on social media,"[29] making them especially vulnerable to misinformation and disinformation. Therefore, investing in digital literacy programs is key.

Like other successful digital literacy efforts, it is critical to educate youth "to explore digital safety, digital privacy, digital presence, online communication."[30] Notably, Finland and Taiwan have focused on media literacy for youth, and the primary education system in those countries includes relevant training on media literacy. These efforts include the Taiwanese *Curriculum Guidelines of 12-Year Basic Education* (since 2014), which teaches students "to effectively use technology, information, and media of all types, develop competencies related to ethics and media literacy, and develop the ability to analyze, speculate about, and criticize human's relationships with technology,

---

27 Mantas, "The Mongolian Fact Checking Center."

28 "Youth in Mongolia," *Amicus Travel* (blog), August 13, 2019, https://www.amicusmongolia.com/youth-in-mongolia.html.

29 "Сошиал медиа хэрэглээ Монголд," [Social media usage in Mongolia], Digital and Inbound Marketing Agency, January 2020, https://dima.mn/2020/01/14/сошиал-медиа-хэрэглээ-монголд/

30 "Digital Literacy Essentials," Boys & Girls Clubs of America, accessed November 16, 2021. https://www.bgca.org/programs/education/digital-literacy-essentials.

Page 2668 of 3957

information, and media."[31] In a 2019 study of Europe, Finland ranked first in media literacy.[32] Mongolian primary schools, and even more importantly, Mongolian universities and colleges did not have this kind of program in their curriculums until most recently. Hence, many youths have become victims of misinformation and crimes on social media due to a lack of media literacy educations.

Out of necessity, the Mongolian National Police has conducted a nationwide campaign called the "unfriend" movement on Facebook to protect teenagers from cybercrimes and abuses. As a result, parents strengthened control over children's use of social media, and the campaign urged social media users to prevent potential risks. Thus, it is considered an effective campaign oriented not only to improving teenagers' media literacy but also that of most Mongolians who have now obtained basic knowledge about the risks associated with social media platforms.

Mongolian youth are the driving force of next generation; thus, they should have comprehensive and solid education on psychological resilience. To start with, media literacy education should begin in secondary schools for teens and those education programs can be designed and delivered in conjunction with expert NGOs. For example, the Mongolian Fact-Checking Center could cooperate with schools and expand their practice across Mongolia. What is more, the governmental and non-governmental organizations can engage with teenagers in boy scouts, sport communities, clubs for life skills, science and health associations, and book clubs regarding how to spot fake news on social media platforms. For instance, Lut-Ochir Vanganjil is an active member of the National Network for Media and Information Literacy in Mongolia and is enthusiastic about sharing the critical use of media and information among children and youths. "Together with his colleagues and fellow members of the national network, Lutaa produced and disseminated 17 video tutorials in 2020, to provide knowledge on essential topics related to access to information, critical and responsible use of information, as well

---

[31] Ministry of Education, "Curriculum Guidelines of 12-Year Basic Education" (official government training curriculum, Taipei, November 2014), 8.

[32] Open Society Institute Sofia, "Finding of the Media Literacy Index 2019: Just Think about It," November 2019, https://osis.bg/?p=3356&lang=en.

as evaluation of information."[33] His initiative was supported by UNESCO and made significant progress in the last two years in Mongolia.

In addition, the Ministry of Education and Science, the Communications and Information Technology Authority (CITA), and 'Faro Foundation Mongolia' (an NGO) agreed to jointly organize in collaboration with Facebook a series of webinars, training, and content on digital literacy, and involve 10,000 people in 2021. The program is labeled "We Think Digital Mongolia" and "aims to teach people how to navigate their privileges and obligations in today's evolving digital space, how they should decipher and share information online, and most importantly, how they should interact with other people in online communities."[34]

B. GOVERNMENT ENTITIES

The Government of Mongolia's five-year mission to build a digital nation is worth noting. A digital nation's mission objectives are to enhance the information technology (IT) industry and digital literacy, as well as highlight personal data protection and cybersecurity issues. For instance, "to support the Government of Mongolia's commitment to become a digital nation, the Accelerator Lab is working with the Communication and Information Technology Authority to develop a National Program on supporting the digital skills and education."[35] Nevertheless, this program "focuses on specific activities to improve the digital access, fill in the digital literacy gaps of the vulnerable groups including people with disabilities, elderly, rural and low-income households",[36] it's a good start.

At present, the Government of Mongolia does not have an agency or organization to address damaging misinformation or disinformation such as the Taiwanese

---

[33] "Lutaa's Journey for Media and Information Literacy in Mongolia," UNESCO, May 2021. https://en.unesco.org/news/lutaas-journey-media-and-information-literacy-mongolia.

[34] "Facebook Launches 'We Think' Digital Program in Mongolia to Cultivate Responsible Digital Citizens," News.mn, April 2021, https://news.mn/en/795665/.

[35] "Bridging the Digital Divide in Mongolia," UNDP Mongolia's Accelerator Lat Team, April 2021, https://www.mn.undp.org/content/mongolia/en/home/blog/2021/bridging-the-digital-divide-in-mongolia.html.

[36] "Bridging the Digital Divide in Mongolia."

Page 2670 of 3957

Disinformation Coordination Team, whose mission "includes drafting policies, interacting with major social media platforms, and leading interagency discussion such as the Ministry of Justice, the Ministry of Education, the Ministry of Interior, the National Communication Commission, to name a few."[37] Dulamkhorloo Baatar, founder and editor-in-chief of the Mongolian Fact-Checking Center has mentioned that "we don't have a Mongolian word for (misinformation), and when you mistranslate that, it has a negative impact on the awareness-raising we're trying to do."[38]

The Government of Mongolia is establishing the Ministry of Cyber and Cyber Academia in Mongolia in 2022 to educate and train personnel of the national agencies and civic organizations as well as citizens. That effort is needed to bolster agencies' interoperability, especially for the subject of social resilience. This challenging effort is made even more difficult by a disengagement between the experts and policymakers who develop nationwide projects and programs. According to the study "Assessing E-Resilience in Kazakhstan, Kyrgyzstan and Mongolia," "in the case of Mongolia, expanded investments and support for fixed broadband may be required to achieve advanced e-resilience and e-readiness of terrestrial networks."[39] The assessment goes further by suggesting "policymakers can consider the following factors: policy regime; regulatory framework; regular trainings for experts; national projects; funding system; and public events or campaign."[40] Compared with other government entities of Mongolia, the Ministry of Defense and the Ministry of Justice and Interior Affairs pay more attention to national and social resilience nationwide. Thus, those two ministries might be good choices to lead social resilience education programs, along with other government agencies in Mongolia. As the NATO CDH emphasized, "education programs are not intended to simply inform decisions or encourage support, but instead to impart

---

[37] Shih-Shiuan Kao, *Taiwan's Response to Disinformation: A Model for Coordination to Counter a Complicated Threat*, NBR Special Report no. 93 (Washington, DC: The National Bureau of Asian Research, September 2021), 5.

[38] Mantas, "The Mongolian Fact Checking Center."

[39] Aida Karashanova and Elena Dyaknova, "Assessing E-Resilience in Kazakhstan, Kyrgyzstan and Mongolia," (Working paper, Asia-Pacific Information Superhighway Series no. 03, 2021), 20.

[40] Karashanova and Dyaknova, "Assessing E-Resilience in Kazakhstan, Kyrgyzstan and Mongolia," 27.

Page 2671 of 3957

knowledge that stakeholders can translate into tangible skills and action."[41] Furthermore, education programs can take the form of situation-based table-top exercises, open seminars with foreign experts, and subject-matter expert exchange programs with other nations. Table-top exercises may sound like a military method, but exercises can be one of the efficient educational program formats for civilian participants who do not already have national level resilience. "Table-top exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation."[42] Also, those exercises are low-cost but highly effective for assessing emergency plans, responses, and more importantly, clarifying roles and responsibilities for other civilian government entities. For example, "Gobi Wolf," the disaster management table-top exercise, is "aimed at enhancing abilities to respond and recover from emergency situations, disasters and hazards that occur in Mongolia, training corresponding disaster and emergency personnel and sharing experiences with experts of other countries."[43] The main purpose of this exercise was a wider understanding of the concept of crisis management by all agencies and organizations across all levels of government.

C. PRIVATE AND CIVIC SECTORS

As the NATO's CDH stressed, "achieving military and civil preparedness in comprehensive defense requires close collaboration across all sectors of society."[44] Furthermore, "the majority of the population is contained in the two non-governmental categories, the private and civic sectors, sometimes referred to as the 98% of society."[45] After the Warsaw Summit of 2016, NATO member states decided "civil preparedness is a central pillar of Allies' resilience and a critical enabler for Alliance collective

41 NATO Comprehensive Defense Handbook, 27.

42 "Exercises," Ready, last updated October 12, 2021, https://www.ready.gov/exercises.

43 "Mongolia-U.S. Joint Disaster Management Exercise 'Gobi Wolf-2019' Underway," Montsame, September 16, 2019, https://montsame.mn/en/read/20077.

44 NATO Special Operations Headquarters, 20.

45 NATO Special Operations Headquarters, 11.

defense."[46] Accordingly, NATO military forces count on civilian assets such as transportation and communications in peacetime and crises situations. Those actions will strengthen collaboration between civil-military and civic-government relationships. Although Mongolia is not a member of NATO, civil preparedness is the main contributor in matters of national resilience even in non-member countries. In this regard, "a renewed effort to broaden and strengthen pro-democratic values and civic education through a range of educational and other civil society organizations is necessary."[47]

The government's effort to strengthen social resilience across the nation has mostly failed the emerging civic-government partnership. On top of that, institutionalized collaboration among the government entities, civic organizations, and the private sector is not fully functional in Mongolia. Compared to other countries, the inadequate civic-government partnership was exposed more than ever during the COVID-19 pandemic in Mongolia. As a result, some civilian NGOs refused to support the government enforcement of vaccinations, and similarly, many private companies went out of business due to the lack of government support for them. In general, the Government of Mongolia is losing the trust of people in all sectors.

It should be emphasized that educating every member of society for whole-of-society defense policies in democratic countries is often difficult to accomplish. More precisely, "with the exception of conscription, members of the private and civic sectors cannot be compelled to participate in defense training beyond that which is included in the nation's public education curriculum or laws governing business."[48] Under such conditions, it is important to consider using all possible education delivery programs to reach the civic and private sectors. In fact, "the civic sector will decide what course the nation follow";[49] thus, "they can communicate their position explicitly, through various

---

46 "Warsaw Summit Communiqué," NATO, July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

47 J.D. Maddox, Casi Gentzel, and Adela Levis, *Toward a Whole-of-Society Framework for Countering Disinformation* (New York: Modern War Institute at West Point, October 2021), https://mwi.usma.edu/toward-a-whole-of-society-framework-for-countering-disinformation/.

48 NATO Special Operations Headquarters, *NATO Comprehensive Defense Handbook*, 51.

49 NATO Special Operations Headquarters, 102.

formal mechanisms, or implicitly by demonstrating disinterest."[50] Consequently, a strong partnership with the civic sector is a key factor in building psychological resilience.

A "civic-government partnership" could be designed for social resilience as follows. First, enhance or promote civic sectors nationwide, including NGOs such as Mongolian Fact-Checking Center (MFC). Even though the Government of Mongolia cannot afford to provide this kind of support and promotion of policies for civic organizations at this moment, it can be one of the areas for collaboration between the government and civic sectors in coming years. For instance, the Communication and Information Technology Authority (CITA) is the regulatory agency of the Government of Mongolia, and the organization itself can enhance and promote any digital literacy education programs in the civic sector. More specifically, CITA can support Mongolian Fact-Checking Center activities on behalf of the government and help expand their practice across the country. According to the MFC, they "train some of Mongolia's 500 media organizations in basic fact-checking"[51] by themselves, and if CITA supports it, those numbers could be doubled. In addition, International Fact-Checking Network certification will enable MFC to team up with social media platforms such as Facebook and Twitter so MFC could work as a bridge between the government and those social media platforms. Nevertheless, collaboration with social media platforms has limitations, and it requires a certain degree of cooperation. According to experts, the Taiwanese Fact-Checking Center is regarded as a pioneer center among other nations. Dr. Yuan-Hui Hu, one of its founders, describes is purpose in these terms: "we are not asking a platform to act as the 'arbiter of truth' who 'controls the content of speech' but rather to be a 'basic online garbage janitor' who cleans up harmful contents."[52]

Taking everything into consideration, if the government takes steps to enhance and promote the private and civic sectors, it does not mean they work as the government's mouthpiece. In terms of enhancing and promoting the civic sector, the

---

[50] NATO Special Operations Headquarters, 102.

[51] Mantas, "The Mongolian Fact Checking Center."

[52] Kao, "Taiwan's Response to Disinformation: A Model for Coordination to Counter a Complicated Threat," 15.

government would make certain decisions/policies to promote the civic sector and support it in all means, while the civic sector maintains its distance from the government and works independent of the government. For instance, the Mongolian NGO law promulgated in 1997 defined NGOs as "not-for-profit, self-governing organizations operating independently from the state and established voluntarily by citizens or by legal persons other than state legislative, executive, and judicial bodies, on the basis of their individual or social interests and opinions."[53] This law focuses on the legal status and the activities of NGOs. But the law itself does not include government support for and cooperation with NGOs. Hence, Mongolian laws and policies regarding the civic and private sectors need to be updated and streamlined, but not at the expense of ensuring the essential freedoms of assembly and open expression.

Second, the government needs to design and promote intensive educational programs on social resilience for NGOs, clubs, civic groups, and private companies. Those programs must focus nationwide, with particular attention on emerging civil societies and private companies and must be conducted by either governmental (such as CITA) or non-governmental organizations (for instance, the MFC). There have been many civil society organizations such as NGOs, clubs, and community groups in Mongolia, not all of them have worked actively. For example, the most well-known and active NGOs are the Mongolian Youth Federation, the Mongolian Women's Federation, the Mongolian Elders Association, the Mongolian National Federation of Disabled People's Organizations, and the Mongolian National Olympic Committee, etc. In general, those NGOs have higher capital, human resources, and also have networks of offices nationwide. Therefore, intensive educational programs need to develop and adjust with those civic organizations. When it comes to the private sector, the economy of Mongolia is attached to agriculture, mining, and construction. Therefore, these areas are considered as the most prominent and influential among other private industries. In fact, "opinions and interests will vary widely among members of the private sectors."[54] So, social

---

[53] "Төрийн бус байгууллагын тухай" Монгол Улсын хууль, [Non-Governmental Organization Law], The State Great Khural - Parliament of Mongolia, January 31, 1997, https://legalinfo.mn/mn/detail/494.

[54] NATO Special Operations Headquarters, *NATO Comprehensive Defense Handbook*, 103.

resilience education "cannot be tailored to every company, or even every type of company, but as many interests as possible should be accounted for when seeking support."[55] Finally, education programs for the civic and private sectors are most important because "the social and psychological pillar within the comprehensive defense framework further reinforces social harmony and civic responsibility."[56]

D. MILITARY AND LAW ENFORCEMENT AGENCIES

While the Armed Forces of Mongolia enhances defense force readiness, it fails to deal with unconventional or hybrid warfare from external sources, namely in the information and cyber domain. The Government of Mongolia has passed the bill for the establishment of Cyber and Special Forces Command in 2020, through which the Cyber command would deal with all kinds of cyber issues including disinformation and misinformation. But the command is only dedicated to Armed Forces (conventional and special forces) service members. Therefore, psychological resilience education programs can be situation-based table-top exercises, open seminars that involve other law enforcement agencies such as Border troops, the National Emergency Management Agency (NEMA), National Police and Intelligence services, and subject-matter expert exchange programs with other nations. Compared to civilians, uniformed service members have established many regulations, norms, and codes of conduct related to social media or information exchange in the digital domain. Consequently, their education programs should focus more on security awareness regarding disinformation, weaponized information, subjects of cyber and operation security.

---

55 NATO Special Operations Headquarters, 103.

56 NATO Special Operations Headquarters, 102.

Page 2676 of 3957

IV. INFORMATION

> Social media has created a historical shift from the historically powerful to the historically powerless. Now everyone has a voice.
>
> —Facebook COO Sheryl Sandberg

A. SOCIAL MEDIA VULNERABILITIES

As the nature of modern warfare changes, so too does the way nations strategize and operate across the spectrum of conflict and competition. This has become increasingly complex in the present information era where we continue to see rapid technological developments in the information warfare space. In the case of Mongolia, the two powerful states on its northern and southern borders are highly advanced actors in the area of social media capability. As a result, Mongolia is technically highly vulnerable to coercive influence. However, for over a hundred years, in its role as a geographic buffer state, Mongolia has served a very useful purpose for both Russia and China. Mongolia does not threaten its neighbors and generally pursues a policy of neutrality. However, as China's power increases, and tensions between Russia and the West rise, it is a prudent policy for Mongolia to strengthen its resilience to malign influence from other actors in cyberspace.

Freedom of information is a foundational principle in democratic societies. Like other democratic countries, the Government of Mongolia does not control its domestic information environment. It upholds the principles of information freedom. Indeed, Mongolian national security policies encourage the "continuity of the Mongolian state governance and national unity, support for political parties, civil society, free press and media, individual liberties as well as safeguarding public order and social stability."[57] While it is a valuable democratic freedom, by promoting inclusive individual liberties,

---

57 "National Security Concept of Mongolia," Ministry of Foreign Affairs of Mongolia, (November 2015) https://mfa.gov.mn/en/documentation/55280/.

Page 2677 of 3957

"democracies are more vulnerable to weaponized information,"[58] which is defined as "a message or content piece that is designed to affect the recipient's perception about something or someone in a way that is not warranted."[59] Of note, not all the weaponized information is false. Some information can be true, but the timing of release or targeting of people can be harmful. For instance, a 13-year-old Mongolian girl who was studying in a high school in South Korea was beaten for six hours by four Korean female high school students, forced to drink alcohol, and locked in a room. "Two of the assailants were handed over to the prosecution on charges of gang violence, but the others were juveniles … under the age of 14; therefore, they escaped criminal punishment."[60] The incident happened in July 2021 in South Korea, but the news reached Mongolia in late November 2021 and triggered a mass anti-Korean movement on social media. This incident also garnered misinformation on Facebook—a fake picture of the Mongolian girl was shared by 200,000 people and had over a million views.

---

[58] Nicholas J. Kane, "Defense against Weaponized Information: A Human Problem, Not Just a Technical One," *InterAgency Journal* 10, no. 3 (2019): 58.

[59] "Weaponization of Information," European Center for Populism Studies. (August 2017), https://www.populismstudies.org/Vocabulary/weaponization-of-information/.

[60] "Four Teenage Girls Assaulted a Mongolian Girl for Six Hours with Her Hands and Legs Tied up," Allkpop, November 2021, https://www.allkpop.com/article/2021/12/tw-cw-four-teenage-girls-assaulted-a-mongolian-girl-for-six-hours-with-her-hands-and-legs-tied-up.

Figure 1. Example of Misinformation, a Fake Picture of Mongolian Allegedly Victimized in South Korea in 2021.[61]

In reality, the girl in the picture is not a victim in South Korea; this fake picture was created by someone intentionally. Nevertheless, this misinformation strengthened the spread of the news all over Mongolia. As a result, the mass response on social media impacted South Korea and Mongolian diplomatic ties and prompted national government-level discussion. The incident serves as a powerful example of how social media news significantly influenced the Mongolian population nationwide.

B. EXISTING POLITICAL DEBATES

Though Mongolia enjoys a democratic system of governance, this system does not work as smoothly in Mongolia as it does in other democratic countries. Part of the reason for this is historical. After a bloodless revolution in 1990, multiple parties entered the Mongolian political system, but only the two dominant parties debated with each other in the last 30 years. The Mongolian People's Party (MPP, left-wing) and

[61] Source: "Mongolian Victim Was Beaten for 6 hours, but the Other Side Was Denied and Tried to Evade Punishment," *Monopolnews*, accessed November 28, 2021, https://monopolnews.com/5230/.

Democratic Party (DP, right-wing) are the two powerful political parties that hold influence nationwide, usually holding power alternately at government and parliament levels. Moreover, the Mongolian people's voting tendencies are not stable in each election session; political support tends to shift between the two parties. For instance, in the last parliamentary election (2020), the MPP won 62 out of 76 seats in parliament,[62] and with the large majority of parliament, MPP determines the government policies. Then again, Mongolian people were divided into two groups as usual—supporters and opponents of the government. There is no doubt that this kind of existing political debate will continue as long as two dominant parties hold so much influence over the Mongolian population. To sum up, the relentless political division negatively impacts the information environment undesirably. This strong rivalry influences the press and social media, and some politicians use these avenues as weapons to influence to the mass population.

C. PRESS

After the successful establishment of a democratic system in Mongolia in 1990, freedom of speech and of the press is guaranteed in the national constitution. Consequently, enhancing the independence and diversity of the media, educating the professionals, and fact-checking the press are a particularly crucial priority to Mongolia. Domestic press organizations play significant roles in social and psychological resilience. Namely, it is essential to any nation to "promote journalistic standards to safeguard independent, fact-based, investigative journalism and establish and bolster fact-checking standards and norms."[63]

At this time, Mongolia, as a small nation has over 500 officially registered press organizations, and Mongolia was ranked 68th out of 180 countries in the Reporters

[62] Wikipedia, s.v. "2020 Mongolian legislative election," last modified February 14, 2022, https://en.wikipedia.org/wiki/2020_Mongolian_legislative_election

[63] Maddox, Gentzel, and Levis, "Toward a Whole-of-Society Framework for Countering Disinformation."

Page 2680 of 3957

without Borders' "2021 World Press Freedom Index."[64] Based on the Resistance Operating Concept, one promising way to counter misleading information and external influences while building psychological resilience is by a "public diplomacy campaign using truthful and independent media."[65] Reliable media sources can clarify current concerns and expose issues while bolstering national psychological resilience.

Compared to other countries in the region, Mongolia has some minor issues with the press. Essentially, the Mongolian press is inadequate on fact-checking or verification of any information. Thus, media or press may amplify misleading information such as disinformation (which represents "deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead"[66]), misinformation ("false or misleading information spread without the intention to deceive"[67]), and fake news. For example, the press provided misinformation when Mongolian peacekeepers returned from a UN peacekeeping mission in South Sudan in late November 2021. Specifically, some press outlets titled the news as "Mongolian peacekeepers come from South Africa," which caused mass panic and fear on social media due to South Africa's noticeable new Covid-19 (omicron) cases just discovered at the same time. Consider another example of the press disinforming the public through Mongol TV. They distributed fake news regarding McDonald's opening a branch in the country in 2013 even though there had not been any discussion about McDonald's opening a branch in Mongolia, and it never did. The planted disinformation was picked up and disseminated by nine major media outlets due to payments they received, and none of them verified the information for themselves. Nomin Chinbat (at present, the Minister of Culture), head of

64 "2021 World Press Freedom Index," Reporters without Borders, accessed November 29, 2021, https://rsf.org/en/ranking.

65 Fiala, *Resistance Operating Concept*, 196.

66 "NATO's Approach to Countering Disinformation: A Focus on COVID-19," NATO, July 2020, https://www.nato.int/cps/en/natohq/177273.htm.

67 Thomas Colley, Francesca Granelli, and Jente Althuis. "Disinformation's Societal Impact: Britain, Covid, and Beyond," *Defence Strategic Communications* (July 2020). https://stratcomcoe.org/publications/disinformations-societal-impact-britain-covid-and-beyond/36.

Mongol TV, emphasizes "They won't check the facts, they'll just be interested in getting paid to run the story."[68]

D. COUNTERMEASURES AND MONGOLIAN EXPOSURES

There are those who argue that "false news spreads more than the truth because humans, not robots, are more likely to spread it."[69] In practice, the misleading information spreads throughout social media, which is then amplified by unknowing digital participants and popular social influencers who do not check the validity of the news. This kind of misleading information threatens one of the pillars of comprehensive defense: social and psychological resilience.

To mitigate this threat, some Western countries have developed approaches to counter misleading information. First, some NATO member states have adopted laws within their legal framework and set up countermeasures to address the spread of misleading information. For example, Germany adopted the Network Enforcement Act in 2017 which made "more than two million users liable for fines of up to €50 million for the failure to delete 'obviously illegal' content within 24 hours of its publication."[70] According to experts, effective building of resilience is not only focused on digital literacy, but also to "continue to pursue policy and regulation of the commercial sector with regard to protection of citizens' privacy."[71]

Currently, Mongolia has not adopted laws or regulations to guard against misleading information, except one part of the criminal law of Mongolia emphasizes the penalty of spreading fake information. The legal penalty for spreading fake information is not robust enough. It is worth mentioning the law itself does not define the term "fake information" and does not classify misleading information such as disinformation and

---

[68] Gavin J. Blair, "Mongolian TV Network Exposes Media Corruption with Fake Story about McDonald's," *The Hollywood Reporter,* December 2013, https://www.hollywoodreporter.com/news/general-news/mongolian-tv-network-exposes-media-665859/.

[69] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (2018): 1146.

[70] Sanchez, Bolstering the Democracy Resilience of the Alliance against Disinformation and Propaganda, 9.

[71] Kane, "Defense against Weaponized Information: A Human Problem, Not Just a Technical One," 60.

misinformation. In addition, the law itself does not address overseas hostile information activities. While the digital nation is appealing in Mongolia, it is also important to bolster the legal bases against spreading misleading and other malicious information. In addition, national law enforcement agencies should "strive to regain and retain the initiative in the information environment"[72] to maintain the national society's stability.

Adopting domestic laws and regulations against the dissemination of misleading information is not generally accepted in Western countries due to freedom of expression, yet some democratic nations are shifting in this direction. For instance, the Latvian Ministry of Culture has initiated financial support (since 2017) for "investigative journalism, deconstruction of lies, development of media literacy, media criticism, support for regional media, and a communication campaign called 'Media are not comedy' against the dissemination of disinformation."[73] These two approaches of Western countries to stop the spread of misleading information illustrate efforts that Mongolia could adopt to address its vulnerabilities in the information environment.

E. CIVIC-GOVERNMENT PARTNERSHIP ON INFORMATION

No single press organization and no simple solution can counter misleading information, and no country is immune from it. Like civic or private organizations, the press organizations prefer to keep a distance from government agencies to maintain their independence. Possibly the best way to understand the need for a whole-of-society framework for countering misleading information today is by understanding the cooperation and collaboration of governmental and non-governmental organizations, as well private and civic ones. Then, the Government of Mongolia should cooperate or collaborate with press organizations to combat misleading information by employing supportive policies or providing financial support. Like Latvia, the Mongolian Ministry of Education and the Ministry of Culture can promote and offer professional educational programs to journalists, focusing specifically on fact-checking information. In addition,

---

[72] Kane, 60.

[73] Klinta Ločmele, "Media literacy in Latvia: The Ministry of Culture's 6 strands," *Media and Learning* (January 2019), https://media-and-learning.eu/type/featured-articles/media-literacy-in-latvia-the-ministry-of-cultures-6-strands/.

government entities should only work on the development of professionals and should not curtail the freedom of expression and the independence of media.

Regarding the press-government relationship that usually does not work smoothly in any country, the Mongolian Press Institute is among the most important. The Press Institute has been "the leading non-government organization to work with journalists and media users to enhance the skills and knowledge of media in society and as a result, has contributed to the vibrant political, social and economic debate that exists in the public today."[74] Also, the Press Institute enjoys a successful collaboration with several international press and aid organizations, so the institute can bring experts from overseas to advise on how to combat misleading information. If the Government of Mongolia can establish a civic-government partnership with the Press Institute of Mongolia effectively, then the institute could work as a bridge between the government and Mongolia's press organizations. On the other hand, the Government of Mongolia can support and fund the creation of civic society organizations which counter misleading information through efforts like the Estonian website '*propastop'* or the Ukrainian website StopFake.

Based on open-source information, there is no evidence of a direct external threat operating in the Mongolian information environment, but information campaigns are happening overseas that could threaten Mongolia's information environment in the future. Mongolia has successfully walked tightrope for many years between its two powerful neighbors. It must continue to do so if it wishes to maintain its sovereignty. On one hand, Mongolia might benefit from increased Russian and Chinese economic and political ties by serving as a geographic transit sight for resources, goods and services between the two countries. However, greater involvement also comes with great risk. Mongolia can help mitigate that risk by enhancing the psychological resiliency of its population in the infosphere.

---

74 "Press Institute of Mongolia," Devex, accessed November 29, 2021, https://www.devex.com/organizations/press-institute-of-mongolia-77781.

Page 2684 of 3957

V. SOCIAL INCLUSION FOR YOUNG PEOPLE

Inclusion is not a matter of political correctness. It is the key to growth.

—Jesse Jackson

A. WHAT IS SOCIAL INCLUSION?

The concept of social inclusion is generally described as a society for all. The Government of Mongolia defines social inclusion as "expansion and creation of an equal access and opportunity to those disadvantaged social groups, especially individuals based on low income, age, gender, disability, ethnic minority, sexuality and geographical location who have limited access to social services and participation."[75] There is a common understanding that social inclusion is only related to individuals with disabilities or from ethnic or sexual minorities. Against this backdrop, social inclusion is simply defined as "the process of improving the terms of participation in society."[76] Thus, this research focuses on social inclusion that fosters youth participation in the whole of society. Greater social inclusion is critical to fostering resilience.

B. WHY IS IT IMPORTANT?

Mongolian youth are the future of Mongolia's existence in the Russian and Chinese geopolitical environment, and their participation in the whole of society is crucial. Under many circumstances, Mongolian youth (people aged 18–29 years) suffers from a series of problems such as unemployment, low incomes, and the breakdown of family in a rapidly modernizing society. For instance, the Mongolian youth unemployment rate has reached "43,5 percent among all unemployed,"[77] and since 2020

---

[75] "Analysis of Social Inclusion and Gender Dynamic for REDD+ in Mongolia," UN-REDD Mongolia National Programme, July 2017, 12.

[76] *Leaving No One Behind: The Imperative of Inclusive Development, Report on the World Social Situation 2016*, Report No. ST/ESA/362 (New York: United Nations Department of Economic and Social Affairs, 2016), 17.

[77] Otgontugs Bayasgalan, "COVID-19 and Unemployment of the Youth," *Ikon,* February 9, 2021, https://ikon.mn/opinion/24i7.

it has been constantly increasing due to the COVID-19 induced economic crises. Therefore, the livelihood of many Mongolian young people depends on their parents' and grandparents' pension and other welfare assistance from the government. There are many reasons for youth unemployment such as "a lack of information on vacancies and requirements, high demands for collateral in employment contracts from some employers, and discrimination based on sex and age."[78] Moreover, youth unemployment renders the country "vulnerable to economic stresses, uninspired, and unable to innovate and contribute to Mongolia's economic growth."[79] Besides, the mass migration of youth from rural areas to urban areas (particularly to Ulaanbaatar city) is increasing as young people seek education and employment. Those young people who migrate from rural areas are compelled "to reside on the outskirts of the city in ger district, where poor service delivery contributes to air pollution, health problems, as well as high rates of alcoholism and gender-based violence."[80] These issues make young people disadvantaged group in society, and Mongolian youth are at risk of living lives of continued poverty and social exclusion. This factor undermines resilience and creates vulnerabilities for and comprehensive defense posture.

C. WHAT ARE THE CURRENT EFFORTS?

Many countries have a specific policy on their youth's social inclusion. It is essential to develop the younger generation to be independent by including their participation in decision-making processes at all levels of government with a positive mindset. Such policies focus on developing young people, educating them, providing them with a safe environment to live and work in, and ensuring healthcare wherever they may reside in urban or rural areas. In the context of burgeoning youth unemployment, the Government of Mongolia proposed various policies to target young people for employment, vocational-training programs, and enhancing employment information exchange programs. For example, the National Programme on Promotion of Youth

---

[78] Mercy Corps, *Mongolia Strategic Resilience Assessment*, *Final Report* (Portland, OR: Mercy Corps, April 2017), 32.

[79] Mercy Corps, 39.

[80] Mercy Corps, 50.

Page 2686 of 3957

Development promotes "basic training in business, management, marketing, legal and financial skills for youth and increasing the awareness of youth business incubation services."[81] This program does not only target government programs for the young but also includes policies for the private and civic sector organizations that employ youths.

Nevertheless, those policies are not addressing psychological and social factors in a manner similar to the European Union (EU). In late 2018 The Council of the European Union passed the resolution for "The EU Youth Strategy 2019–2027.," It promotes youth contribution in the democratic life. For example, the EU's Youth Strategy offers "new tools for mutual learning, such as peer reviews and peer counseling, high-level forums, analysis, and studies, following the priorities of the EU Youth Strategy at large."[82] Also, the strategy captured most of the key issues for youth, and the strategy itself emphasizes "positive change inspired by EU values and a European identity."[83] However, Mongolia has also taken action., The State Great Khural of Mongolia (parliament) implemented the "Vision-2050" long-term development policy of Mongolia in 2020. The policy itself fosters national identity, preserves traditional language and scripts, and acknowledges nomadic civilization as part of the national identity among the youth. A unified national identity is the foundation of social and psychological resilience. Without it, no comprehensive defense strategy can survive for long.

1. National Identity and Shared National Values

Why is national identity so important? David W. Johnson, of the Cooperative Learning Center at the University of Minnesota, stresses "a national identity unites and builds a bond among all members of the society."[84] Hence, the participation of youth in nation-building or decision-making processes is important to any nation. The Mongolian policy document "Vision-2050" emphasizes the need to "educate the entire population

---

[81] "Youth Employment Policy Summary for Mongolia," International Labour Organization, December 2016, https://www.ilo.org/asia/publications/WCMS_536713/lang--en/index.htm.

[82] "The European Union Youth Strategy 2019–2027," Resolution of the Council of the European Union and the Representatives of the Member States meeting within the Council on a framework for European cooperation in the youth field: 2018/C 456/01, December 18, 2018, 6.

[83] "The European Union Youth Strategy 2019–2027," 4.

[84] Lybi Ma, "Need for a National Identity," *Psychology Today,* September 2, 2019.

with 'the mother tongue, the history and the heritage' based on solid facts, and develop shared values that will be the pillar to build a nation-state with a deep sense of national similarities/differences and resilience."[85] As a result, Mongolia would flourish as a nation with a deep-rooted sense of national identity and sharing common values by 2050.

What is Mongolian national identity? This question appeared with Mongolia's peaceful transition from a socialist to a democratic country, and the question remains unanswered. According to "Vision-2050," nomadic civilization is considered a part of the Mongolian national identity. Mongolians tried to settle the term "national identity" in many ways, but disputes are still ongoing. Some people argue that "Mongolian Blue Spot" (which refers to the "blue-gray spots and congenital dermal melanocytotic, the marks … often present at birth but [which] may also appear during the first weeks of life"[86]) is a part of national identity. But Mongolian blue spots do not happen only among Mongols and appear in many nations around the world. As William Bloom, occasional lecturer at the Department of International Relations, London School of Economics, suggested back in the 1990s, "the mass national public will mobilize when it perceives that national identity is threatened."[87] Neither nomadic civilization nor Mongolian blue spot would cause the mass of people to mobilize even if those factors were threatened in Mongolia. On the other hand, it is of primary importance to define the national identities of Mongolia and support them with firm policies such as "Vision-2050." Furthermore, Mendee Jargalsaikhan points out "accepting as a centerpiece in its national identity democratization, Mongolia has gained geopolitical balance and increased its capacity to affirm its distinctiveness versus China and Russia as well as Central Asian states or former Asian communist states (Laos, North Korea, and Vietnam)."[88] Dr. Mendee argues that Mongolian democracy is in the ranks of electoral democracies of the world

---

[85] The State Great Khural Resolution 52/2020, "Vision-2050 Long-Term Development Policy of Mongolia," May 13, 2020, 1.

[86] Jennifer Berry, "Recognizing and Treating Mongolian Blue Spots," *Medical News Today*, August 21, 2020, https://www.medicalnewstoday.com/articles/318853.

[87] William Bloom, *Personal Identity, National Identity and International Relations* (Cambridge, UK: Cambridge University Press, 1990), 79.

[88] Mendee Jargalsaikhan, "Democratization, National Identity, and Foreign Policy in Mongolia in 2019," *The Asan Forum*, June 25, 2019, https://theasanforum.org/democratization-national-identity-and-foreign-policy-in-mongolia-in-2019/.

Page 2688 of 3957

beyond its expansionist neighbors. Against this backdrop, Jargalsaikhan Dambadarjaa (known as Jargal DeFacto), who is an independent economist and media representative of Mongolia, explains "the basic values of the Mongolian society are now democracy, human rights, and freedom."[89] Undoubtedly, if either democracy or human rights were threatened or violated in Mongolia, it could cause mass protests.

2. National Language and Script

From a subjective point of view, "national identity is based upon the sentiment of belonging to a specific nation, endowed with its own symbols, traditions, sacred places, ceremonies, heroes, history, culture and territory."[90] What this means is that each nation is distinctive in its traditional cultures, history, language, and script. According to the Pew Research Center survey, "language far and away is seen as the most critical to national identity."[91] Moreover, the survey stressed that "it is very important to speak the native language to be considered a true member of the nation."[92] Pew Research Center's Global Attitudes survey, conducted in 2016, involved 14 Western countries. Like other Asian countries, Mongolians are struggling to promote their traditional national language and script since the fall of the Soviet Union. The Mongolian language is part of a family within the Altaic language group and is used not only by Mongolians but also in the autonomous regions of Inner Mongolia, the PRC, and the Russian Far East (in particular, among the Buryat and Kalmykia ethnic groups). Mongolia's long history with its language has never been smooth. Specifically, the traditional Mongolian script (written in vertical lines top-down) faded away, "while under Soviet influence, Mongolia adopted the Cyrillic alphabet in 1941, which it uses to this day."[93] Cyrillic has been the standard script for official communications for decades, and nowadays, the Mongolian national

---

[89] Jargalsaikhan Dambadarjaa, "The Vision-2050 Criticism 9: Shared National Values," *Jargal DeFacto*, May 11, 2020, https://jargaldefacto.com/article/mongolia-s-national-identity.

[90] Montserrat Guibernau, "Nation Formation and National Identity," *Belgisch Tijdschrift voor Nieuwste Geschiedenis [Magazine of Belgian Latest History],* vol. 4 (April 2004): 658.

[91] Bruce Stokes, "What It Takes to Truly Be 'One of Us,'" Pew Research Center, February 2017, 9.

[92] Stokes, 9.

[93] Andrew Warner, "Card Game Aims to Revitalize Traditional Mongolian Script," *Language Magazine*, December 2020, https://www.languagemagazine.com/2020/12/10/card-game-aims-to-revitalize-traditional-mongolian-script/.

script has become almost an ancient script. As result, most Mongolians are poor at reading the traditional script, and while the young learn to read and write it in school, it plays only a small part in modern life. In addition, the old script contains many idiosyncratic spellings that varied to make it harder to read and write. For example, the city of Ulaanbaatar is written the same in English, but "the traditional script writes it as Ulaganbagator."[94]

In 2020, the Government of Mongolia declared "plans to restore the use of its traditional alphabet by 2025, replacing the Cyrillic script adopted under the Soviets,"[95] following the shift in other Central Asian countries such as Kazakhstan, Uzbekistan, and Turkmenistan. To that end, "Vision-2050" confirmed as one of its objectives the need to "incorporate the Mongolian language and script into national values and foster its proficiency and use by every citizen."[96] The decision, however, faced much criticism from the population, but young people, especially, are welcoming the change. An incident happened in Inner Mongolia in September 2020 that strengthened the government's decision in Mongolia. Thousands of ethnic Mongolians protested in Inner Mongolia, which is part of the PRC, against replacing the Mongolian language with Mandarin Chinese in schools. The *Guardian* emphasized "the official explanation for the change to a bilingual education system was to ensure the curriculum and textbooks were of a high standard, and that government documents cited by analysts also referred to President Xi Jinping's push for shared language as part of a common identity."[97] However, the Inner Mongolian objection to the PRC's proposal triggered social media movements in Mongolia expressing anti-China sentiments and calling to "Save the Mongolian language," and it also fostered Mongolian youth's nationalism. Since then, many Mongolians understand why the Mongolian national script is important, and the

---

[94] Anand Nyamdavaa, "How Much Can Mongols Read Traditional Script?," *Mongolia FAQ*, October 2018, https://mongoliafaq.com/2018/10/26/how-much-can-mongols-read-traditional-script/.

[95] Didi Tang, "Mongolia Abandons Soviet Past by Restoring Alphabet," *The Times,* March 2020, https://www.thetimes.co.uk/article/mongolia-abandons-soviet-past-by-restoring-alphabet-rsvcgqmxd.

[96] "Vision-2050 Long-Term Development Policy of Mongolia," 3.

[97] Helen Davidson, "Inner Mongolia Protest at China's Plans to Bring in Mandarin-only Lessons," *The Guardian*, September 2020, https://www.theguardian.com/world/2020/sep/01/inner-mongolia-protests-china-mandarin-schools-language.

Government of Mongolia promotes some policies that focus on boosting traditional literacy among the young. For instance, "Foremost Traditional Script Writers of Mongolia" is a popular contest conducted annually that attracts participants of all ages. Over 1,500 participants sent their works to the annual contest in 2021, and the Minister of Education and Science, Enkh-Amgalan Luvsantseren, participated and delivered remarks at the award ceremony. Mr. Enkh-Amgalan emphasized, "the Mongolian traditional script is a guarantee for national security, and we have an utmost important duty to protect the culture and history written in Mongolian traditional script as a cultural heritage of humankind and to pass it down to the next generation."[98] That was an indication of Mongolia's progress in preserving this area of national identity. This increased interest and involvement in the traditional Mongolian script is a significant potential source of psychological resilience.

3. Mongolia and Nomadic Lifestyles

Nomadism is defined as the "way of life of peoples who do not live continually in the same place but move cyclically or periodically."[99] Long after the supremacy of Genghis Khan, nomadism remained a way of life that continues in modern Mongolia as it does in Kazakhstan and Kyrgyzstan. Nomad ideology has emerged to become "a strong pillar of Mongolian national identity, [and] it has also divided the Mongol population into distinct groups not only within the present borders of Mongolia, but also in the surrounding territories of Central Asia."[100] Mass migration from rural areas to cities has been increasing since the 1990s due to many reasons, and consequently, one-third of the population now lives in urban areas. In the rural areas, there is little opportunity for economic activities that would maintain a household's livelihood at a decent level, except for herding. Today, the Mongolians have increasingly adapted to globalized cultures. The youth find these cultures appealing, especially the South Korean or a Western lifestyle,

---

98 "Winners of 25th 'Foremost Traditional Script Writers of Mongolia' Awarded," Montsame, January 2022, https://www.montsame.mn/en/read/286540.

99 *Encyclopaedia Britannica*, s.v. "nomadism," April 2016, https://www.britannica.com/topic/nomadism.

100 Zsolt Szilagyi, "Lingering Nomad Ideology in 21st Century Mongolia," *Acta Ethnographica Hungarica: An International Journal of Ethnography* 61, no. 1 (June 2016): 199.

and urban daily life makes the young willing to dispense with nomadic traditions. Moreover, challenges such as climate change and natural threats such as zuds (an extreme winter), drought, dust storms, earthquakes, and fires (forest and steppe) cause young people to leave rural areas. On the other hand, the Mongolian mindset has changed in recent years, and urban life has been viewed as the only way to live in the modern world. In fact, "Mongolian intellectuals for generations have been taught to regard the herders' life as non-progressive, old-fashioned, even though the repository of Mongolian heritage."[101]

Due to air pollution in Ulaanbaatar city and mass migration to an urban area, the Government of Mongolia is making some attempts to develop rural areas and support nomadic lifestyles as part of the national heritage and as a tourist attraction. For example, "Vision-2050" is aiming to position Mongolia to "become a leading country with preserved nomadic civilization, based on national mentality, heritage, culture, and mindset, and centered on the creative Mongolian citizen."[102] The policy will adapt to the conveniences of modern society while keeping an ancient and fascinating lifestyle alive. Migrating from an urban to a rural area is challenging for young people, and it requires strong motivation. The policy will require significant investment in providing robust support to herders, particularly during harsh winters, connecting the nomadic lifestyle. There have been some cases of young people migrating from "the opposite" direction. For instance, Batbayar "Baavar," the President of the Mongolian Hip-hop Association, moved to the countryside with his family in 2019, and his family now lives in the northern part of Mongolia. Mr. Baavar once emphasized "Living in the countryside is wonderful and challenging,"[103] which inspires many young people on social media today.

---

[101] Alicia J. Campi, "Moving Mongolian Nomadism into the 21st century: Cultural and Ecological Preservation Coupled with Economic Vitality and National Security," Research thesis, (Washington, University of the District of Columbia, 1997), 7.

[102] "Vision-2050 Long-Term Development Policy of Mongolia," 2.

[103] А.Цээсүрэн, "Хөдөөний амьдрал дэндүү сайхан бас сонирхолтой" [Living in the countryside is wonderful and challenging], News.mn, January 2022, https://news.mn/r/2518672/.

VI. CONCLUSION AND RECOMMENDATIONS

Victory comes from finding opportunities in problems.

—Sun Tzu

The survival of small democratic nations bordered by superpowers requires constant vigilance, especially as the nature of warfare evolves. Warfare is not limited to the physical domain; it increasingly cuts across psychological and social frameworks as well. Mongolian national defense policies have relied on conventional military capacity for decades, but those policies never included psychological and social preparation against any external influences. This thesis has examined three lines of effort to develop and maintain Mongolia's social and psychological resilience capacities as part of its national defense strategy. Notably, Mongolia must sustain and develop strategic partnerships with its neighbors and enhance its military-to-military cooperation.

Building psychological and social resilience is one of the core pillars of NATO's comprehensive defense posture. Comprehensive defense policies have been based on total defense strategies from Western Europe during the Cold War period and have not been tested since then. Many countries such as the Nordic states (Norway, Finland, and Sweden) and Taiwan are currently applying comprehensive defense policies. Those countries have some similarities with Mongolia such as conscription (mandatory military service), small populations, and borders with superpowers and therefore provide useful insights into the development of Mongolia's comprehensive defense strategic efforts.

Mongolia, a small nation, is located in a significant geopolitical environment. Failing to invest in social and psychological resilience now puts Mongolia at risk, as has been observed elsewhere. Consider Kazakhstan's unrest in January 2022 as an example. The International Crisis Group summarizes Kazakhstan unrest as resulting from "economic stagnation, a sharp rise in predatory consumer debt, rising internal migration, the pandemic, increasing protests and widening inequality," which means that "weakened

Page 2693 of 3957

institutions faced significant tests."[104] Authorities in Kazakhstan accused protesters of being "terrorists," "bandits," and "foreigner mercenaries," but those claims were not confirmed officially. According to an Al Jazeera interview, "the main group of protesters—young unemployed people from the regions expressing their frustrations against injustice,"[105] were manipulated by social media and social influencers. Those unemployed youth were victims of information and psychological operations, and many of them ended up in prison. A very similar situation arose in Mongolia in 2008, when "police arrested over 700 people on the night of 1 and 2 July,"[106] an action that resulted in the deaths of five young people. In addition, the current Russian-Ukrainian conflict confirms that military objectives aim not only at the military in combat but also at civilians back home. For example, during this conflict, "military propagandists delivered false and demoralizing messages to Ukrainian soldiers at the front and their family members back home via cyber-electromagnetic means."[107] These incidents demonstrate just how crucial psychological and social resilience is in today's world.

When it comes to Mongolia, the current defense law states that defense policy relies on the participation of government entities and all citizens. But the law fails to include participants from the private and civic sectors as the asymmetric defense component. This is the gap where Mongolia should understand, and consider, the concept of the NATO CDH by strengthening integrated layered defense policies. It takes time to change conventional defense posture within the whole-of-government approach as a comprehensive defense. A critical first step of this approach is to bolster social and psychological resilience. Thus, the following recommendations could improve and provide support for the psychological resilience of Mongolia.

---

104 "Behind the Unrest in Kazakhstan," International Crisis Group, January 2022. https://www.crisisgroup.org/europe-central-asia/central-asia/kazakhstan/behind-unrest-kazakhstan.

105 Agnieszka Pikulicka-Wilczevska, "Do Kazakhstan's Protests Signal an End to the Nazarbayev Ear?," Al Jazeera, January 2022, https://www.aljazeera.com/news/2022/1/11/qa-kazakh-activist-yevgeniy-zhovtis-on-mass-unrest.

106 "'Where Should I Go from Here?' The Legacy of the 1 July 2008 Riot in Mongolia," Amnesty International, December 2009, 4.

107 Aaron F. Brantly, Nerea M. Cal, and Devlin P. Winkelstein, *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW* (New York: Army Cyber Institute at West Point, December 2017), 28.

A. RECOMMENDATIONS

To invest in Mongolia's comprehensive defense strategy, this thesis provides three recommendations for building psychological resilience in Mongolia.

1. A persistent national information campaign, initiated and conducted by the Government of Mongolia in cooperation with civil society and NGOs, would make Mongolians aware of the comprehensive defense concept

Compared to neighboring states, the Mongolian economy, population, and military are relatively small, and there is no direct threat currently. There are, however, many indirect threats that could escalate. For example, a recent case of Beijing's new policy replacing the Mongolian language with the Mandarin Chinese language in Inner Mongolia triggered a protest in Mongolia. The main concern of the Mongol people was "if the traditional written language dies in Inner Mongolia, it would be a massive loss of identity for all the Mongols around the world."[108] As described by the CDH, understanding the strategy is not only for decision-making politicians and military personnel, but requires awareness and participation across all sectors of society. This means that Mongolian citizens should be aware of current and potential future threats to its democratic values.

But the world is changing day by day, and citizens of Mongolia need to be prepared for potential future threats, especially in terms of psychological and social resilience. Today, some malicious acts threaten the safety, security, and sovereignty of superpowers and small nations equally. For example, the Russian disinformation campaign against the U.S. election in 2016 was a significant surprise to the world. That example demonstrates that no country can afford to lack psychological and social resilience in the information era. Such a threat requires that every member of society get a basic knowledge of psychological resilience.

There are already frameworks in place that the Government of Mongolia could adapt for the purpose of education and information. Furthermore, the Government of Mongolia could start by "establishing online and public media-based training and

108108 "The War You Never Heard of," *Trips@Asia,* (January 2021), accessed on 8 February 2022, https://www.tripsatasia.com/newsletter-articles/inner-outer-mongolian-language.

Page 2695 of 3957

information programs"[109] to promote digital literacy. One example of how this is already being accomplished is Mongolian CITA establishing the "Information Technology Center" in 2022 "to improve citizens' digital literacy skills and enable youth to have the skills to use modern technologies."[110]

Specifically, programs that exist for disaster response and prevention can translate to responses for national security crises. These programs extend nationwide and are not difficult to set up. For example, Sweden's "If Crisis or War Comes"[111] contains information about how to respond to natural disasters and malicious acts (such as disinformation, terrorism, physical occupation). Moreover, the National Emergency Management Agency (NEMA) has successfully established early warning systems nationwide in Mongolia through the media, internet, national radio, and communication companies to alert the public to potential storms and flooding (see Figure 2).

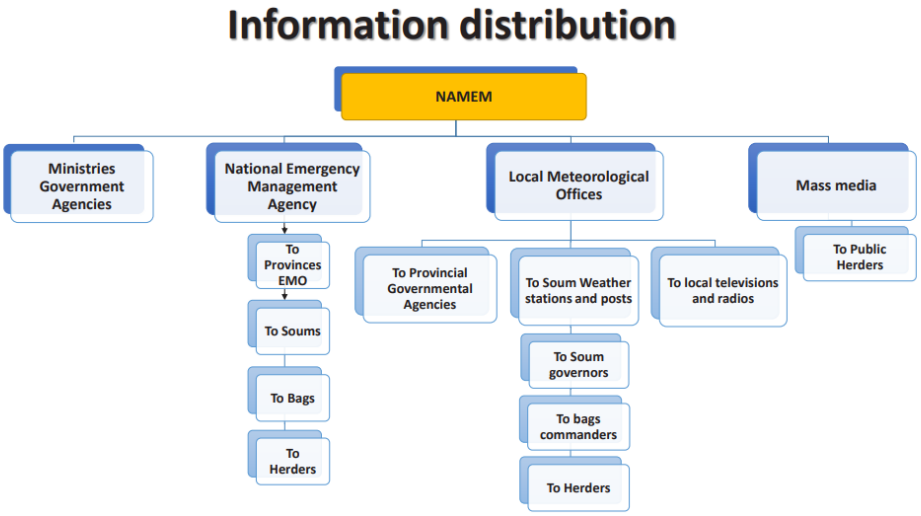


Figure 2. Flood and Storm Warning Information Distribution[112]

109 NATO Comprehensive Defense Handbook, 64.

110 Unurzul Majdaa, "Information Technology Center to be Established," Montsame, November 2021, https://montsame.mn/en/read/280389.

111 "If Crisis or War Comes," Swedish Civil Contingencies Agency, May 2018, https://www.msb.se/en/rad-till-privatpersoner/the-brochure-if-crisis-or-war-comes/.

112 Center for Excellence in Disaster Management and Humanitarian Assistance, *Mongolia Disaster Management Reference Handbook* (Hickam, Hawaii: Joint Base Pearl Harbor, 2018), 33.

The way information flow is as follows. It begins with Mongolia's National Agency of Meteorology and Environmental Monitoring (NAMEM) and is "disseminated down though the ministries, NEMA, local meteorological offices and through mass media until it makes it was to the herders."[113] This system and structure could also work for disseminating accurate information that may affect national security.

2. A basic education curriculum in elementary and high school should include digital literacy

Section IV of this thesis examined social media vulnerabilities in Mongolia, and these vulnerabilities require a long-term solution. As Section IV mentioned, there is no distinction between "disinformation" and "misinformation" in Mongolia. At this time, Mongolia does not have rock-solid laws or regulations against misleading information or online phishing matters. The misleading information includes not only internal matters in Mongolia, but some information that comes from overseas. Chapters II and III of the thesis covered case studies on misleading information in Mongolia, and it is not going to be stopped in the future.

The Government of Mongolia is enhancing adult education and professional development in certain areas, but this education is not good enough to target the whole of society. Teenagers, youth, and older people are still at risk of being manipulated by misleading information. Therefore, digital or media literacy programs should be included in elementary schools' educational curricula as is done in Taiwan and Finland. In addition, fact-checking norms and digital literacy are essential skills to the student who studies journalists for the press personnel capacity building and professionalism. It's commonly known that media always plays a considerable role in social and psychological resilience. This is not a quick-fix issue but will take some time.

[113] Mongolia Disaster Management Reference Handbook, 33.

Page 2697 of 3957

3. Mongolia should promote civil society organizations and enhance their capabilities

According to Mercy Corps, "Mongolia's civil society sector is still small and focuses primarily on environmental and child welfare issues."[114] In fact, civil society organizations are inadequate due to the legal framework that constrains their activities. Furthermore, as Mercy Corps emphasized, "an enabling environment for resilience and development must be supported by citizen demand for good governance through civic engagement and collective action."[115] Consequently, the Government of Mongolia and its entities are hardly influenced by civil society organizations, and NGOs remain out of the circle of political decision-making processes. This is the space for the emerging civic-government partnership, and authorities should adapt proper legal frameworks. For example, the Mongolian Fact-Checking Center can collaborate with the government on media literacy education for the young or effective measures to counter misleading information. The Taiwanese FactCheck Center is considered a model for coordination with the government and to counter disinformation among other centers.

What is more, "targeting civic engagement efforts towards youth will be especially critical, as this helps cultivate a sense of agency and future purpose that underlies resilient individuals and communities."[116] Access to all kinds of information is inadequate, and only civic organizations tend to be effective at reaching and engaging youth. The government's policies on youth are not always as effective as those of civic organizations, and some countries use this opportunity to promote defense policies in creative ways—for example, the Norwegian NGO People and Defense provides "support for the armed forces and Norwegian defense policies"[117] by employing policies aimed at youth. Norwegian practice confirms Mercy Corps' conclusion that "strengthened social networks have been shown in many contexts to have a multiplier effect on inclusive

---

114 "Mongolia Strategic Resilience Assessment," 25.

115 "Mongolia Strategic Resilience Assessment," 48.

116 "Mongolia Strategic Resilience Assessment," 48.

117 Nina Graeger, From 'Forces for Good' to 'Forces for Status'?, Small States and Status Seeking (New York: Routledge, 2015), 99, 86–108.

decision-making, civic engagement and an overall enabling environment that supports resilience."[118]

Similar to Norway, there used to be civic societies in Mongolia that supported the defense force during the Soviet era, called "Community for Defense Support."[119] That community consisted of various sports clubs such as parachuting, shooting, cross-country skiing, and wrestling. Most of the activities were dedicated to youth. The Government of Mongolia can promote such kinds of civic organizations to foster psychological resilience among the youth.

B. AREAS FOR FURTHER STUDY

Establishing a comprehensive defense is complicated, and it "requires all sectors of society to be capable of integrating into a single, coherent, multi-layered system."[120] An example of such a multi-layered system is shown in Figure 3. This thesis outlines education, information, and inclusion efforts to develop psychological resilience, highlighting instruments needed to contribute to comprehensive defense. Furthermore, it identified psychological resilience as a strong foundation for the resistance movement. The outcome of the ongoing conflict in the Ukraine should also be studied closely for potential lessons.

---

118 "Mongolia Strategic Resilience Assessment," 49.

119 С.Туул, "Эвлэлээс төв зөвлөл хүрсэн түүх," [History of the community from council], GoGo.mn, June 2009, https://gogo.mn/r/55823.

120 Source: NATO Comprehensive Defense Handbook, 33.

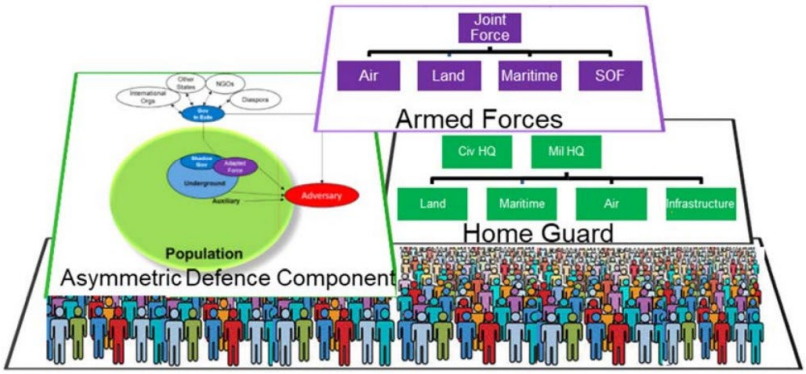


Figure 3. Integrated Layered Defense[121]

Therefore, the thesis focuses on resilience as "the first line of a multi-layered deterrence and response system,"[122] and primarily aims to strengthen asymmetric defense components. This means the thesis has not discussed the concern of the armed forces and home guards in comprehensive defense policies.

Future research should consider how the inclusion of the Mongolian Armed Forces (particularly the Special Forces Command) and Local Defense Forces (which are equivalent to the Home Guard shown in Figure 3) could contribute to comprehensive defense policies. The latter was established on June 27, 2018, when the Mongolian Parliament passed the law for the "Local Defense Force" (LDF), the purpose of which is to regulate local defense force relations aimed at establishing and strengthening the state defense system. Mongolia's new LDF is considered to be a paramilitary organization like the Swiss territorial service, Swedish home guard, and the U.S. National Guard. Given its close relationship with local populations, it can be a valuable bridge to the civic sector in developing a comprehensive defense policy.

121 *NATO Comprehensive Defense Handbook*, 33.
122 *NATO Comprehensive Defense Handbook,* 34.

LIST OF REFERENCES

Allkpop. "Four Teenage Girls Assaulted a Mongolian Girl for Six Hours with Her Hands and Legs Tied Up." December 2021. https://www.allkpop.com/article/2021/12/tw-cw-four-teenage-girls-assaulted-a-mongolian-girl-for-six-hours-with-her-hands-and-legs-tied-up.

Amicus Travel (blog). "Youth in Mongolia." August 13, 2019. https://www.amicusmongolia.com/youth-in-mongolia.html.

Amnesty International. 'Where Should I go from Here?' The Legacy of the 1 July 2008 Riot in Mongolia." December 18, 2009. https://www.amnesty.org/en/documents/asa30/003/2009/en/.

Arreguin-Toft, Ivan. "*How the Weak Win Wars: A Theory of Asymmetric Conflict*" International Security, Vol. 26, No. 1 (Summer 2001), pp. 93-128.

Baumeister, Roy F., and Mark R. Leary. "The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation." *Psychological Bulletin* 117, no. 3 (1995): 497–529. https://doi.org/10.1037/0033-2909.117.3.497.

Bayasgalan, Otgontugs. "COVID-19 and Unemployment of the Youth." *IKON.* February 9, 2021. Accessed February 8, 2022. https://ikon.mn/opinion/24i7.

Berry, Jennifer. "Recognizing and Treating Mongolia Blue Spots." *Medical News Today*, August 21, 2020. https://www.medicalnewstoday.com/articles/318853.

Blair, Gavin J. "Mongolian TV Network Exposes Media Corruption with Fake Story about McDonald's." *The Hollywood Reporter,* December 2013. https://www.hollywoodreporter.com/news/general-news/mongolian-tv-network-exposes-media-665859/.

Bloom, William. Personal Identity, National Identity and International Relations. Cambridge: Cambridge University Press, 1990.

Brantly, Aaron F., Nerea M. Cal, and Devlin P. Winkelstein. *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*. New York: Army Cyber Institute at West Point, December 2017. https://apps.dtic.mil/sti/citations/AD1046052.

Boys & Girls Clubs of America. "Digital Literacy Essentials." Accessed November 16. 2021. https://www.bgca.org/programs/education/digital-literacy-essentials.

Page 2701 of 3957

Campi, Alicia J. “Moving Mongolian Nomadism into the 21st Century: Cultural and Ecological Preservation Coupled with Economic Vitality and National Security.” Thesis, University of the District of Columbia, 1997.

Center for Excellence in Disaster Management and Humanitarian Assistance. *Mongolia Disaster Management Reference Handbook.* Hickam, Hawaii: Joint Base Pearl Harbor, 2018.

Center for Public and Political Studies. “WIN/Gallup International’s Global Survey Shows Three in Five Willing to Fight for Their Country.” Gallup International, May 7, 2015. https://www.gallup-international.bg/en/33483/win-gallup-internationals-global-survey-shows-three-in-five-willing-to-fight-for-their-country/.

Cheterian, Vicken. “The August 2008 War in Georgia: from Ethnic Conflict to Border Wars,” Central Asian Survey, no. 2 (July 2009): 155–170. https://doi.org/10.1080/02634930903056768.

Colley, Thomas, Francesca Granelli, and Jente Althuis. “Disinformation’s Societal Impact: Britain, Covid, and Beyond.” Defence Strategic Communications, (July 2020): 89–140. https://stratcomcoe.org/publications/disinformations-societal-impact-britain-covid-and-beyond/36.

Council of the European Union. Resolution of the Council of European Union and the Representatives of the Member States Meeting within the Council on a Framework for European Cooperation in the Youth Field: 2018/C 456/01. “The European Union Youth Strategy 2019–2027,” December 18, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2018:456:FULL&from=EN.

Davidson, Helen. “Inner Mongolia Protest at China’s Plans to Bring in Mandarin-only Lessons.” *The Guardian*, September 2020. https://www.theguardian.com/world/2020/sep/01/inner-mongolia-protests-china-mandarin-schools-language.

Devex. “Press Institute of Mongolia.” Accessed November 29, 2021. https://www.devex.com/organizations/press-institute-of-mongolia-77781.

Digital and Inbound Marketing Agency. “Сошиал медиагийн хэрэглээ Монголд,” [Social Media Usage in Mongolia]. DIMA, January 2020. https://dima.mn/2020/01/14/сошиал-медиа-хэрэглээ-монголд/.

European Center for Populism Studies. “Weaponization of Information,” August 2017. https://www.populismstudies.org/Vocabulary/weaponization-of-information/.

Fiala, Otto. *Resistance Operating Concept*. 1st ed. Stockholm, Sweden: Swedish Defence University, 2019.

Page 2702 of 3957

Graeger, Nina. "From 'Forces for Good' to 'Forces for Status'?" In *Small States and Status Seeking*, 86–108. New York: Routledge, 2015.

Greenbaum, Zara. "5 Questions for Arie W. Kruglanski." *American Psychological Association,* April 2018. www.apa.org/monitor/2019/04/conversation-kruglanski#.

Guibernau, Montserrat. "Nation Formation and National Identity." *Belgisch Tijdschrift voor Nieuwste Geschiedenis [Magazine of Belgian Latest History],* vol. 4, April 2004, 657–682.

International Labour Organization. "Youth Employment Policy Summary for Mongolia," December 2016. https://www.ilo.org/asia/publications/WCMS_536713/lang--en/index.htm.

Jargalsaikhan, Mendee. "Democratization, National Identity, and Foreign Policy in Mongolia in 2019." *The Asan Forum*, June 25, 2019. https://theasanforum.org/democratization-national-identity-and-foreign-policy-in-mongolia-in-2019/.

Kane, Nicholas J. "Defense Against Weaponized Information: A Human Problem, Not Just a Technical One." *InterAgency Journal* 10, no. 3 (2019): 46–65.

Kao, Shih-Shiuan. *Taiwan's Response to Disinformation: A Model for Coordination to Counter a Complicated Threat*. Special Report No. 93. Washington, DC: The National Bureau of Asian Research, September 2021.

Karashanova, Aida, and Elena Dyaknova. "Assessing E-Resilience in Kazakhstan, Kyrgyzstan and Mongolia." *Asia-Pacific Information Superhighway Working Paper Series* no. 03 (July 2021): 1–29.

Kemp, Simon. "Digital 2021: Mongolia." Datareportal. Accessed October 17, 2021. https://datareportal.com/reports/digital-2021-mongolia.

Kuul, Margus. "Civil: An Essential Element of a Total Defense Strategy." Master's thesis, Naval Postgraduate School, 2014. https://calhoun.nps.edu/handle/10945/42667.

Lai, Christina. "More than Carrots and Sticks: Economic Statecraft and Coercion in China–Taiwan Relations from 2000 to 2019." *Politics*, February 2021, 1–16. https://doi.org/10.1177/0263395720962654.

Lkhagvasuren, Bayasgalan. "Book Review: Resistance Operating Concept." *Small Wars Journal*, June 2021. https://smallwarsjournal.com/jrnl/art/book-review-resistance-operating-concept.

Page 2703 of 3957

Ločmele, Klinta. "Media Literacy in Latvia: The Ministry of Culture's 6 Strands." *Media and Learning*, January 2019. https://media-and-learning.eu/type/featured-articles/media-literacy-in-latvia-the-ministry-of-cultures-6-strands/.

Ma, Lybi. "Need for a National Identity." *Psychology Today*, September 2, 2019.

Maddox, J.D., Casi Gentzel, and Adela Levis. "Toward a Whole-of-Society Framework for Countering Disinformation." Modern War Institute, October 2021. http://mwi.usma.edu/toward-a-whole-of-society-framework-for-countering-disinformation/.

Majdaa, Unurzul. "Information Technology Center to be Established." Montsame, November 2021. https://montsame.mn/en/read/280389.

Mantas, Harrison. "The Mongolian Fact Checking Center Fights Misinformation in a Country where the Word Doesn't Exist." *Poynter*, August 2021. https://www.poynter.org/fact-checking/2021/the-mongolian-fact-check-center-fights-misinformation-in-a-country-where-the-word-doesnt-exist/.

Mercy Corps. *Mongolia Strategic Resilience Assessment*. Portland, Oregon: 2017. https://www.mercycorps.org/sites/default/files/2019-12/Mercy_Corps_Strategic_Resilience_Assessment_Mongolia_April_2017.pdf.

Ministry of Education (Taiwan). *Curriculum Guidelines of 12-Year Basic Education*. Official Training Curriculum. Taipei, Taiwan: Government of Taiwan, Ministry of Education, November 2014.

Ministry of Foreign Affairs of Mongolia. "National Security Concept of Mongolia." November 2015. https://mfa.gov.mn/en/documentation/55280/.

Montsame. "Mongolia-U.S. Joint Disaster Management Exercise 'Gobi Wolf-2019' Underway." September 16, 2019. https://montsame.mn/en/read/200776.

NATO. "NATO's Approach to Countering Disinformation: A Focus on COVID-19." July 2020. http://www.nato.int/cps/en/natohq/177273.htm.

———. "Warsaw Summit Communiqué (2016a)." July 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NATO Special Operations Headquarters. *NATO Comprehensive Defense Handbook*. Vol. 1. Shape, Belgium: Quartier General, 2020.

News.mn. "Facebook Launches 'We Think' Digital Program in Mongolia to Cultivate Responsible Digital Citizens." April 2021. https://news.mn/en/795665/.

Page 2704 of 3957

Nyamdavaa, Anand. “How Much Can Mongols Read Traditional Scrip?” Mongolia FAQ. October 2018. https://mongoliafaq.com/2018/10/26/how-much-can-mongols-read-traditional-script/.

Open Society Institute Sofia. “Finding of the Media Literacy Index 2019: Just Think about It.” OSIS. November 2019. https://osis.bg/?p=3356&lang=en.

Ready. “Exercises.” Ready.gov. Last updated October 12, 2021. https://www.ready.gov/exercises.

Reporters without Borders. “2021 World Press Freedom Index.” Accessed November 29, 2021. https://rsf.org/en/ranking.

Reuters. “Mongolia Arrests 800 Chinese Citizens in Cybercrime Probe.” October 31, 2019. https://www.reuters.com/article/us-mongolia-crime-china-idUSKBN1XA0NW.

Sanchez, Linda. Bolstering the Democracy Resilience of the Alliance Against Disinformation and Propaganda,” Preliminary Draft Special Report to NATO Committee on the Civil Dimension of Security. Brussels, Belgium: NATO Parliamentary Assembly, March 2021.

Shore, Lynn M., and Beth G. Chung. “Inclusive Leadership: How Leaders Sustain or Discourage Work Group Inclusion.” *Group & Organization Management.* May 2021. DOI:10.1177/1059601121999580

Standish, Reid. “Why Is Finland Able to Fend off Putin’s Information War?” *Foreign Policy*, March 2017. https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.

The State Great Khural - Parliament of Mongolia. “Төрийн бус байгууллагын тухай Монгол Улсын хууль,” [Non-Governmental Organization Law], January 31,1997. https://legalinfo.mn/mn/detail/494.

———. Resolution 52/2020. “Vision-2050 Long-Term Development Policy of Mongolia.” May 13, 2020. www.https://cabinet.gov.mn/wp-content/uploads/2050_VISION_LONG-TERM-DEVELOPMENT-POLICY.pdf.

Stokes, Bruce. “What It Takes to Truly Be ‘One of Us’.” Pew Research Center, February 2017.

Swedish Civil Contingencies Agency. “If Crisis or War Comes,” May 2018. https://www.msb.se/en/rad-till-privatpersoner/the-brochure-if-crisis-or-war-comes/.

Szilagyi, Zsolt. “Lingering Nomad Ideology in 21st Century Mongolia.” *Acta Ethnographica Hungarica: An International Journal of Ethnography* 61, no. 1 (June 2016): 197–211.

Page 2705 of 3957

Tajfel, H., and J.C. Turner. “The Social Identity Theory of Intergroup Behavior.” In *Psychology of Intergroup Relations,* edited by S. Worchel and W. G. Austin. Chicago: Hall Publishers, 1986.

Tang, Didi. “Mongolia Abandons Soviet Past by Restoring Alphabet.” *The Times,* March 2020. https://www.thetimes.co.uk/article/mongolia-abandons-soviet-past-by-restoring-alphabet-rsvcgqmxd.

Trips at Asia. “The War You Never Heard of.” Accessed on 8 February 2022. https://www.tripsatasia.com/newsletter-articles/inner-outer-mongolian-language.

Tseesuren, A. “Хөдөөний амьдрал дэндүү сайхан бас сонирхолтой” [Living in the countryside is wonderful and challenging]. News.mn, January 2022. https://news.mn/r/2518672/.

Turvallisuus, Yhteiskunnan. *Security Strategy for Society*. Helsinki, Finland: The Security Committee, November 2017. https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

Tuul, S. “Эвлэлээс төв зөвлөл хүрсэн түүх” [History of the community from council]. GoGo.mn, June 2009. https://gogo.mn/r/55823.

UN Department of Economic and Social Affairs. Leaving No One Behind: The Imperative of Inclusive Development, Report on the World Social Situation 2016. Report No. ST/ESA/362. New York: United Nations, 2016.

UNDP Mongolia’s Accelerator Lat Team. “Bridging the Digital Divide in Mongolia.” *UNDP* (blog). April 2021. https://www.mn.undp.org/content/mongolia/en/home/blog/2021/bridging-the-digital-divide-in-mongolia.html.

UNESCO. “Lutaa’s Journey for Media and Information Literacy in Mongolia.” May 2021.https://en.unesco.org/news/lutaas-journey-media-and-information-literacy-mongolia.

UN-REDD Mongolia National Programme. “*Analysis of Social Inclusion and Gender Dynamic for REDD+ in Mongolia*,” Ulaanbaatar, Mongolia: 2017.

Vosoughi, Soroush, Roy Deb, and Sinan Aral. “The Spread of True and False News Online,” *Science* 359, no. 6380 (2018): 1146–1151.

Warner, Andrew. “Card Game Aims to Revitalize Traditional Mongolian Script.” *Language Magazine*, December 2020. https://www.languagemagazine.com/2020/12/10/card-game-aims-to-revitalize-traditional-mongolian-script/.

Page 2706 of 3957

Wikipedia. S.v. “2020 Mongolian legislative election.” Last modified February 14, 2022. https://en.wikipedia.org/wiki/2020_Mongolian_legislative_election

Wither, James Kenneth. “Back to the Future? Nordic Total Defense Concepts.” *Defense Studies* 20, no. 1 (January 2020): 61–81. https://doi.org/10.1080/14702436.2020.1718498.

Page 2707 of 3957

Page 2708 of 3957

INITIAL DISTRIBUTION LIST

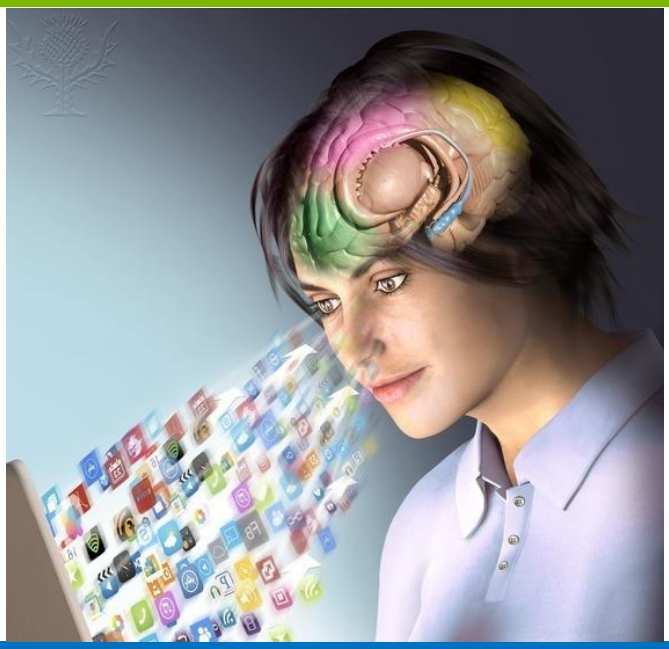
1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

Page 2709 of 3957

CNA

September 2021



The Psychology of (Dis)information: A Primer on Key Psychological Mechanisms

Heather Wolters, Kasey Stricklin, Neil Carey, and Megan K. McBride

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

DRM-2021-U-029337-1Rev-2

Abstract

Disinformation is a growing national security concern with a primary impact occurring in the mind. This study explores the underlying psychological principles facilitating the absorption and spread of disinformation and outlines options for countering disinformation grounded in in cognitive and social psychological literature. The report serves as an introduction to the topic for policy- and defense-decision makers with no prior background in psychology or disinformation. It first examines what disinformation is and why it is important before turning to the four key psychological principles relevant to this topic. A key finding is that the principles themselves are neutral and normal cognitive processes that malign actors can exploit to achieve their own objectives.

This document contains the best opinion of CNA at the time of issue.

It does not necessarily represent the opinion of the sponsor.

Distribution

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

9/27/2021

This work was performed under Federal Government Contract No. N00014-16-D-5003.

Cover image credit: "Internet effects on brain, conceptual illustration," Science Photo Library via Britannica ImageQuest, accessed Sept. 21, 2021, https://quest.eb.com/search/132_3125015/1/132_3125015/cite.

Approved by: **September 2021**

Jonathan Schroden, Research Program Director
Countering Threats and Challenges Program
Strategy, Policy, Plans, and Programs Division

Request additional copies of this document through inquiries@cna.org.

Copyright © CNA 2021

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
September 2021	1Rev	

4. TITLE AND SUBTITLE
(U) The Psychology of (Dis)information: A Primer on Key Psychological Mechanisms

5a. CONTRACT NUMBER
N00014-16-D-5003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0605154N

6. AUTHOR(S)
Heather Wolters, Kasey Stricklin, Neil Carter, Megan McBride

5d. PROJECT NUMBER
R0148

5e. TASK NUMBER
E236.00

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Center for Naval Analyses
3003 Washington Blvd
Arlington, VA 22201

8. PERFORMING ORGANIZATION REPORT NUMBER

DRM-2021-U-029337-1Rev

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Chief of Naval Operations (N803)
2000 Navy Department
Washington, D.C. 20350

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Disinformation is a growing national security concern with a primary impact occurring in the mind. This study explores the underlying psychological principles facilitating the absorption and spread of disinformation and outlines options for countering disinformation grounded in in cognitive and social psychological literature. The report serves as an introduction to the topic for policy- and defense-decision makers with no prior background in psychology or disinformation. It first examines what disinformation is and why it is important before turning to the four key psychological principles relevant to this topic. A key finding is that the principles themselves are neutral and normal cognitive processes that malign actors can exploit to achieve their own objectives.

15. SUBJECT TERMS
disinformation, psychology, psychological principles, policy, defense-decision making, psychology of disinformation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Knowledge Center/Tanya McCants
U	U	U	SAR	72	19b. TELEPHONE NUMBER *(include area code)* 703-824-2123

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Executive Summary

The rise of disinformation

Disinformation, or the intentional creation and spread of false information, is a growing national security concern. While the use of information operations is not a new phenomenon—various actors have used them throughout history for a range of objectives—the connectivity that characterizes the world today allows both information and disinformation to spread faster and with a much greater reach. It is not surprising that a rapidly increasing number of adversaries and domestic US actors are coming to understand the utility of the information space for achieving their objectives and are seeking to weaponize it. The use of disinformation has led directly to real-world events and violence, can have a demonstrable impact on a recipient's behavior, and can lead its promulgators to achieve some goals simply through its existence, regardless of its believability. Because disinformation's primary impact occurs in the mind, technological, political, or military solutions alone cannot sufficiently mitigate the threat.

Psychological principles associated with disinformation spread

This report is the result of an extensive literature review across multiple domains, including disinformation, psychology, military science, foreign affairs, economics, computer science, and marketing. Through the literature review, we identified four key psychological principles related to the absorption and spread of disinformation: initial information processing; cognitive dissonance; the influence of groups, beliefs, and novelty; and the role of emotions and arousal. This report describes each psychological principle, explains how the principle contributes to the absorption and spread of disinformation, and details ways to mitigate the effect of the principle on the spread of disinformation.

A critical takeaway from the identification of these principles is that they are not unique to absorbing and spreading disinformation. These same principles are key to absorbing and spreading true information as well. Thus, at an individual level, it appears that disinformation is absorbed and spread through normal, routine, and adaptive mechanisms, which malign actors can exploit and manipulate for their own objectives. The four psychological principles we identified are:

Page 2714 of 3957

- **Initial information processing:** Our mental "processing capacity" is limited; we simply cannot deeply attend to all new information we encounter. Our brains take mental shortcuts to incorporate new information, and those shortcuts can open us up to mistakes. To the extent that we do not process information as deeply as we should, disinformation can be construed as true information.
- **Cognitive dissonance:** Cognitive dissonance describes the discomfort we feel when we are confronted with two competing ideas. We are motivated to reduce the dissonance by changing one attitude, removing (ignoring) the contradictory information, discounting the importance of contradictory information, or increasing the importance of compatible information. If disinformation supports our initial beliefs or creates less dissonance than true information, we are more likely to believe the disinformation.
- **Influence of group membership, beliefs, and novelty (the GBN model):** Not all information is equally valuable to individuals. Our group memberships, our beliefs, and the uniqueness of the information influence whether we absorb and share disinformation. We are more likely to share information with people we consider members of our group, when we believe the information is true, and when it is novel or urgent. If disinformation is coming from a group member with whom we identify, is consistent with our beliefs, or is new information for us, we are more likely to share it.
- **Role of emotion and arousal in our sharing of disinformation:** Just as not all information is equally valuable, not all information affects us the same way. Research demonstrates that we pay more attention to information that makes us feel positively or that arouses us to act. That means we are more likely to share information if we feel awe, amusement, or anxiety than if we feel sadness or contentment. Given that disinformation is, by definition, created by someone, it is more likely to be absorbed and shared if it is constructed to be emotional and arousing.

Countering the absorption and spread of disinformation

The research team identified several techniques in the literature that could be useful for countering disinformation absorption and spread. Two techniques to help counter disinformation were associated with more than one psychological principle: (1) preventive inoculation (i.e., warning people about the effects of disinformation and how to spot it) and (2) encouraging deeper, analytic thinking. The literature also details techniques that could combat the effects of a single psychological principle. For example, to counter the effects associated with groups, beliefs, and novelty, researchers recommend creating unique content that encourages individuals to identify with a broader "group" and increases their access to opposing information. In addition, researchers recommend that disinformation containment

Page 2715 of 3957

policies emphasize behavioral interventions aimed at countering the psychological principles activated by disinformation, rather than solely focusing on stopping the malicious use of bots, algorithms, and technologies. Before disinformation is shared, it is absorbed by an individual. Thus, interventions that disrupt how an individual absorbs disinformation should interrupt the chain between seeing disinformation and sharing it.

Page 2716 of 3957

This page intentionally left blank.

Page 2717 of 3957

Contents

Introduction **1**

Report elements 5
Report organization 6
Approach and sources 6

What Is Disinformation? **8**

Types of disinformation 11

Why Disinformation Matters **15**

Adversary use of disinformation 15
Domestic use of disinformation 18
Is disinformation effective? 19
Summary 22

Psychological Principles That Can Facilitate Disinformation Adoption and Spread **24**

Initial information processing (dual process theory) 25
Implications of initial information processing for disinformation 28
What can we do about it? 30
Cognitive dissonance theory 34
Implications of cognitive dissonance for disinformation 38
What can we do about it? 39
The Group, Belief, Novelty (GBN) model 42
Example of the GBN model using authoritarian attitudes 44
Implications of the GBN Model for disinformation 45
What can we do about it? 46
Emotions and arousal 48
Implications of emotionally arousing content for disinformation 50
What can we do about it? 51
Summary 52

Conclusion **53**

Glossary **54**

Figures **56**

Tables **57**

References **58**

Page 2718 of 3957

This page intentionally left blank.

Page 2719 of 3957

Introduction

On the morning of September 11, 2014—the anniversary of 9/11—the news in St. Mary Parish, Louisiana, was alarming. At around 8:30 A.M., the director of the regional Office of Homeland Security and Emergency Preparedness received a call from a citizen concerned about a text message suggesting that there had been a chemical spill: "Toxic fume hazard warning in this area until 1:30 PM. Take Shelter. Check Local Media and columbiachemical.com."

However, as reporters and analysts documented months later, the text message did not occur in isolation. Hundreds of Twitter accounts, many of which appeared to belong to concerned citizens in the area, used the hashtag #ColumbianChemicals to report on the unfolding crisis by asking questions, sharing pictures, and posting videos (Figure 1).

Figure 1. Twitter post showing the Columbian Chemicals plant explosion

Source: John Borthwick, "Media hacking," Render, Mar. 7, 2015, https://render.betaworks.com/media-hacking-3b1e350d619c.

At the same time, reporters and politicians as far away as New York City began to hear about the emergency. One user tweeted at New Orleans *Times-Picayune* reporter Heather Nolan:

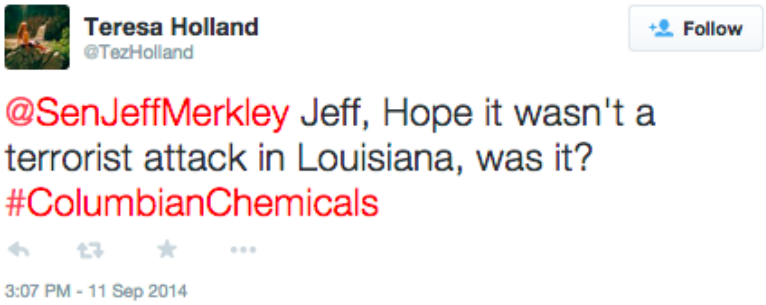
> @EricTraPPP: Heather, I'm sure that the explosion at the #ColumbianChemicals is really dangerous. Louisiana is really screwed now.

Another tweeted at political consultant Karl Rove:

> @zpokodon9: Karl, Is this really ISIS who is responsible for #ColumbianChemicals? Tell @Obama that we should bomb Iraq!

Yet another user tweeted at Oregon senator Jeff Merkley (Figure 2):

Figure 2. Twitter post asking Oregon senator Jeff Merkley about the Columbian Chemicals plant explosion



Source: Matt Kodama, "#ColumbianChemicals Hoax: Trolling the Gulf Coast for Deceptive Patterns," June 12, 2015, https://www.recordedfuture.com/columbianchemicals-hoax-analysis/.

Twitter was not the only platform involved. On YouTube, a video in which "a man showed his TV screen, tuned to an Arabic news channel, on which masked ISIS fighters delivered a speech next to looping footage of an explosion" suggested that ISIS [Islamic State of Iraq and Syria] was responsible for what was now being called an attack.[1] Another video, titled "Panic due to the explosion on a Columbian Chemicals facility in Louisiana," showed an ambulance on the highway. Yet another, titled "Flash from an explosion on a Columbian Chemicals facility in Louisiana," allegedly showed footage of the actual explosion.[2] A Wikipedia page, citing the video, became active, and a public Facebook page (called "Louisiana News") posted an article about the crisis and an alleged statement from ISIS in which the group claimed

[1] Adrian Chen, "The Agency," *New York Times Magazine*, June 2, 2015, accessed Feb. 2, 2021, https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[2] "Columbian Chemicals Plant Explosion Hoax," Know Your Meme, 2014, accessed Feb. 4, 2021, https://knowyourmeme.com/memes/columbian-chemicals-plant-explosion-hoax.

Page 2721 of 3957

responsibility for the attack. Finally, both the New Orleans *Times-Picayune* and CNN appeared to pick up the story as tweets of coverage on their websites began to circulate.

Figure 3. Twitter account posting a fake CNN homepage showing the story of the Columbian Chemicals plant explosion

Source: John Borthwick, "Media hacking," Render, Mar. 7, 2015, https://render.betaworks.com/media-hacking-3b1e350d619c.

All of this, however, was news to the people working at Columbian, *as there had not actually been any sort of leak or explosion*. The entire event had been fabricated, perpetuated by a

Page 2722 of 3957

skillfully coordinated social media infrastructure that included a botnet spreading content and "fully functional clones of the websites of Louisiana TV stations and newspapers."[3]

This particular hoax had a relatively small reach since none of the tweets went viral, the mainstream media did not report on the false story at the time if the ongoing operation, and its breakthrough at the national level came months later when *New York Times* reporter Adrian Chen linked the effort to Russia's now infamous Internet Research Agency (IRA). Yet, despite the hoax's failure, it is an almost perfect example of a disinformation campaign.

As the Columbian Chemicals example demonstrates, disinformation (i.e., false information created with the intent to deceive) has the potential to be concerning when it comes to national security. As adversaries and domestic actors alike increasingly use disinformation to achieve a variety of objectives, the study of how disinformation works and how it can be effectively countered has become a national security priority. Most of the study on this topic has thus far focused on disinformation tactics and tools. This report is different because it looks beyond these topics to examine how disinformation affects the recipient and the role psychology plays in one's acceptance of disinformation, since disinformation is a method of exercising psychological influence.

The primary impact of disinformation takes place in the mind. While the psychological principles behind the absorption of disinformation are normal principles invoked when individuals take in any type of information, malign actors can exploit these principles to enhance the likelihood of disinformation's assimilation and spread. Thus, understanding how to counter disinformation's impact requires a firm understanding of disinformation's effect on the mind.

To date, very little work on the subject of the psychology of disinformation has been aimed at policy-makers and defense decision-makers. This report seeks to fill that gap by detailing the psychological principles that allow disinformation to flourish in a way that is easy to understand for those with no psychology background. It can also serve as a primer for those new to the general topic of disinformation because it details the definition of disinformation and why it poses a national security threat.

[3] Chen, "The Agency." A botnet is a network of bots working in coordination. For additional information on the role of bots and botnets in propagating disinformation, please see Megan McBride, Zack Gold, and Kasey Stricklin, *Social Media Bots: Implications for Special Operations Forces*, CNA, DRM-2020-U-028199-Final, Sept. 2020, https://www.cna.org/CNA_files/PDF/DRM-2020-U-028199-Final.pdf.

Page 2723 of 3957

Report elements

To make this complex topic accessible and useful for practical application, there are several important elements of this study. First, for the purposes of this paper, *we make no distinction between disinformation and misinformation*. While the two concepts are distinct, with the intent of the information's creator (i.e., malicious versus benign) as the key difference, this paper instead focuses on the information itself and the effect on the person viewing or hearing it. In most cases, the recipient doesn't know who created the information (e.g., the meme, the video, or the email), so the creator's intent is irrelevant to the psychological impact of these types of disinformation on the audience. We will discuss and include examples of both disinformation and misinformation, categorizing them both as disinformation for simplicity (despite their definitional differences, which we recognize).

Second, the term *disinformation* has come to mean many different things to different people, with a number of distinct, though related, concepts at various times classified as disinformation. In this report, *we focus on the elements of disinformation included in a recent State Department-funded report*, and we make the conscious decision to leave out some of the other concepts occasionally included in this category. First, we exclude such techniques as the creation of fake accounts (bots, trolls, etc.) and fake communities. For our purposes, we consider these tools and actions to be part of "influence operations," a category that includes disinformation but is not exclusively composed of the disinformation itself. Second, while disinformation is a type of influence operation, not all influence operations are disinformation, so we also exclude influence operations that do not include disinformation. In other words, this study centers on the psychology of disinformation, and not on the broader psychology of influence operations. By scoping our report in this way, we are able to speak directly to a pressing national security risk in a clear, concise, and focused manner.

In addition, we are approaching this topic from a *nontechnical perspective*, with the intent of gearing explanations toward those with no prior knowledge of this subject. Therefore, we do not include the universe of potentially relevant psychological principles because that could get overwhelming and unwieldy. The psychological principles discussed in this report emerge from the literature as highly relevant to absorbing and spreading disinformation. Additional information on these principles can be gleaned from the cited material. Moreover, the tone of this study provides clear explanations and examples to make this report useful for its intended audience—policy- and decision-makers.

Page 2724 of 3957

Report organization

In addition to this introduction, this report has three sections all of which address important aspects of our study questions. We first describe what disinformation is within the scope of this report and hone in on the definition we then use for the remainder of the report. While there are many different and conflicting definitions of "disinformation," our first section outlines how we are defining the topic for purposes of this report.

Our second section addresses the issue of why the topic of disinformation, and therefore this paper, is important in the first place. While much has been written on disinformation, in most cases this particular question is sidestepped and the importance of disinformation is simply stipulated. To effectively counter this threat, it is critical to understand why it matters. Consequently, we begin with an exploration of why disinformation is important from a national security perspective before turning to the tricky question of whether disinformation is actually effective at achieving its objectives. We conclude with why it is important to study the psychology of disinformation as a part of this discussion.

With a firm grounding in what disinformation is and why it matters, we then turn to the psychological principles relevant to disinformation. While many principles are tangentially related to this topic, we chose to focus on the four mechanisms critical to the absorption and spread of disinformation: initial information processing; cognitive dissonance theory; the group, belief, novelty (GBN) model; and the effect of emotions and arousal. For each principle, we explain the concept in plain language (with examples) before detailing its implications for disinformation and what can be done to counter its effects.

This report ends with a brief conclusion that highlights the importance of continuing this area of study. The conclusion summarizes how this study has advanced the conversation on countering the spread of disinformation and highlights additional questions to address.

Approach and sources

This report relies primarily on a thorough review of the (1) disinformation and (2) psychology literature to pull out the information relevant to the national security space. For the first two sections on the what and why of disinformation, our primary sources are reports from think tanks and academic institutions as well as news reports, with CNA's previous studies on memes and bots serving as a foundation.[4] We also included some foreign language sources in the

[4] Vera Zakem, Megan McBride, and Kate Hammerberg, *Exploring the Utility of Memes for U.S. Government Influence Campaigns*, CNA, DRM-2018-U-017433-Final, 2018, https://www.cna.org/cna_files/pdf/DRM-2018-U-017433-Final.pdf; McBride, Gold, and Stricklin, *Social Media Bots: Implications for Special Operations Forces*.

Page 2725 of 3957

discussion of adversary use of disinformation to better understand the place disinformation has come to hold in adversary thinking, doctrine, and strategy.

For the third section, we conducted an extensive literature review of psychology journals. Where relevant, we also included literature from other disciplines (e.g., economics, computer science, and marketing). Finally, some of the psychological principles related to modern, technology-enhanced disinformation have roots in foundational experimental psychology. Where applicable, we discuss the root theory first and then apply it to disinformation.

Page 2726 of 3957

What Is Disinformation?

In the messy mainstream and social media ecosystem that characterizes the contemporary world, it is nearly impossible to untangle concerns about disinformation, misinformation, influence operations, adversary interference, propaganda, and online manipulation. Particularly problematic in the context of this report is the distinction between disinformation and misinformation. While these terms are often used interchangeably, they are distinct concepts easily differentiated by attention to the *intent of the content's creator* (Figure 4).

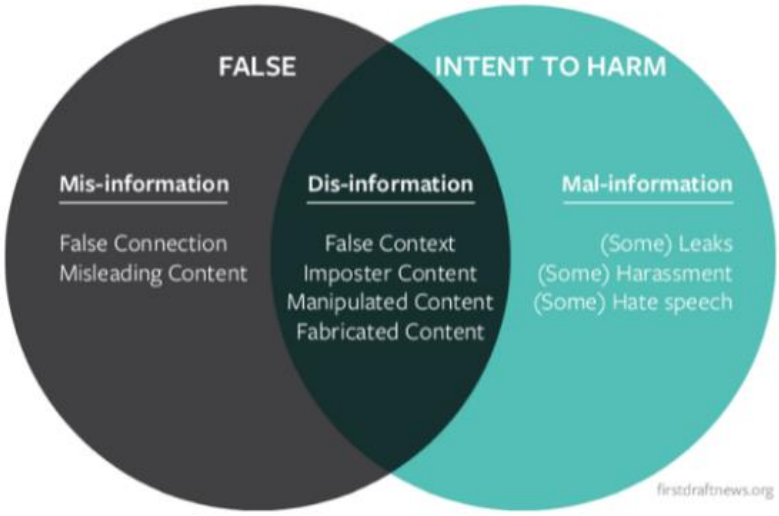
- *Disinformation* is information that is known to be false, and that is spread with the explicit goal of deceiving. In this case, the creator of the information (i.e., the tweet, the post, the email) *intends to deceive.*
- *Misinformation* is information that is false, but that is spread without a desire to deceive. In this case, the creator of the information (i.e., the tweet, the post, the email) has *no intention to deceive*.

It may also be helpful to add a third term to the mix:

- *Mal-information* is information that is known to be true, and that is spread intentionally, with the explicit goal of harming. One example might be sharing private information with the goal of harming the reputation of a politician. Mal-information is slightly different than disinformation and misinformation in that it is not necessarily false (it might contain false elements, but it might also be entirely true). We include it here, though, in an effort to provide a comprehensive oversight of the information ecosystem.

Page 2727 of 3957

Figure 4. Taxonomy of disinformation, misinformation, and mal-information



Source: Temir Asanov, "Fake News in Modern News Media: Disinformation, Misinformation and Malinformation," Medium.com, Mar. 17, 2019, https://medium.com/@tasanoff/fake-news-in-modern-news-media-disinformation-misinformation-and-malinformation-e4fdfa2ab571.

While this relatively simple taxonomy may seem to solve the problem, the reality is that the correct application of these labels (particularly those of disinformation and misinformation) is contingent on the tricky task of identifying the intent attached to the creation of the content.

To illustrate this, let's assume, for example, that Alice, Bernard, Claire, and David are active Twitter users.

One day, Alice wakes up planning to go to the beach with friends, but her mother insists that she wear sunscreen. Alice doesn't want to wear sunscreen because her friends don't wear sunscreen, so she creates a fake graphic detailing the negative consequences of wearing sunscreen and posts it to Twitter with the hashtag #sciencefacts. She then shows it to her mother in an attempt to get out of wearing sunscreen. In this case, the stakes are relatively low and modest, but we could accurately label this content as disinformation because Alice's post meets the criterion of that definition: *intentionally shared false information designed to deceive*.

A few days later, Bernard is on the subway and the people sitting across from him are having a heated debate about sunscreen (perhaps because they saw Alice's post). Bernard finds the argument against wearing it compelling. When he gets home, he creates a graphic to share with his friends. Because Bernard's graphic is not designed to deceive, it would be accurately

Page 2728 of 3957

categorized as misinformation: *information that is false but that is spread without the intent to deceive*.

These examples are relatively straightforward because in both cases we know the intention of the individual who created the content. Classifying content becomes far more complicated, though, when information is retweeted, reposted, and forwarded.

For example, imagine that a few weeks later Claire is online and she finds a graphic detailing the negative consequences of wearing sunscreen. Concerned about the data in the graphic, she shares it via social media. While in some ways Claire does the same thing as Alice and Bernard (sharing a graphic via social media), we need to know the intention of the graphic's *creator* in order to accurately categorize it. If Claire shared Bernard's graphic, then her earnest post would be misinformation: *information that is false but that is spread without a desire to deceive*. If, however, Claire had accidentally stumbled across Alice's graphic, then her post would meet the definition of disinformation, and Claire would simply be an unwitting accomplice in Alice's disinformation campaign. The difference, again, is in the intention of the content's original creator.

Because this report focuses on the *psychology of how disinformation works* (and not on, for example, adversary intentions) the distinction between disinformation and misinformation is not critical. It's true that the *perceived* or *assumed* intent of the content's originator is important; we read material generated by comedians (who we assume intend to amuse us) differently from how we read material generated by news organizations (who we assume intend to educate us). These perceived and assumed intentions, though, are facilitated by a set of cognitive shortcuts that we use to negotiate the world. We see the *New York Times* or *Wall Street Journal* banners and assume that we know the content creator's intent. Sometimes disinformation takes advantage of these heuristics—as the Columbian Chemical hoax creators did by creating a fake screenshot of the CNN website. This is possible because most of the time all we have are our perceptions and assumptions; most people don't know the origins of the material they view and share online, or the true intention of the person who created that content. As a result, we receive disinformation and misinformation the same way.

To hammer this home, let's take David's perspective. David is an everyday social media user scrolling through Twitter. Assuming he doesn't know anything about Alice, Bernard, or Claire, the graphics that he sees in their Twitter feeds are exactly the same. The disinformation/misinformation distinction just isn't relevant for David (i.e., for the end user or consumer), and, psychologically, disinformation and misinformation exploit the same principles. Note that, in many cases, these same principles are also exploited by those attempting to share accurate information. News agencies, as one example, will also rely on these principles to ensure that you visit their sites, view their channels, and click their links. The principles themselves are neutral and normal. This report, therefore, will not distinguish

Page 2729 of 3957

between disinformation and misinformation in discussing the relevant psychological principles; moreover, in an effort to avoid unnecessarily complicating things, we will use the term *disinformation* to refer to both throughout the remainder of this report.

Types of disinformation

While the definitions offered in the section above are accurate and useful, they fall short in capturing the range of material that analysts assess under the rubric of disinformation. A recent State Department-funded report, however, highlights the nuanced and complex nature of this phenomenon:

> To understand the disinformation environment, it is useful to dissect the different elements it encompasses. Disinformation can include authentic material used in a deliberately wrong context to make a false connection, such as an authentic picture displayed with a fake caption. It can take the form of fake news sites or ones that are deliberately designed to look like well-known sites. Disinformation can further include outright false information, shared through graphics, images, and videos. It can also take the form of manipulated image and video content, where controversial elements are photoshopped into innocuous contexts to evoke anger or outrage.[5]

In other words, understanding the psychological impact of disinformation isn't merely about understanding why a simple graphic might trick a few people. Disinformation exists in a context—it exploits our cognitive shortcuts and heuristics in order to be effective—that can be fabricated to varying degrees.

To take just the first part of the definition from the State Department report above, disinformation consists of not only patently inaccurate information designed to appear true (such as the Columbian Chemicals hoax), but also accurate information that has been manipulated or taken out of context. As one example, on September 20, 2015, a pro-Russia media outlet falsely claimed that US Ambassador John Tefft had been spotted at an anti-government rally earlier in the day.[6] In support of its claim, the website quoted Tefft as saying

[5] Christina Nemr and William Gangware, *Weapons of Mass Distraction*, Park Advisors, 2019, accessed Feb. 2, 2021, https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

[6] "US Ambassador to Russia John F. Tefft Is Sent to Opposition Rally in Maryino," Посла США в России Джона Ф. Теффта отправили на митинг оппозиции в Марьине, Ren.TV, Sept. 20, 2015, http://ren.tv/novosti/2015-09-20/posla-ssha-v-rossii-dzhona-f-teffta-otpravili-na-miting-oppozicii-v-marine.

Page 2730 of 3957

that he was attending the rally in order to assess the "caliber" of Russian democracy.[7] More interesting, the post included a photo of Tefft mid-interview, with the opposition rally visible behind him (Figure 5). The media outlet even tweeted the photo with the following caption: "US Ambassador to Russia John Tefft strolled at an opposition rally in Marino."[8]

Figure 5. Russian disinformation regarding US Ambassador Tefft

Source: "Посол США в России Джон Ф. Тефт прогулялся на митинге оппозиции в Марьино," Sept. 20, 2015, https://twitter.com/rentvchannel/status/645658877426593792.

[7] Some of this language remains in the REN TV article. Carl Schreck, "Photoshop Wars: U.S. Ambassador 'Attends' Russian Opposition Rally...and the Moon Landing," Radio Free Europe/Radio Liberty, Sept. 21, 2015, accessed Feb. 3, 2021, https://www.rferl.org/a/russia-photoshop-us-ambassador-tefft-opposition-rally-ren-tv/27260885.html.

[8] "The American Ambassador to Russia John F. Tefft Walked at an Opposition Rally in Maryino," Посол США в России Джон Ф. Тефт прогулялся на митинге оппозиции в Марьино, Twitter, Sept. 20, 2015, https://twitter.com/rentvchannel/status/645658877426593792.

Page 2731 of 3957

As the US Embassy in Russia promptly pointed out, though, the image was doctored. In fact, they tweeted a response that included the doctored image, the original image, and other doctored images of Ambassador Tefft at the moon landing and a hockey game (Figure 6).

Figure 6. US Embassy response to Russian disinformation regarding US Ambassador Tefft

Source: "The American Ambassador to Russia John F. Tefft Walked at an Opposition Rally in Maryino," Посол США в России Джон Ф. Тефт прогулялся на митинге оппозиции в Марьино, Twitter, Sept. 20, 2015, https://twitter.com/rentvchannel/status/645658877426593792.
Notes: The original image (upper left); the Photoshopped image that REN TV tweeted (upper right); Tefft at the moon landing (lower left); Tefft at a hockey game (lower right). Translation of Twitter post: Ambassador Tefft spent yesterday's weekend at home. But thanks to Photoshop you can be anywhere. #fake #fake.

In this case, the disinformation very clearly consisted of "authentic material used in a deliberately wrong context to make a false connection" and a manipulated image in which an innocuous element (Ambassador Tefft at a news conference) was Photoshopped into a controversial environment (an opposition rally) in order to "evoke anger or outrage." By

Page 2732 of 3957

contrast, the Columbian Chemicals disinformation campaign is one that involved "fake news sites or ones that are deliberately designed to look like well-known sites" and "outright false information, shared through graphics, images, and videos."

That said, the State Department definition—and, by extension, this report, as we have adopted the State Department definition—leaves out a number of techniques that are often included in discussions of disinformation campaigns but that are better classified as influence campaigns. It does not, for example, include instances in which a fake account or persona is used to spread true information, amplify the posts of a real person, galvanize a new community, or infiltrate a closed community to some ulterior end. There is no doubt an element of deception at play in these behaviors, but they don't meet the definition of disinformation and they rely predominantly on a different set of core psychological mechanisms (some, but not all, of which are explored in this report).

Disinformation poses a critical threat, but there is no standard for how it will look, where it will come from, or what tools might be necessary to identify it. As seen in the State Department definition, it can take many different forms: it can be a skillfully doctored screenshot of the CNN website or a typo-laden meme with no references; it can come from a friend or a media outlet or a stranger; and it might be easily traced via a simple Google query or impossible to track to its source. This project thus takes a different tack, focusing not on how disinformation can be identified but on how it affects—consciously and unconsciously—the recipients that are exposed to it and on how we might mitigate these effects.

Page 2733 of 3957

Why Disinformation Matters

Since the uncovering of widespread Russian meddling in the 2016 election, the US government, academics, think tanks, and social media companies have poured a wealth of resources into the study of disinformation. Every few months, Congress drags the leaders of the largest tech companies to Capitol Hill to grill them on their plans for countering the threat of disinformation; published reports on the issue now abound, tackling topics including Russian tactics, enabling technologies, and strategies for pushing back. Of interest, however, is that most of these resources seem to take for granted the fact that disinformation matters, rather than spelling out why that is the case. This chapter will endeavor to explain why we should care about disinformation, with a focus on the threat it poses in the national security context.

Adversary use of disinformation

While it is tempting to view adversary use of disinformation as a contemporary problem, the use of such means by adversaries attempting to shift the balance of political or military power is a long-standing issue. As just one example, in the first century CE, Octavian waged a fake news smear campaign—deploying primarily "short, sharp slogans written upon coins in the style of archaic Tweets"—to turn public opinion against Mark Antony and secure the role of first Roman Emperor.[9] Disinformation, however, has always been contingent on its ability to circulate widely; operating centuries before the printing press, Octavian had to use coins to spread his message. Consequently, it should come as no surprise that adversary use of disinformation has become something of an international crisis in the social media age, when information spreads globally—leaping between continents and across language barriers—in mere seconds. It should also come as no surprise that our adversaries would seek to weaponize this powerful tool.

The objectives of disinformation are situationally specific. In discrete instances, disinformation might be used to obscure the purpose of a military campaign or cast aspersions on an enemy. The type of disinformation that the modern world is struggling with—even when that disinformation is coming from adversaries—is typically far less restrained or limited. The most commonly cited goals for adversary use of disinformation include causing chaos and confusion, sowing discord, distracting from an issue, casting doubt, and making the truth seem

[9] Izabella Kaminska, "A Lesson in Fake News from the Info-Wars of Ancient Rome," *Financial Times*, Jan. 17, 2017, accessed Feb. 3, 2021, https://www.ft.com/content/aaf2bb08-dca2-11e6-86ac-f253db7791c6.

Page 2734 of 3957

unknowable.[10] However, while threatening in themselves, these short-term objectives may also be part of a broader long-term strategy for gaining global influence, diminishing US influence, claiming great power status, securing a regime, and more.[11] As states have increasingly become aware of the benefits of information for achieving these objectives (including the ease with which they can harness the power of social media, the inexpensive nature of these efforts, and the relatively low risk of engaging in such behavior), disinformation and related types of information influence have come to hold a more prominent place in many adversaries' doctrine, strategy, and thinking.

One of the US's primary adversaries in this space, Russia has come to view the information space as one of the foundational areas in which states compete today.[12] Rather than seeing the use of information (including disinformation) merely as support for traditional military operations during a conflict, Russia views it as integral to and indistinguishable from conventional capabilities, with utility during every phase of conflict and even in peacetime.[13] In fact, many Russian thinkers have asserted that the boundaries between war and peace are increasingly blurry, with the growing emphasis on nonmilitary means (such as information) asserted as one cause.[14] In 2013, the Russian Chief of the General Staff Valeriy Gerasimov stated that the development of information weapons had the ability to reduce an adversary's combat potential.[15] He further elaborated on this notion in 2019, writing that nonmilitary means are now the primary choice for attaining goals, with military force necessary only when nonmilitary means are unsuccessful.[16] Gerasimov also expressed that, while military means are decisive once armed conflict begins, nonmilitary means make it possible to create the

[10] Dean Jackson, "Issue Brief: How Disinformation Impacts Politics and Publics," National Endowment for Democracy, May 29, 2018, accessed Feb. 2, 2021, https://www.ned.org/issue-brief-how-disinformation-impacts-politics-and-publics/.

[11] Kasey Stricklin, "Why Does Russia Use Disinformation?," Lawfare, Mar. 29, 2020, accessed Feb. 2, 2021, https://www.lawfareblog.com/why-does-russia-use-disinformation.

[12] Daniel Kliman et al., *Dangerous Synergies*, CNAS, 2020, accessed Feb. 1, 2021, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Dangerous-Synergies-May-2020-DoS-Proof.pdf?mtime=20200506164642&focal=none.

[13] Makhmut A. Gareev, "Anticipate Changes in the Nature of War: Every Era Has Its Own Kind of Military Conflict, and its Own Constraints, and its Own Special Biases," Voyenno-Promyshlennyy Kuryer Online, June 5, 2013.

[14] Ibid.

[15] Valery V. Gerasimov, "The Value of Science is Foresight," Ценность науки в предвидении, VPK, ВПК, Feb. 26, 2013, accessed Feb. 1, 2021, https://vpk-news.ru/articles/14632.

[16] Ibid.; Valery V. Gerasimov, "Vectors of the Development of Military Strategy," Векторы развития военной стратегии, Krasnaya Zvezda, Красная звезда, Mar. 4, 2019, accessed Feb. 1, 2021, http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1.

conditions and influence the operating environment to make the employment of military means more effective.[17] In fact, it is thought that the use of such nonmilitary means as information can even preclude an armed conflict by allowing Moscow to assert influence and shape internal dynamics within an adversary state, creating conditions favorable to Russia.[18]

Another US adversary in this space, China has long sought to exercise control over information that circulates regionally, and has recently begun to extend its influence beyond its borders and neighbors.[19] In the last decade, the Chinese Communist Party has sought opportunities to shape the digital information space and, in 2013, Chinese President Xi Jinping stated that the use of innovative techniques to spread narratives positive for China, and promoting the Chinese view globally, was a priority.[20] The Chinese government has historically employed these tactics in regions close to its borders, such as Taiwan, to attempt to shape the geopolitical situation in a favorable manner.[21] These efforts were typically overt propaganda efforts to push Beijing's preferred narrative.[22] After the onset of the coronavirus pandemic, China began to take a page out of the Russian playbook, employing more covert disinformation on social media to obscure the virus's roots and shift the blame, typically to the US.[23] While it is unclear whether Beijing will continue to employ these methods after the pandemic has passed, the Chinese government has certainly evolved its thinking on how to use information for influence and the utility of disinformation in reinforcing the government's reputation.

Both Iran's conventional military and the Islamic Revolutionary Guard Corps (a parallel military structure tasked with upholding the ideals of the revolution) underscore the importance of informational control for offensive and defensive purposes alike.[24] Iran sees

[17] Gerasimov, "Vectors of the Development of Military Strategy."

[18] Kliman et al., *Dangerous Synergies*.

[19] Ibid., p. 5.

[20] Ibid.

[21] Joshua Kurlantzick, "How China Ramped Up Disinformation Efforts During the Pandemic," Council on Foreign Relations, Sept. 10, 2020, accessed Feb. 2, 2021, https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic.

[22] Sarah Cook, "Welcome to the New Era of Chinese Government Disinformation," *The Diplomat*, May 11, 2020, accessed Feb. 1, 2021, https://thediplomat.com/2020/05/welcome-to-the-new-era-of-chinese-government-disinformation/.

[23] "How China Ramped Up Disinformation Efforts During the Pandemic."

[24] "IRGC (Islamic Revolutionary Guard Corps)," Counter Extremism Project, accessed Feb. 3, 2021, https://www.counterextremism.com/threat/irgc-islamic-revolutionary-guard-corps; Emerson Brooking and Suzanne Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*, Atlantic Council, 2020, accessed Feb. 1, 2021, https://www.atlanticcouncil.org/wp-content/uploads/2020/02/IRAN-DIGITAL.pdf.

Page 2736 of 3957

itself as constantly on the defensive from information efforts emanating from other countries' broadcasters, lobbyists, and so on.[25] A recent report on Iran's digital disinformation efforts describes them as "public diplomacy under duress" and notes that pro-Iranian messaging proves most effective when it appears to come from a neutral third party.[26] Iran thus endeavors to set up a narrative structure that its adversaries cannot easily meddle with or take down in order to achieve its objectives, which include positioning itself as a leader in the Muslim world and serving as a bastion against perceived US and western regional intervention.[27]

The pandemic has seen these three adversaries increasingly amplify each other's disinformation, helping China's recent disinformation efforts gain a wider reach than they likely would otherwise. Despite varied objectives, the shared goal of undermining US influence has caused something of a convergence as Russia, China, and Iran work together to diminish the influence of their common adversary. For its part, the US government views disinformation in a patently different way than its adversaries. While many adversaries are increasingly emphasizing the utility of information for achieving a range of objectives, the US is grappling with a range of ethical and legal implications that simply are not issues for its adversaries in this space. As a result, it still does not have a clear strategy for countering information operations, and its efforts in this space tend to be largely reactive.[28] In addition, because the US views information influence through a different lens than many of its adversaries, the role of such efforts in adversary strategy and thinking is not always well understood. Therefore, the study of disinformation is important for ensuring that the US does not find itself unwittingly behind or vulnerable in a key area of competition.

Domestic use of disinformation

It would be naïve to write a paper on disinformation—especially one grappling with its real-world impacts—without acknowledging that domestic US actors are active in this space as well. As with adversary use of disinformation, the objectives for domestic actors using disinformation vary with prominent examples including attempts to shift political discourse on a range of controversial issues, such as election integrity, medical advice, and climate change. The objectives may also be motivated by a desire to garner support—measured in the form of votes, subscriptions, or clicks. Again, though, this is hardly a new phenomenon. In 1835,

[25] Brooking and Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*.

[26] Ibid.

[27] Ibid.

[28] Doowan Lee, "The United States Isn't Doomed to Lose the Information Wars," *Foreign Policy*, Oct. 16, 2020, accessed Feb. 3, 2021, https://foreignpolicy.com/2020/10/16/us-election-interference-disinformation-china-russia-information-warfare/.

The Sun (a newspaper in New York City) published a series of six articles claiming that life—including unicorns—had been observed on the moon by a one of the world's foremost astronomers. The hoax wasn't uncovered for weeks, and the newspaper never printed a retraction, but circulation did allegedly increase. The discovery of the hoax did not put an end to the practice; almost a decade later, *The Sun* again published fake science news. In this case, though, it was famed author Edgar Allen Poe who "sold an ingenious scientific hoax to a newspaper publisher for fifty dollars," though this time the newspaper apparently issued a retraction. [29]

In contemporary America, disinformation circulates on a variety of issues ranging from the absurd (e.g., a 2017 story that Hollywood elites were using "the blood of babies to get high") to the deadly serious (such as that related to the supposed dangers of the COVID-19 vaccine, which could deter large quantities of people from getting the vaccine).[30] The reality, though, is that the psychological mechanisms that allow disinformation to spread are the same, despite the motives of the individual behind such content or its potential impacts.

Is disinformation effective?

Given the variety and prevalence of disinformation, the existence of disinformation is not particularly debatable. Rather, the critical question remaining is whether disinformation is actually effective at changing peoples' minds and helping adversaries achieve their objectives. This effectiveness is incredibly difficult to assess; after all, it is difficult to know whether someone would have taken a certain action or had a certain thought even without the presence of disinformation.[31]

Several recent studies looking into the 2016 presidential election have attempted to answer the effectiveness question, often with disparate results. A 2018 study released by researchers from Ohio State concluded that disinformation likely helped Donald Trump secure victory because around 4 percent of Barack Obama's 2012 supporters did not vote for Hillary Clinton

[29] "Edgar Allan Poe—'The Balloon Hoax'," The Edgar Allan Poe Society of Baltimore, Last updated July 15, 2020, https://www.eapoe.org/works/info/pt049.htm.

[30] David Mikkelson, "Did Keanu Reeves Say Hollywood Elites Use the 'Blood of Babies' to Get High?," Snopes, Nov. 22, 2017, accessed Feb. 1, 2021, https://www.snopes.com/fact-check/keanu-reeves-blood-drinking/; Lois Beckett, "Misinformation 'Superspreaders:' Covid Vaccine Falsehoods Still Thriving on Facebook and Instagram," *The Guardian*, Jan. 6, 2021, accessed Feb. 3, 2021, https://www.theguardian.com/world/2021/jan/06/facebook-instagram-urged-fight-deluge-anti-covid-vaccine-falsehoods.

[31] "Issue Brief: How Disinformation Impacts Politics and Publics."

Page 2738 of 3957

after reading false stories about her.[32] By contrast, researchers from the Stanford Institute for Economic Policy Research released findings in 2017 showing that only a small portion of Americans saw the most widely circulated fake stories, suggesting disinformation during the election may not have been that convincing or influential, though the authors did not offer an opinion on whether this disinformation ultimately had an impact on the election outcome.[33] In January 2020, researchers released a study purporting to show that interaction with trolls from the Russian IRA during the 2016 election did not have any impact on Americans' political behaviors or thoughts because the trolls interacted most with individuals who already held strongly partisan attitudes and were unlikely to change their thinking.[34] However, the study's small sample size means that more research is needed on this topic for findings to be taken as conclusive. Therefore, none of these studies are decisive for answering the question of disinformation effectiveness. In addition, none of these studies explored the question of whether the disinformation campaigns might have affected voter turnout (i.e., perhaps suppressing Clinton voters and energizing Trump voters).

Most alarmingly, even if consumers of disinformation do not believe the false stories they read or change their attitudes or behaviors as a result, the very existence of disinformation or perception that it is spreading can help adversaries achieve their objectives. The perception that adversaries are excelling in the field of disinformation and may be manipulating events could help promote adversary goals by introducing doubt or anxiety about government institutions, journalistic outlets, and other staples of democracy. Russia, for example, often promulgates a number of narratives on unfolding events, not because it hopes that audiences will believe all of the various, often contradictory, messages, but because doing so makes the truth seem unknowable, and makes citizens doubt the official government versions of events. Russia hopes the long-term effect will lead to democratic systems appearing less appealing, engendering a loss of US influence worldwide, while making political systems similar to the one found in Russia seem stronger and more effective in contrast.[35]

---

[32] Aaron Blake, "A New Study Suggests Fake News Might Have Won Donald Trump the 2016 Election," *The Washington Post*, April 3, 2018, accessed Feb. 1, 2021, https://www.washingtonpost.com/news/the-fix/wp/2018/04/03/a-new-study-suggests-fake-news-might-have-won-donald-trump-the-2016-election/.

[33] Krysten Crawford, "Stanford Study Examines Fake News and the 2016 Presidential Election," Stanford News, Jan. 18, 2017, accessed Feb. 2, 2021, https://news.stanford.edu/2017/01/18/stanford-study-examines-fake-news-2016-presidential-election/.

[34] Christopher Bail et al., "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *PNAS: Proceedings of the National Academy of Sciences of the United States of America* 117, no. 1 (2020), accessed Feb. 3, 2021, https://www.pnas.org/content/117/1/243.

[35] "Why Does Russia Use Disinformation?"

Page 2739 of 3957

While it is unclear if disinformation can actually change an individual's opinion, attitude, or vote on a specific issue, there are many examples where disinformation has affected behaviors. The psychological principle of cognitive dissonance (to be discussed later) posits that one's actions have a powerful effect on one's attitudes since you need to rationalize to yourself why you are doing something. Furthermore, it has been shown to affect the national discourse on a variety of topics and to even sometimes make its way into the mainstream media. This is at least partially because disinformation on social media has proved to spread more widely and more rapidly than accurate information. A large 2018 MIT study of Twitter data found that, according to every normal metric, disinformation wins out over the truth on social media by diffusing "significantly farther, faster, deeper, and more broadly than the truth in all categories of information."[36] The authors concluded that this was true because of human nature, rather than the use of bots, because the bots studied in the report amplified just as many true stories as false stories.[37]

In some cases, the promulgation of disinformation has spurred real-world events, and even violence. Countries such as India and Burma have seen social media used to spread disinformation on religious minorities that led to actual violence.[38] An additional salient example was the 2005–2006 rallies in response to the publication of images of Muhammad in a series of European newspapers, which resulted in violence around the world, leading to over 100 deaths and 800 injuries. An often-overlooked component of this dynamic, though, was an informal publication known as the Akkari-Laban dossier. This document, written by Danish-Muslim clerics, was shared widely across the Muslim world. While experts later confirmed that much of its content was accurate, they also noted that it contained inflammatory and false information. Specifically, the dossier implied that one of the images it contained (of a picture of a man dressed as a pig) was meant to depict Mohammad when, in fact, it was an Associated Press photo of a French pig-squealing contest.[39] The dossier did contain accurate images of cartoons as well, but the inclusion of this especially inflammatory image makes it an example of disinformation. It is an instance in which "authentic material" (i.e., the Associated Press image) was "used in a deliberately wrong context to make a false connection" (i.e., implying that the image was part of a larger effort to disrespect Islam).[40] Again, it is impossible to know if this particular image—one among many—was directly responsible for causing the rallies,

[36] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (2018), https://science.sciencemag.org/content/359/6380/1146.

[37] Ibid.

[38] "Issue Brief: How Disinformation Impacts Politics and Publics."

[39] Martin Asser, "What the Muhammad Cartoons Portray," BBC, Jan. 2, 2010, http://news.bbc.co.uk/2/hi/middle_east/4693292.stm.

[40] Nemr and Gangware, *Weapons of Mass Distraction*.

Page 2740 of 3957

violence, injuries, and death. Its inclusion, though, is widely recognized to have exacerbated an already delicate situation (because Islam identifies the pig as an unclean animal) and thus contributed to significant real-world consequences.

Summary

It is not always immediately clear exactly why disinformation matters for national security or whether the spread of disinformation is even having an effect. While much has been done to map out adversary disinformation tactics and the digital space that enables them, this work often takes for granted the fact that we should be studying disinformation in the first place. There are, however, demonstrable reasons why it is important to pay attention to disinformation. As adversaries and domestic actors alike increasingly turn to information means as a way to achieve a range of objectives, the study of disinformation is also growing more important to ensure that malign actors do not catch the US flat footed. While it is difficult to prove that disinformation is effective in directly changing minds or votes, there is much evidence it can affect behaviors and discourse. In addition, the lack of conclusive study on whether disinformation is effective means that we cannot discount it; just as we do not know exactly how effective disinformation is, we also cannot prove that it is *not* effective. The issue, therefore, requires greater attention and study.

That study should center not just on disinformation tactics but also on how those tactics affect the mind since disinformation's primary impact occurs in the mind. It is by definition a method of exercising psychological influence. Those spreading disinformation hope that a recipient will believe it, thus allowing the promulgators to achieve their objectives. As mentioned, though, disinformation can have an impact even if it is not believable; the mere perception that disinformation exists may be enough to lead to certain effects, such as the erosion of trust in democratic institutions and the media. This perception, of course, is a mental process as well.

The impact of disinformation, however, is not *limited* to the mind. It can have concrete and critical secondhand effects beyond the foregoing examples of real-world violence. For example, the erosion of trust in democratic institutions can affect voting behavior, increased suspicions about medical care can change willingness to receive that care, and distrust of the police can lead to increased resistance to arrest. As a result, it is important to understand not merely the technical issues of how disinformation is transmitted or how it can be prevented—issues that have received considerable attention over the past few years—but also the psychological question of how disinformation works and how it can be countered. Increased familiarity with the psychology of disinformation is important for understanding how the spread of false information aids in the achievement of objectives and, in turn, how to prevent its harmful impacts. Moreover, because countering the effects of disinformation is also a cognitive process, understanding the psychological principles that make disinformation effective can assist in

Page 2741 of 3957

understanding what principles may counter it. As the use of disinformation and other types of psychological influence become more important to the achievement of malign objectives for both adversaries and domestic actors, understanding how to counter these tactics more efficiently is a national security imperative.

Page 2742 of 3957

Psychological Principles That Can Facilitate Disinformation Adoption and Spread

This section addresses why people are vulnerable to disinformation by examining innate psychological mechanisms that govern how people process and share information. The primary thesis of this section is that disinformation is processed and shared through *routine and ordinarily adaptive psychological processes.*[41]

We begin by describing the psychological principles associated with initial information processing and the subsequent reinforcement of initial judgments through cognitive dissonance. Next, we describe how group membership, beliefs, and novelty affect the way we process and communicate information. Finally, we describe the role of emotion and arousal in people's tendency to share information. In each section, we describe the principles, apply them to disinformation specifically, and describe how normal, routine, and adaptive processes can be used to further spread disinformation. We also describe how these principles can be used to counter the spread of disinformation. Table 1 summarizes these psychological principles, provides a brief explanation, and shows the connection between that concept and disinformation.

[41] Here, the word *adaptive* is used in an evolutionary context. Behavior is adaptive if it helps a person to accomplish a goal.

Page 2743 of 3957

Table 1. Psychological principles relevant for disinformation adoption and spread

Principle	Explanation	Application to disinformation
Initial information processing	We process information as efficiently as possible and that can make us vulnerable to mistakes.	We can accept disinformation as true because we aren't thinking deeply and critically.
Cognitive dissonance	When we are confronted with something that goes against our beliefs, we are motivated to resolve the conflict.	We accept disinformation that supports our initial beliefs and try to reject information that disconfirms our initial beliefs.
Group, belief, and novelty	We more readily share information with people with whom we identify, when we believe it is true, and when it is novel or urgent.	We accept and share disinformation more readily when it comes from people we know, it appeals to what "our group" believes, and when we think it is new.
Emotions and arousal	We pay more attention to information that makes us feel positively or arouses us to act.	We are more likely to share disinformation if it is constructed to elicit high-arousal emotions.

Source: CNA.

Humans are constantly processing information that comes in through our senses. Encoding, cataloging, deciding on action, and storing all that information could be a full-time job without mechanisms to efficiently process it all. Indeed, we don't have the "computing power" to appropriately process each new piece of information as entirely novel. This section describes multiple psychological theories and their effects. They all come down to the same bottom line: our brains have adaptive mechanisms to triage and organize information as quickly and efficiently as possible.

Initial information processing (dual process theory)

Dual process theory is the foundation for understanding how people process information.[42] The theory posits that we have two mechanisms to evaluate new information that comes in through our senses. Table 2 describes the key elements of these two processes: automatic thinking and controlled thinking.

[42] Shelly Chaiken and Yaacov Trope, *Dual-Process Theories in Social Psychology*, (New York: Guilford Press, 1999); Susan T. Fiske and Shelly E. Taylor, *Social Cognition: From Brains to Culture*, 3rd ed. (London: SAGE Publishing, 2016).

Page 2744 of 3957

Table 2. Dual process theory

Process	Characteristics	How it works
Automatic thinking	Fast, effortless, uses few resources	People rely on previous experience with similar information and best guesses (heuristics), easy-to-process information (fluent), and information that is easy to remember to determine how to think about new information and act on it with very little "thought"
Controlled thinking	Slow, deliberate, requires many cognitive resources	People rely on analytical and deep thinking involving questioning assumptions to understand and act upon new information

Source: CNA.

The first process, called *automatic*, requires very little effort and is fast, efficient, and "cognitively cheap." Essentially, when the information comes in, it is immediately associated with something already known and is dealt with or "filed away" appropriately. For example, if someone were driving the same road to work every day and came upon their exit sign, they would automatically turn on their signal and proceed to the exit ramp. This action requires very little thought. Kahneman argues that attention requires effort and that we conserve mental energy by focusing on only a few things and letting automatic processes handle the rest.[43]

The second process is called *controlled*. Controlled processes are slower, more cognitively involved, and require deliberate attention. Going back to the driving example, if the exit you were expecting to see was closed, your brain would begin controlled processes to determine alternative routes for getting to work. While the theory posits two processes, researchers acknowledge that there is really a gradient from the most automatic to the most controlled processes.[44] Fully automatic processes are those that are completely unintentional and happen with little or any cognitive awareness. As processes become more controlled, your brain recognizes novel information and attends more deeply to it. And for processes that are more fully controlled, people are more likely to seek additional information and think about whether the information they have is accurate.

[43] Daniel Kahneman, *Thinking, Fast and Slow*, (New York: Farrar, Straus, and Giroux, 2011).

[44] Fiske and Taylor, *Social Cognition: From Brains to Culture*.

Page 2745 of 3957

The amount of information that people can respond to at any given time is finite,[45] so they default to the processing option that requires the lowest level of effort.[46] This makes our brains highly efficient because we do not waste resources thinking more deeply about things than we need to. There is a downside, however: we can make mistakes. Returning to the exit ramp example, if the exit sign that we see every day is blocked or closed, using the automatic processes to proceed as usual can be dangerous. If we fail to recognize the blocked exit information as important to attend to, we can make mistakes.

Heuristics are one of the primary means used to determine the appropriate level of attention to give information. Heuristics are mental shortcuts we use to make sense of the world.[47] Heuristics are developed through previous experience and connections we make between similar pieces of information. For example, if you have lived in a given climate for several years, you have a heuristic about what the likely temperature will be in January. Most of the time, you will be close to correct and you can dress for the day without checking the temperature. However, *some* days you will be wrong—it will be abnormally warm or cold—and your choice of clothes will be inappropriate. By definition, heuristics are correct (or close enough) most of the time, but can lead to huge errors at other times.

In addition to heuristics, information fluency affects our likelihood of processing information and the depth at which we process it. Information fluency refers to how easily people process information. Processing is more fluent if the information is easier to understand (this includes font, color contrast, accent, and cadence in addition to actual message content).[48] In addition, information that is easier to understand is more likely to be incorporated into what someone believes, regardless of whether it is true.[49] Information that is easy to understand "feels right" and so it seems true.[50] Once that information is incorporated into our scheme, it becomes

[45] Researchers demonstrated that individuals can reliably recall five to nine pieces of information reliably. Beyond that, they are inconsistent or unable to accurately recall. (T. L. Saaty and Müjgan Sagir Özdemir, "Why the Magic Number Seven Plus or Minus Two," *Mathematical and Computer Modelling* 38 (2003), doi: 10.1016/S0895-7177(03)90083-5.).

[46] Fiske and Taylor have coined the term *cognitive miser* to describe the tendency to process information at the lowest acceptable level of effort.

[47] Daneil Kahneman and Amos Tversky, "On the Psychology of Prediction," *Psychological Review* 80, no. 4 (1973).

[48] Christian Unkelbach, "Reversing the Truth Effect: Learning the Interpretation of Processing Fluency in Judgments of Truth," *Journal of Experimental Psychology: Learning, Memory, and Cognition* 33, no. 1 (2007), doi: 10.1037/0278-7393.33.1.219.

[49] Ibid.

[50] Tommy Shane, "The Psychology of Misinformation: Why We're So Vulnerable," First Draft News, June 30, 2020, https://firstdraftnews.org/latest/the-psychology-of-misinformation-why-were-vulnerable/.

Page 2746 of 3957

previous knowledge that we can use to build more heuristics and make future judgments about new information.

Another important cognitive psychological principle that influences what we remember is the primacy and recency effect.[51] It is easier for people to remember information that is presented first (primacy) and presented most recently.[52] Studies demonstrating the primacy and recency effect traditionally focused on which words in a list people could remember. The primary and recency effect was displayed when people were more likely to remember the first few and the last few words presented. Studies have also shown that the primacy effect is particularly important for determining what website links people choose.[53] People most often click the links listed first in a search, for example.

Implications of initial information processing for disinformation

The phenomenon of spreading disinformation may appear to be the result of ideology and deep commitment to the material. However, some research suggests that's not the case. Pennycook and Rand demonstrated that individuals who were more prone to think deeply about issues (based on their Cognitive Reasoning Test score) were more able to discern fake from real news and were *more* discerning regarding information that was ideologically consistent than information that was ideologically inconsistent.[54] The implication of this work is that susceptibility to fake news is driven more by "lazy thinking" than it is by entrenched belief structures. Therefore, if people thought more deeply (i.e., used more controlled and less automatic processes), they would be less likely to believe and share disinformation.

Routine initial information processing mechanisms are adaptive and help people to quickly organize information, make sense of it, and decide on action to take. However, the efficiency in these processes leaves people vulnerable to making mistakes and processing information incorrectly. The default automatic processing, relying on heuristics and information fluency, leaves us with "blind spots" that prevent us from recognizing when we need to slow down to distinguish information from disinformation.[55] This results in credible information and

[51] Bennet B. Murdock., Jr., "The Serial Position Effect on Free Recall," *Journal of Experimental Psychology* 64, no. 5 (1962), doi: https://doi.org/10.1037/h0045106.

[52] Cong Li, "Primacy or Recency Effect? A Long-Term Memory Test of Super Bowl Commercials," *Journal of Consumer Behavior* 9, no. 1 (2009).

[53] Jamie Murphy, Charles Hofacker, and Richard Mizerski, "Primacy and Recency Effects on Clicking Behavior," *Journal of Computer-Mediated Communication* (2020).

[54] Gordon Pennycook and David G. Rand, "Lazy, Not Biased: Susceptibility to Partisan Fake News Is Better Explained by Lack of Reasoning than by Motivated Reasoning," *Cognition* 188 (July 2019), doi: https://doi.org/10.1016/j.cognition.2018.06.011.

[55] Kahneman, *Thinking, Fast and Slow*.

Page 2747 of 3957

disinformation being treated the same and can lead one to miscategorize disinformation as true.

Automatic thinking makes it likely that miscategorized information will be used. Familiarity plays in our initial information processing. Rather than rely on controlled processes to evaluate the veracity of new information, if the new information is similar to something we are familiar with, we might use a heuristic and assimilate the new information just as we did the old information. The Columbian Chemicals example, described in the introduction, demonstrates how the natural tendency to use automatic thinking could have influenced the spread of that fake story. As noted, the story spoofed the CNN website banner and logo. People familiar with the CNN logo and reputation as a news outlet were likely to use those heuristics to determine that *this* CNN story was as credible as others. Therefore, they may have shared it to inform others of the supposed harm from the explosion.

Information that is more familiar to us (repeatedly presented) is more likely to be recalled as true.[56] This is called the illusory truth effect, when familiarity with something gives the illusion that it is more accurate, and that inadvertently increases someone's belief in that information.[57] This can be especially problematic when attempting to correct disinformation because the correction often repeats the original claim.[58] Swire provides a clear and illustrative example of this challenge:

> Truthfully stating that playing Mozart to your child will *not* boost its IQ mentions the two concepts of "Mozart" and "increased IQ," thereby making the link between the concepts more familiar even though the statement seeks to dispel the Mozart-IQ myth. This inadvertent increase in familiarity may reduce the effectiveness of the correction and may thus contribute to the continued influence effect of misinformation [emphasis in original].[59]

---

[56] Nicholas DiFonzo et al., "Validity Judgments of Rumors Heard Multiple Times: The Shape of the Truth Effect," *Social Influence* 11 (2016), doi: https://doi.org/10.1080/15534510.2015.1137224.

[57] Ian Maynard Begg, Ann Anas, and Suzanne Farinacci, "Dissociation of Processes in Belief: Source Recollection, Statement Familiarity, and the Illusion of Truth," *Journal of Experimental Psychology: General* 121, no. 4 (1992), doi: https://doi.org/10.1037/0096-3445.121.4.446.

[58] Some researchers have argued for a "truth sandwich" to counter this phenomenon. In a truth sandwich, you would say the truth, refute each point in the disinformation, then repeat the truth. This puts the truth first and last, using the cognitive principles of primacy and recency. It also mitigates the tendency for repeating the lie to make it more accepted. However, the usefulness of a truth sandwich in combating disinformation has not yet been empirically investigated to our knowledge.

[59] Briony Swire, Ulrich K. H. Ecker, and Stephan Lewandowsky, "The Role of Familiarity in Correcting Inaccurate Information," *Journal of Experimental Psychology: Learning, Memory, and Cognition* 43, no. 12 (2017), doi: 10.1037/xlm0000422.

Page 2748 of 3957

Automatic processing does not provide deep consideration of information (source, context, etc.). Thus, when processing automatically, individuals might be more likely to recall repeated information without the context of *why* it was repeated to them. This causes errors in judgment. When those errors in judgment allow us to encode disinformation as true, it is very challenging to undo.

Once we make initial judgments about information, they become part of our scheme and how we understand the world. If that information is inaccurate (because of disinformation or a mistake in processing or remembering), we can be left with encoded inaccurate information to draw from later. There is a memory effect associated with the likelihood of recalling disinformation as opposed to the idea that the disinformation was debunked. The continued influence effect describes how corrected disinformation can continue to influence memory and reasoning.[60] Examples are the persistence of people's belief that Michael Jackson invented the moonwalk, Edison the lightbulb, and Guillotin the guillotine.[61] Essentially, this theory posits that disinformation, once acquired, is very difficult to correct (unlearn). Corrections through debunking and fact-checking can "fail" to correct because the disinformation can be recalled later as fact separate from the debunked information. Essentially, both pieces of information are stored in a person's memory: the disinformation and the disinformation plus the correction. A correction fails when the disinformation is recalled without the correction. Swire, Ecker, and Lewandowsky found that effective corrections (those that have a lot of detail and affirm the facts) can "wear off" in a week and the participants will retell the inaccurate information.[62] Dual process theory and the tendency toward automatic processing may be partially responsible for this phenomenon. If the disinformation was easier to understand and recall, or more familiar than the correction information, then when confronted with new information, we are more likely to rely on the disinformation.

What can we do about it?

Given the difficulty of correcting disinformation once present in a person's memory, it is more fruitful to attempt to *prevent* disinformation from taking root than to *correct* disinformation that has been encoded as truth. Here we focus on two relevant avenues for combating disinformation: the first is bolstering our own internal toolkit, and the second is helping those around us. Table 3 summarizes the prevention mechanisms described in detail in this section.

[60] Ulrich K. H. Ecker et al., "Correcting False Information in Memory: Manipulating the Strength of Misinformation Encoding and its Retraction," *Psychonomic Bulletin & Review* 18 (2011), doi: 10.3758/s13423-011-0065-1.

[61] Bianca Pellegrino, "People Famous For Doing Things They Didn't Do," ListVerse, Sept. 8, 2019, https://listverse.com/2019/09/08/top-10-people-famous-for-doing-things-they-didnt-do/.

[62] Swire, Ecker, and Lewandowsky, "The Role of Familiarity in Correcting Inaccurate Information."

Page 2749 of 3957

Table 3. Disinformation prevention mechanisms for initial information processing

	Concept	Description
Internal (with yourself)	Skepticism	Recognizing that people might have hidden agendas, scrutinize information presented to you
	Alertness	Warnings about the effects of disinformation can make you more alert to the possibility
	Analytic thinking	Purposefully make deliberate, controlled, thoughtful evaluations of new information
External (with others)	Create friction	Asking questions that make others process information more deliberately (e.g., asking, "what makes you say that?")
	Inoculation	Provide awareness of possible disinformation so others can recognize it when confronted by it later
	Nudges	Provide subtle cues of the behavior you want someone to exhibit; in this case, processing information more deliberately

Source: CNA.

Bolstering your resistance to disinformation

The first preventive mechanism we describe involves building resistance to disinformation in your own information processing. There are three concepts, all of which can be taught, that guard against the inadvertent adoption of disinformation: skepticism, alertness, and analytic thinking.[63] All three of these processes for individually combating disinformation require the person to move from a greater reliance on automatic to a greater reliance on controlled processes.

Skepticism is the awareness of possible hidden agendas and a personal desire to understand the evidence.[64] It works to fight disinformation because skepticism requires the person to use more cognitive resources to evaluate information.[65] Research indicates that skepticism can be encouraged and trained through exposure to and discussion of pseudoscience and false advertising campaigns.[66]

[63] Tommy Shane, "The Psychology of Misinformation: How to Prevent It," First Draft News, July 27, 2020, https://firstdraftnews.org/latest/the-psychology-of-misinformation-how-to-prevent-it/.

[64] Ruth Mayo, "Cognition Is a Matter of Trust: Distrust Tunes Cognitive Processes," *European Review of Social Psychology* 26 (2015), doi: https://doi.org/10.1080/10463283.2015.1117249.

[65] Briony Swire and Ulrich K. H. Ecker, "Misinformation and Its Correction: Cognitive Mechanisms and Recommendations for Mass Communications," in *Misinformation and Mass Audiences*, ed. Brian Southwell, Emily A. Thorson, and Laura Sheble (Austin: University of Texas Press, 2018).

[66] Rodney Schmaltz and Scott Lilenfeld, "Hauntings, Homeopathy, and the Hopkinsville Goblins: Using Pseudoscience to Teach Scientific Thinking," *Frontiers in Psychology* 5 (2014), doi: https://doi.org/10.3389/fpsyg.2014.00336.

Page 2750 of 3957

Alertness is a heightened awareness to the effects of disinformation.[67] Warning people about the effects of disinformation—such as the continued influence effect (i.e., the way that once disinformation becomes part of our schema for processing the world, it can be difficult to correct)—can reduce the continued reliance on disinformation, but it will not eliminate it.[68] Research shows that the *specific* description of the continued influence effect had the greatest impact for countering disinformation. More general warnings about the possibility of publishing unverified information are not as effective as a specific warning.

Analytic thinking involves deliberate, controlled, thoughtful evaluation of information as opposed to quick, automatic judgments. Bago, Rand, and Pennycook performed an experiment in which they asked people to make initial (automatic) judgments under time constraints while doing other tasks.[69] Then they asked the participants to reconsider the information without time constraints. They found that deliberation (controlled, analytic thinking) was associated with more accurate perceptions than initial judgments (automatic) made under constrained conditions. This finding indicates that, with deliberation, people can more accurately discern the true information from the false, even if they first made incorrect initial judgments.

Bolstering resistance to disinformation in others

The second avenue to combat disinformation believed because of initial processing errors involves attempts to influence other people's encoding of disinformation. Similar to the individual and internal mechanisms described previously, these techniques are based on the premise that deeper thinking can overcome fallacies in initial, automatic processes. Three related techniques can be used to interrupt the automatic information processing of others: creating friction, inoculation, and nudges.[70]

Friction is the opposite of fluency. Whereas fluency consists of information that is easy to process, understand, and incorporate, friction occurs when something is difficult to process. Fazio found that adding friction to processing by asking people to explain why they think a headline is true or false reduced their likelihood of sharing stories with false headlines and had

[67] "The Psychology of Misinformation: How to Prevent It."

[68] Ulrich K. H. Ecker, Stephan Lewandowsky, and David T. W. Tang, "Explicit Warnings Reduce But Do Not Eliminate the Continued Influence of Misinformation," *Memory and Cognition* 38 (2010), doi: 10.3758/MC.38.8.1087.

[69] Bence Bago, David G. Rand, and Gordon Pennycook, "Fake News, Fast and Slow: Deliberation Reduces Belief in False (But Not True) News Headlines," *Journal of Experimental Psychology: General* 149, no. 8 (Aug. 2020), doi: 10.1037/xge0000729.

[70] "The Psychology of Misinformation: How to Prevent It."

Page 2751 of 3957

no effect on the likelihood of sharing stories with true headlines.[71] The implication here is that, if someone is asked to justify the veracity of something prior to sharing it, they are *less likely* to spread disinformation. Creating friction increases the depth at which individuals have to process information. Those who engage in more reflective thinking have been shown to be more discerning in their social media use. Mosleh and colleagues demonstrated that those who were higher in reflective thinking were more selective about whom they followed, shared news content from more reliable sources, and tweeted about more substantive topics.[72] It is relevant to note that Mosleh's study looked at reflective thinking as a trait, not a state that could be induced through friction. However, the finding is consistent with Fazio's finding regarding induced deep processing.

Inoculation involves building preemptive resistance to disinformation by exposing people to examples of disinformation or disinformation techniques to help them recognize and reject them in the future.[73] This is similar to the concept of inoculation to viruses through the use of vaccines, where individuals are given a small dose, or antibodies for, a disease and that allows a body to prepare an informed defense against it.[74] Cook, Lewandowsky, and Ecker experimentally tested multiple preemptive interventions designed to reduce the effect of disinformation and found that inoculating messages that explain flawed arguments or highlight real scientific consensus on climate change affected climate attitudes.[75] The most substantial effect was on attitudes of perceived consensus in the scientific community; however, other attitudes (including increased trust in climate scientists and decreased trust in contrarian scientists) were also observed. Those that were inoculated were more likely to express perceived consensus among scientists, trust in climate scientists, and decreased trust in contrarian scientists than those who were not inoculated. The implication of these findings is that inoculation *prior to* presentation of disinformation can buffer the disinformation from affecting the individual's perceptions.

The concept of "nudging," introduced by Richard Thaler, involves providing small and subtle suggestions to encourage the type of behavior you want someone to perform or the decision

[71] Lisa K. Fazio, "Pausing to Consider Why a Headline Is True or False Can Help Reduce the Sharing of False News," *Harvard Kennedy School (HKS) Misinformation Review* 1, no. 2 (2020).

[72] Mohsen Mosleh et al., "Cognitive Reflection Correlates with Behavior on Twitter," *Nature Communications* 12, no. 921 (2021).

[73] "The Psychology of Misinformation: How to Prevent It."

[74] Gustav J. Nossal, "Vaccination," in *Encyclopedia of Life Sciences*, (Hoboken, NJ: Wiley, 1999), www.els.net.

[75] John Cook, Stephan Lewandowsky, and Ulrich K. H. Ecker, "Neutralizing Misinformation Through Inoculation: Exposing Misleading Argumentation Techniques Reduces Their Influence," *PLoS ONE* 12, no. 5 (2017), doi: https://doi.org/10.1371/journal.pone.0175799.

Page 2752 of 3957

you want them to make.[76] Single-serve snack packaging is an example of a nudge. The manufacturer is suggesting the quantity for one sitting, but the person is free to eat more than one single-serve snack in a sitting. In the realm of disinformation, a nudge would subtly prompt more analytical (controlled) thinking.[77] Pennycook and colleagues measured participants' truth discernment and willingness to share a headline with or without a nudge about accuracy in headlines.[78] Note that, in this case, they were not provided a lecture on the importance of accuracy or prevalence of inaccuracy on the internet. They were simply asked to make a judgment about the accuracy of a single headline (unrelated to the topic). They were then shown other headlines and asked how likely they were to share them on social media. The researchers found that participants were more likely to share true headlines (relative to false headlines) if they had been asked to rate the accuracy of a single headline.[79] Asking them to consider accuracy was a subtle nudge before they were asked if they would share a headline. This finding demonstrates that a minor, unobtrusive, and nonthreatening "nudge" can affect the likelihood of sharing false information on social media, even on a topic unrelated to the disinformation that might be shared.

Cognitive dissonance theory

Cognitive dissonance happens when a person is confronted with two competing thoughts. For example, a person might simultaneously think the following: Exercise is good for my body; when I exercise, it hurts. It is uncomfortable to hold two competing ideas/beliefs at one time. Therefore, people are motivated to reduce the conflict or remove the dissonance.

Dissonance theory describes how people are influenced to either accept or reject beliefs, as well as the information/arguments that accompany those beliefs. The theory includes both cognitive and emotional components. It posits that people feel uncomfortable when they have to reconcile conflicting information. Conflicting information is dissonant, whereas nonconflicting information is consonant, consistent, or compatible (we will use these as synonyms here).

---

[76] Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness*, (New Haven, CT: Yale University Press, 2008).

[77] "The Psychology of Misinformation: How to Prevent It."

[78] Gordon Pennycook et al., "Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy Nudge Intervention," *Psychological Science* 31, no. 7 (2020), doi: https://doi.org/10.1177/0956797620939054.

[79] Ibid.

Page 2753 of 3957

When information is incompatible with our beliefs, we react in one of four ways: (1) adding new, consonant cognitions, (2) removing the inconsistent information, (3) reducing the importance of opposing information, or (4) increasing the importance of compatible cognitions.[80] Festinger's classic example was of smokers encountering information indicating that smoking was bad for their health. In this case, the smoker has four options:

1. Change behavior or adopt new attitude (e.g., stop smoking) (adding new, consonant cognitions).
2. Continue to believe that smoking is not bad for health (remove the incompatible information).
3. Compare risk from smoking to risk from something worse, such as auto accidents (reducing the importance of opposing information).
4. Think about the enjoyment of smoking and its good effects (increase the importance of compatible information and that it might assist with weight control).

If someone saw the Columbian Chemicals story and believed it to be true, cognitive dissonance would be created when the reader was confronted with information that it was untrue. For example, if the person saw the fake CNN story about the explosion first, but then saw a news story showing "live footage" of the plant where all was seemingly normal, cognitive dissonance would occur in the person's mind. When confronted with that contradictory information (i.e., the story initially believed to be turned out to be false), people could (1) change their belief and agree they were misled, (2) refuse to believe the corrected information, (3) question or discredit the source trying to convince them it was a hoax (e.g., believing the correction is a "government cover-up," or (4) remind themselves of the importance of protecting ourselves against terrorist attacks and "err on the side of caution."

Cognitive dissonance affects behavior in several ways. Harmon-Jones (editor of *Cognitive Dissonance: Reexamining a Pivotal Theory in Psychology*) summarizes several paradigms of dissonance theory that have demonstrated aspects of human behavior that can be manipulated.[81] These paradigms are first summarized in Table 4 and then described.

[80] Leon Festinger, *A Theory of Cognitive Dissonance*, (Evanston, IL: Row, Peterson, 1957).

[81] Eddie Harmon-Jones, ed., *Cognitive Dissonance: Reexamining a Pivotal Theory in Psychology*, (Washington, DC: American Psychological Association, 2019), doi: https://doi.org/10.1037/0000135-000.

Page 2754 of 3957

Table 4. Cognitive dissonance paradigms

Paradigm	Description
Norms consistency	People are more likely to believe information that is congruent with their previous norms, beliefs, and actions
Induced compliance	People will be more likely to change their beliefs if they act in a way consistent with the new belief for little or no direct benefit to them
Belief disconfirmation	People will more likely maintain their belief in disconfirmed information if they believe that a group they identify with still believes it, and they are provided arguments why it is still true
Effort justification	People are more likely to maintain their beliefs if they had to expend significant effort to commit to the belief in the first place; effort also includes incurring costs for committing to a belief
Free choice	People are more likely to maintain their beliefs if they made a willing choice to believe something in the first place; this is especially true if the choice was hard

Source: CNA.

The norms-consistency paradigm. People are more likely to accept and defend information that is consistent with their previous norms and actions. For example, people whose actions are consistent with norms are harsher toward those who fail to conform to them. When sixth graders were given an opportunity to cheat, those who cheated revised their attitudes to believe that cheating was not so bad, whereas those who refused to cheat moved their attitudes to be harsher toward those who cheated. Real-world examples would be with how people dress. Those who follow a traditional dress code can harshly judge men who let their hair grow long, or women who dress in revealing outfits. The men and women who violate these norms believe that dress standards are not important. Adults who pay their taxes can be annoyed at those who do not. Those who do not pay taxes feel justified (e.g., "My loopholes are legal," or "I am genuinely poor").

The induced-compliance paradigm. When people are paid to say something that they do not believe, their belief will change to reflect what they have outwardly said. This is particularly true when the reward offered is small (say $2) and less so if the reward is large (say $20). That is because people can justify saying something against their beliefs for a large amount of money (they can tell themselves: I did not mean it; I did it for the money). However, to justify lying for a small amount of money, they revise their opinion to be more congruent with what they said.

The belief-disconfirmation paradigm. When a group commits to a belief that can be clearly shown to be false, the social circumstances of learning the truth makes a large difference in people's opinions. In other words, for a group that believes the world will end on a specific date (a prediction that can be clearly and easily proved false when it didn't happen), it matters how

Page 2755 of 3957

they learn this information. Festinger provides the example of a group that believed that a flood would engulf the continent but that they (the believing group) had been chosen to be saved. When the anticipated flood did not materialize, the believers who were not with the group at the time changed their beliefs about whether or not the flood would ever occur. However, the believers who were physically with the group—those who were assembled together as the countdown occurred—decided that the flood had simply been temporarily postponed. Thus, the believers who were isolated from the group ultimately rejected the disinformation, and those who were colocated created an alternative form of the original disinformation.

The effort-justification paradigm. When people have had to undergo an unpleasant experience or have exerted a lot of effort to join a group, their commitment to that group will be higher than for groups that do not demand an unpleasant initiation or effort to join. An example is initiation processes at fraternities and sororities. Local chapters with difficult initiations elicit more commitment than do those with easier inductions. This principle is also evident in the observation that converts are often more committed to their religion than natives (i.e., someone who converts to Presbyterianism is likely to be more committed to the faith than someone who was born and raised as a Presbyterian).

The free-choice paradigm. Once someone has made a choice, dissonance is likely to be activated. There will be more dissonance if the choice is difficult, and less dissonance if the choice is easy (e.g., if the superiority of the thing chosen is more obvious). For example, someone choosing between chocolate and strawberry ice cream will experience more dissonance (because the choice is difficult) than someone choosing between chocolate and broccoli ice cream (where the superiority of the chocolate is more obvious). To reduce their experience of dissonance, people will tend to increase their opinion of the alternative they chose, and decrease their opinion of the choice they did not make. In our ice cream example, this means that once I choose chocolate ice cream over strawberry ice cream, my opinion of chocolate will increase and my opinion of strawberry will decrease.

Aronson explains these phenomena in terms of dissonance with a person's self-concept.[82] This is known as the *self-consistency* explanation, and it posits that these phenomena occur when we need to reduce the dissonance between something we've done or said or thought, and the kind of person that we think we are. For example, our brains will work to reduce our discomfort if our decision to cheat or say bad things about someone is dissonant with our self-concept as a good person.

[82] Elliot Aronson, "Dissonance Theory: Progress and Problems," in *Theories of Cognitive Consistency: A Sourcebook*, ed. Robert P. Abelson, et al. (Chicago: Rand-McNally, 1968); Elliot Aronson, "The Return of the Repressed: Cognitive Dissonance Theory Makes a Comeback," *Psychological Inquiry* 3, no. 4 (1992), doi: 10.1207/s15327965pli0304_1.

Page 2756 of 3957

Harmon-Jones puts it this way: [83]

> Once an individual commits to a given action, any information inconsistent with that commitment is likely to arouse dissonance and prevent the action from occurring. To maintain the commitment in the face of this inconsistent information, the individual selectively enhances the value of the chosen course of action and reduces the value of the unchosen course of action. Doing so makes effective execution of the chosen action more likely. (p. 17)

Implications of cognitive dissonance for disinformation

Dissonance theory has implications concerning whether someone will believe disinformation. First, in the free-choice paradigm, people will emphasize the good aspects of a choice that they freely chose. For example, if Russian disinformation persuades someone to freely join a faked rally (e.g., with paid actors), the person has to justify why they made that choice and went to the rally. People are likely to convince themselves that they attended the rally because it was for a good cause.

This has another implication. If disinformation can limit or shape the reader's response options to a preferred subset of options, then any response will solidify the reader's commitment to that information. Imagine, for example, that someone asks what you might do if you found a wallet on the ground. This could be presented as an open-ended question, but the options could also be shaped and limited by offering a binary choice: take the money for yourself or leave the wallet and walk away. In this case, you aren't presented with an option to return the wallet to the owner, but you are forced to make a choice, thus increasing your commitment to a choice that you may never have chosen on your own.

Disinformation can limit or shape choices by only providing one set of facts, all consistent with the goals of the person pushing the disinformation. For example, disinformation might say that fluoridation causes blindness because (1) my uncle Dave moved to an area with fluoridation and he went blind right after, (2) a survey of people showed that most people believe it does, or (3) the "Honesty in Dentistry Foundation" emphatically states that fluoridation is linked to blindness. [84]

Second, in the belief-disconfirmation paradigm, people will become more resistant to unequivocal disconfirmation if they have others who will confirm the original erroneous belief. Let's say that someone believes that fluoridation causes blindness and sees news of a comprehensive study refuting that belief. They forward the news to a like-minded friend who

[83] Harmon-Jones, *Cognitive Dissonance: Reexamining a Pivotal Theory in Psychology*.

[84] In reality, this was an unscientific survey of the "Honesty in Dentistry Foundation" funded by an anti-fluoridation group.

Page 2757 of 3957

says, "That flies in the face of everything we know. The study was probably biased for the big toothpaste companies." That reassurance will be enough to discount the comprehensive study. In another example, if you belong to an online community that believes in UFOs, and you are presented with "proof" that a recent sighting did not occur, you are more likely to reject this proof if your online UFO friends also reject it. This is a reason why the comments sections of articles often contain messages from people who immediately contradict authoritative voices. Having one or more people echoing their disbelief in contrary information is often enough to maintain commitment to a belief that is disconfirmed by facts.

In the effort-justification paradigm, people are more committed to something if they have to work for it. We already discussed that in terms of hazing and initiation *processes* at sororities and fraternities. This also applies to the *content* of information. Providing disinformation that portrays the recipient as hard-working and moral, while others outside the group are lazy and dishonest, finds a willing audience (people like to feel virtuous) and might also make them recall that they had to work hard to be part of the special group of people receiving the disinformation.

In the induced-compliance paradigm, people are more committed to an idea if they perform an act for little or no compensation than for a large compensation. If a person can be nudged to spread disinformation for little or no financial gain, they will be more committed to the ideas they are disseminating than if they are paid significant amounts of money to do so.

In the final paradigm—norms consistency—people who comply with norms are less tolerant and harsher in their judgment of others who break norms. Those who break norms are more tolerant of others who also break them. Those who see and reject disinformation will judge "disinformation spreaders" harshly. Conversely, those who have spread or supported disinformation will reduce any previous commitments they might have made to fight disinformation in general.

What can we do about it?

When countering disinformation absorption through dissonance, preventive inoculation is a promising technique. An offshoot of dissonance theory, developed by McGuire, preventive inoculation applies the analogy of vaccination as a method of preventing people from being persuaded by propaganda.[85] As explained in the cognition section, inoculation theory states that forewarning people about propaganda will reduce its influence, just as vaccines prevent or lessen the effects of disease. In the case of dissonance, inoculation can remind individuals

[85] William McGuire, "Resistance to Persuasion Conferred by Active and Passive Prior Refutation of Same and Alternative Counterarguments," *Journal of Abnormal Psychology* 63, no. 2 (1961).

Page 2758 of 3957

about aspects of their self-concept and help them rehearse counterarguments to combat disinformation and remove the dissonance in a way that does not introduce disinformation.

However, when attempting to protect against disinformation or refute disinformation, it is important to try not to *create* cognitive dissonance for the receiver. To avoid creating dissonance when using inoculation, messages should be crafted in a way to appeal to previous beliefs:

1. Craft messages that are consistent with the receiver's self-concept.
2. Craft messages that are congruent with previous beliefs.
3. Frame responses in a way that is congruent with your goals and reminds recipients of their group identification.[86]

As a theory of the emotion and cognitive aspects of social influence, dissonance theory posits ways that inoculation can be strengthened. The four key components of using dissonance to strengthen inoculation against disinformation are as follows:

1. *Threat.* By framing the incoming disinformation as a threat, the individual will be emotionally primed to identify the argument as propaganda, fight it, and solidify their previous beliefs. If people are not forewarned and given tools to combat the disinformation, they will be less likely to fight the message or think of counterarguments. Some research suggests that the forewarning of an attack is enough to induce resistance to a message, even without the other key element of refutational preemption (discussed below).[87] This first element is the motivational/emotional part of the effect.
2. *Refutational preemption*. This part allows the receiver to practice making arguments against the propaganda. By providing the receiver with arguments against the propaganda, the person's initial beliefs become stronger and prime them to think of additional reasons why their initial beliefs are correct. Sometimes people accept disinformation simply because they cannot bring to mind reasons for their prior beliefs.
3. *Involvement*. In order for inoculation to have an impact, it helps that the topic be one that the receiver finds important and salient.[88] A key part of this is pointing to the

[86] In the case of disinformation, the group should be defined as an in-group of people who are about to lose something very important. In combating disinformation, this would mean reminding people of the larger groups they are part of, including people with whom they might disagree. We will discuss this more fully in the next section, Group, Belief, Novelty Model (GBN).

[87] Josh Compton and Bobi Ivanov, "Untangling Threat During Inoculation-Conferred Resistance to Influence," *Communication Reports* 25 (2012), doi: 10.1080/08934215.2012.661018.

[88] Michael Pfau et al., "Enriching the Inoculation Construct: The Role of Critical Components in the Process of Resistance," *Human Communication Research* 24, no. 2 (1997), doi: 10.1111/j.1468-2958.1997.tb00413.x.

Page 2759 of 3957

receiver's interest (for example, "the real reason they are going to say this is to take away your right to unfluoridated waters"). Unless someone has a stake in the subject of the disinformation, he or she is less likely to fight it. As explained earlier, another way to obtain involvement is to get people to act on those initial beliefs.

4. *Delay/dosage*. McGuire's original theory posited that, just as it takes time for the body to develop defenses against bacteria, it will take time for inoculation arguments to take hold in the receiver. This portion of the theory is controversial since evidence concerning the need for time has been mixed. However, the evidence does point to the fact that successful inoculation can have long-lasting effects. We think that delay might not be as important as repetition (or dosage) of the inoculation. In our view, the issue is not time, but amount of inoculation. Many inoculations require multiple doses. For example, with rabies vaccine, people should get their first dose as soon as possible (if not received early, the disease is almost always fatal), and on days 3, 7, and 14.[89]

Dissonance has pointed to ways that the inoculation effect can be made stronger. One of those ways is to make the propaganda seem like an immediate attack on one's vested interests. For example, "They will take away your house tomorrow if you do not respond immediately." Additional ideas are to encourage anger at the attack source. For example, "The message will lie to you and assume you are stupid." Third, inoculation will be stronger if it encourages the idea that the propaganda/disinformation is a threat to your core beliefs. For example, "If they have their way, they will spit on the ideals of our religion and democracy." As noted earlier, dissonance theory predicts that inoculation will be stronger if it appeals to our self-concepts as smart, tough, and moral. For example, "Resisting this disinformation means you are clever, stalwart, and principled."

When preventive inoculation is not possible, "therapeutic inoculation" might be valuable. The analogy here is to the rabies vaccine, which is given to people after they have been bitten by a potentially rabid animal. In the case of the rabies vaccine, a dose is given as close as possible to the attack and additional doses are given in succession. Compton and Pfau report that so far, examples of successful therapeutic inoculation are sparse[90] and, in our opinion, conflicting. Table 5 shows how these principles can be used for crafting messages.

Table 5. Key components of using dissonance for inoculation

	Intervention
Threat	Framing anticipated disinformation as a threat motivates the receiver to gather ways to reject it.

[89] Nossal, "Vaccination."

[90] Josh Compton, "Prophylactic Versus Therapeutic Inoculation Treatments for Resistance to Influence," *Communication Theory* 30, no. 3 (2020), doi: https://doi.org/10.1093/ct/qtz004.

Page 2760 of 3957

	Intervention
Refutational preemption	Providing counterarguments, even weak ones, will help the receiver recognize how to react how to reject the disinformation.
Involvement	Casting disinformation as an *immediate* threat activates mechanisms to speed reactions and bypass slower thinking processes, rejecting it more quickly
Delay and dosage	Getting the counterargument to the receiver quickly and repeatedly allows time for counterarguments to become familiar and rote before disinformation is believed.

Source: CNA.

The Group, Belief, Novelty (GBN) model

Not all information is equally valuable to an individual. Some information (or disinformation) resonates with some people more than others. The Group, Belief, Novelty (GBN) model helps explain the likelihood that someone will pass information (rumors specifically) on to others.[91] The theory posits that we accept and share information more readily when it comes from people we know, it appeals to what "our group" believes, and when we think it is new.

Because the theory is built primarily related to rumors (a subset of information), we briefly describe rumors and how they apply to this study on disinformation. Rumors are "unverified and instrumentally relevant information statements in circulation that arise in context of ambiguity, danger, or potential threat and that function to help people make sense of and manage risk."[92] While this can include conspiracy theories, they are outside the scope of this paper. For our purposes, all conspiracy theories are rumors but not all rumors are conspiracy theories. In this section, we focus solely on rumors that are not conspiracy theories. Researchers who developed the model cite empirical evidence that rumors are important to study because they alter purchase behaviors,[93] "spark" riots in conflict situations,[94] and

[91] Bernard P. Brooks, Nicholas DiFonzo, and David S. Ross, "The GBN-Dialogue Model of Outgroup-Negative Rumor Transmission: Group Membership, Belief, and Novelty," *Nonlinear Dynamics, Psychology, and Life Sciences* 17, no. 2 (2013).

[92] Nicholas DiFonzo and Prashant Bordia, *Rumor Psychology: Social and Organizational Approaches*, (Washington D.C.: American Psychological Association, 2007). doi: https://doi.org/10.1037/11503-000.

[93] Nicholas DiFonzo and Prashant Bordia, "How Top Professionals Handle Hearsay: Corporate Rumors, Their Effects, and Strategies to Manage Them," *Public Relations Review* 26 (2000); Alix Freedman, "Rumor Turns Fantasy Into Bad Dream," *The Wall Street Journal*, May 10, 1991, 1991.

[94] Donald L. Horowitz, *The Deadly Ethnic Riot*, (Berkeley, CA: Univeristy of California Press, 2001).

influence stock market buying and selling.[95] In addition, they reference research findings that rumors affect attitudes.[96]

The GBN model is a "two step agent-based mathematical model of negative rumor spread in the context of conflicting groups"[97] that uses concepts and findings from psychology and sociology research as the basis for its equations. According to the first step, the probability of rumor transmission between two people is based on the following three factors:

1. Group memberships (G) of the receiver and transmitter
2. Strength of their belief (B) in the rumor
3. The perceived novelty (N) of the rumor

The second step models how belief (B) levels and the perceived rumor novelty (N) of participants change over time, using findings from the literature on attitude change.

The first factor (G) encompasses several findings regarding how group membership affects the sharing of rumors. In the case of negative (derogatory) rumors, people share them with their in-group (people with whom they identify with, whether age, race, and gender, occupation, or political leaning). They rarely share rumors with the out-group (people with whom they feel little affiliation). It is not surprising that the rumor target (whether it attacks individuals in the in-group or the out-group) and valence (whether it praises or derogates) affect whether a rumor is shared and spreads.

Rumors that derogate the out-group are called "wedge-driving" rumors because they attempt to drive a wedge between groups. They can also be used for self-enhancing motives (boosting one's self-esteem and those of the in-group)[98] or the desire to increase liking between the spreader and the hearer. Conversely, people rarely share derogatory rumors about the out-group with people from that out-group.

The second factor, belief, is the person's degree of confidence that the information is true. In general, people are much more likely to share information they believe to be true. However, the threshold of degree of belief needed to share information is lower when the stakes are

[95] Nicholas DiFonzo and Prashant Bordia, "Rumor and Prediction: Making Sense (But Losing Dollars) in the Stock Market," *Organizational Behavior and Human Decision Processes* 71 (1997).

[96] DiFonzo and Bordia, *Rumor Psychology: Social and Organizational Approaches*.

[97] Brooks, DiFonzo, and Ross, "The GBN-Dialogue Model of Outgroup-Negative Rumor Transmission: Group Membership, Belief, and Novelty."

[98] Prashant Bordia and Nicholas DiFonzo, "Psychological Motivations in Rumor Spread," in *Rumor Mills: The Social Impact of Rumor and Legend*, ed. Gary Allen Fine, Veronique Campion-Vincent, and Chip Heath (NY: Aldine Press, 2005).

Page 2762 of 3957

higher and it involves planning future actions.[99] For example, college professors involved in tense labor negotiations shared information they believed to be true, but, because of the high stakes involved, they did not require a high degree of confidence in its veracity before sharing it. College students, in a very different context, were reluctant to share information about a recent campus attack that had occurred, for fear of upsetting others with false information.

The third factor, novelty, refers to whether the rumor is novel to the hearer, and whether the hearer thinks it might be new to others. The hearer may spread the rumor as a way to make sense of an uncertain and ambiguous situation. However, once the rumor becomes "old news," people avoid sharing it because it has become stale. This accounts (in part) for why fact-checking and corrections are less shared than the original rumor—and why therapeutic inoculation is more difficult than is preventive inoculation (which we discussed earlier).

Buchanan explored multiple factors to determine which had the greatest effect on self-reported sharing of disinformation online.[100] He considered attributes of the message, including how authoritative the source was and how much consensus information was available (e.g., amount of "likes" on the platform). He also considered viewer characteristics, such as digital literacy, personality, and demographic variables. Across four studies, people who reported the greatest likelihood of sharing disinformation are those who thought the material was true or those who had preexisting attitudes consistent with the information.

Example of the GBN model using authoritarian attitudes

In this section, we use the construct of authoritarian attitudes to describe how the GBN model can illustrate disinformation sharing. People with authoritarian attitudes have been shown to have three predominant beliefs:[101]

- Conventional thinking
- Submission to authority
- A belief in aggression toward out-groups

They also tend to be considerably less open to experience and somewhat more conscientious than other people, whereas those on the other end of the scale ("anti-authoritarians") are more

[99] Ralph L. Rosnow, James L. Esposito, and Leo Gibney, "Factors Influencing Rumor Spreading: Replication and Extension," *Language and Communication* 8, no. 29-42 (1988); ibid.

[100] Tom Buchanan, "Why Do People Share False Information Online? The Effects of Message and Viewer Characteristics on Self-Reported Likelihood of Sharing Social Media Disinformation," *PLoS ONE* 15, no. 10 (2020), doi: 10.5255/UKDA-SN-854297.

[101] Bob Altmeyer, "The Other Authoritarian Personality," *Advances in Experimental Social Psychology* 30 (1998), doi: https://doi.org/10.1016/S0065-2601(08)60382-2.

Page 2763 of 3957

open to experience and slightly less conscientious. More recent literature suggests that those with authoritarian attitudes might also be more disagreeable, dogmatic, and lacking in intellectual humility.[102] However, this work is preliminary.

Note that authoritarian beliefs are, to a degree, situation dependent. Research has shown that people could relax these attitudes when they did not feel threatened, or when new experiences led them to question some of their previous beliefs. [103] Therefore, those with authoritarian attitudes are very likely to share disinformation framed as a threat to conventional beliefs (in the GBN model, it lowers the threshold of belief in the information's veracity before sharing it). Again, using the GBN model, they will share that disinformation with others with whom they identify. Maintaining a sense of being under threat is important for maintaining the cohesion of authoritarian groups.

In the Columbian Chemicals example described earlier, when the photo of the explosion was paired with the idea that Islamist terrorists had caused it, the explosion became threatening to those who are especially threatened by Islamist radicalism and believe that Islamist terrorist attacks in the US are rampant. This made the news appeal to previous beliefs (Beliefs). Sharing the novel photo was not only a civic duty (dissonance theory's explanation) but a way to boost one's self esteem and maintain the group's feelings of threat (Group). The time value of sharing the photo is also important: Sharing the photo immediately (Novelty) gets noticed. Trying to verify the validity of the photo slows you down and makes it less likely that you will be the first with the information.

Implications of the GBN Model for disinformation

The GBN model posits that group identity, degree of belief in the information, and information's novelty are powerful factors in whether information gets shared, with whom we share it, and when we share it. Once disinformation gets shared, it can be amplified and further distorted by those who find the information compelling (as in the old "telephone game" people sometimes play at group gatherings, the original story almost invariably gets distorted in the retelling). These factors coincide with characteristics of the current information environment, where people can stay connected with their smart phones 24/7, allowing people to feel that (1) they are never alone, (2) their voice will always be heard, and (3) they can put their attention

[102] Thomas H. Castello et al., "Clarifying the Structure and Nature of Left-Wing Authoritarianism," *Journal of Personality and Social Psychology* (2021 pre-print), doi: doi 10.31234/osf.io/3nprq.

[103] Martin Roiser and Carla Willig, "The Strange Death of the Authoritarian Personality: 50 Years of Psychological and Political Debate," *History of the Human Sciences* 15, no. 4 (2002), doi: 10.1177/952695102015004682.

Page 2764 of 3957

anywhere they want to put it.[104] In a sense, we live in a 24/7 virtual telephone game. Although these characteristics of the information environment can speed up rumor spread, the GBN model provides areas where the telephone game can be interrupted, slowed, or corrected.

What can we do about it?

In this section, we discuss how interventions can address all three aspects of the GBN model. Table 6 summarizes the insights, which are described in the subsequent paragraphs.

The first link in the rumor/disinformation chain is the identification with people who are similar to us, whether in terms of opinions, race, religion, gender, or age. The first implication of GBN is to start with people's narrow group identification.

Table 6. Using components of the GBN model to counter disinformation

	Intervention
Group	Expand the "group" with which an individual identifies by highlighting aspects of shared destiny and shared values
Belief	Increase a person's access to opposing opinions/information
Novelty	Create new content to expand the group and open up beliefs

Source: CNA.

Shared destiny

One of the ways that the effects of disinformation can be reduced is through direct contact with the out-group in a situation with a shared destiny.[105] For example, a set of experiments showed that children in integrated classrooms became more accepting of minorities when they were placed into "jigsaw" groups where each child had to teach the others a piece of information that only they knew. This arrangement made it in the best interest of everyone in the group to listen to one another and root for each other's success with learning their part of the materials. We see this effect in the military, where everyone in the unit depends on particular individuals to do their job well; in fact, they entrust their lives to individuals of different races.

[104] Lauren C. Davis, "The Flight from Conversation," *The Atlantic*, Oct. 7, 2015, http://www.theatlantic.com; Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet*, (New York: Touchstone, 1997); Sherry Turkle, *Alone Together: Why We Expect More from Technology and Less from Each Other*, (New York: Basic Books, 2011); Sherry Turkle, *Reclaiming Conversation: The Power of Talk in the Digital Age*, (New York: Penguin Books, 2015); Sherry Turkle, *The Empathy Diaries: A Memoir*, (New York: Penguin Publishing, 2021).

[105] Elliot Aronson and Diane Bridgeman, "Jigsaw Groups and the Desegregated Classroom: In Pursuit of Common Goals," *Personality and Social Psychology Bulletin* 5, no. 4 (1979), doi: https://doi.org/10.1177/014616727900500405.

Page 2765 of 3957

To emphasize shared destiny in the internet age, it would be useful for login screens to feature information about the shared contributions different groups make to a common goal. Military commands depend on each other for resources, information, skillsets, and use of tools. Although login information can become part of the "background noise" quickly, a rotating set of reminders of interdependence and photos of individuals across the globe with whom one works for could reduce the likelihood of forming "gangs" of like-minded individuals unnecessarily sharing information only with an in-group. Knowing that information will be seen by others can have a moderating effect on what one says and what one shares.

It is important to frame arguments to be sure that people feel that they are not isolated in their original beliefs.[106] That is why advertisements often stress that many other people like their product (e.g., "99% of customers who tried our product liked it"). In the case of disinformation, "Everybody knows that this information is true."

Shared values

Disinformation can be combated by pointing to areas where the out-group and in-group share common values.[107] For example, common values could include admiration of past leaders, respect for the rule of law, fairness, and justice.[108]

Easier access to opposing opinions

The second area of GBN is the degree of belief. The GBN model posits that, when information is shared with another individual, that person's feedback will modify one's belief in the information. A good option to combat the tendency to share information only with like-minded individuals is to provide easier access to opposing opinions.

Two earlier methods of making it easier to access opposing opinions appeared soon after World War II. The fairness doctrine required holders of broadcast licenses to (1) present discussion of controversial issues of public importance and (2) do so in a way that is honest, equitable, and balanced. In the digital world, this might require access to opposing opinions and information on controversial issues in discussion format or question-and-answer format.

A second method was the equal-time rule. This required candidates of both parties to have access to a certain amount of broadcast time at the same rate as the opposing candidate. In this

[106] Wei-Kuo Lin and Michael Pfau, "Can Inoculation Work Against the Spiral of Silence? A Study of Public Opinion on the Future of Taiwan," *International Journal of Public Opinion Research* 19, no. 2 (2007), doi: 10.1093/ijpor/edl030.

[107] Kate Woodsome, Danielle Kunitz, and Joy Sharon Yi, "Our Political Divide Is Dangerous. A Neuroscientist and Political Scientist Explain Why," *Washington Post*, Dec. 24, 2020.

[108] These last suggestions of respect for the rule of law, fairness, and justice might not be accepted by those who are truly authoritarian.

Page 2766 of 3957

way, broadcasts could not favor a preferred political candidate by denying the opposing candidate a forum to respond. If candidate A bought 30 seconds of TV time for ads, the opposing candidate would buy 30 seconds at the same rate. For the digital world, this might require allowing like-minded social media groups to allow people with different viewpoints some sort of access to the group.

Maintaining novelty of shared destiny and values

The third area of GBN is novelty. One of the common complaints about government information campaigns of the past (e.g., vaccination information, seat belt information) was that it was repetitive and predictable. If disinformation is to be counteracted, true information needs to be presented in different ways (Google updates its screen with a new factoid daily), and preferably by a diverse group of people, with humor and other ways to lighten the message. We see this in advertising campaigns all the time—GEICO constantly updates its ads, and some brands adopt a new slogan on a regular basis. The point is that old information gets more attention when it is repackaged as new.

Emotions and arousal

A person's state of emotion and arousal can also make them more susceptible to disinformation. It is no secret that some information and messages affect people more than others. In fact, marketing campaigns rely on the effect a message has on a person's emotions and subsequent behavior to buy products, donate to a cause, or vote for a candidate. Countless books, courses, and practices have been built on the concept of using messages to influence people's perceptions and behaviors, including the ubiquitous *How to Win Friends and Influence People* by Dale Carnegie and the extensively researched *Influence: Science and Practice* by Robert Cialdini.[109] While there are multiple compelling aspects of a message that can affect the message's ability to persuade, people are more likely to respond to (and share) information that is interesting, elicits positive emotions, or arouses action.[110]

Novelty, discussed at length in the GBN model section, is a primary determinant of what people consider interesting.[111] In addition, content can inspire emotional feelings (positive or

[109] Dale Carnegie, *How to Win Friends and Influence People*, (New York: Simon & Schuster, 1936); Robert B. Cialdini, *Influence: Science and Practice*, 4th ed. (Boston: Allyn and Bacon, 2001).

[110] Katherine L. Milkman and Jonah Berger, "The Science of Sharing and the Sharing of Science," *Proceedings of the National Academies of Science* 111 no. Supplement 4 (2013), doi: 10.1073/pnas.1317511111; William J. Brady, Ana P. Gantman, and Jay J. Van Bavel, "Attentional Capture Helps Explain Why Moral and Emotional Content Go Viral," *Journal of Experimental Psychology: General* 149, no. 4 (2020).

[111] Brooks, DiFonzo, and Ross, "The GBN-Dialogue Model of Outgroup-Negative Rumor Transmission: Group Membership, Belief, and Novelty."; ibid.

negative) and can motivate or depress a response (high or low arousal). The following table provides examples that are commonly explored in the literature.

Table 7. Examples of positive and negative emotions that differ on level of arousal

	High arousal	Low arousal
Positive emotion	Awe or amusement	Contentment
Negative emotion	Anxiety or fear	Sadness

Source: CNA.

Emotion and arousal theories would explain that the sharing of the false Columbian Chemicals story was enhanced because the story elicited highly arousing negative emotions of anxiety and fear. Indeed, the cover graphic explicitly included the word "panic" on the page, further priming the arousing emotion.

Multiple researchers have explored characteristics that make information more likely to be shared. Commonly studied characteristics are message placement (i.e., prominence on a page), length, interest, usefulness of the information, emotions evoked from the story, and arousal evoked from the story. Research demonstrates that positive-emotional content is more viral than negative-emotional content, but there is evidence that high-arousal content (regardless of whether it is positive or negative) is more likely shared than low-arousal content.[112] Put simply, the level of arousal the content evokes—or the level of arousal a person feels when he or she sees the content—is even more important than positive or negative content when evaluating the likelihood of sharing information. That means that things that inspire awe, anger, and anxiety are more likely shared than things that inspire sadness. It is important to note that this relationship remains true even when a variety of other factors are held constant, including how interesting the material was, how practical (informative) it was, how prominently it was displayed, how long it was available, how long it was, the influence of the author, and the gender of the author. This research suggests that, when considering how information spreads, focusing on the content of a contagious message is valuable: how does it make people feel? Is that emotion arousing or depressing?

The psychological principles illuminated in this section thus far have described what is happening, but they have not offered explanations as to *why* the relationships exist. Our preliminary research has uncovered two possibilities: (a) an illustration of the Yerkes-Dodson

[112] Jonah Berger and Katherine L. Milkman, "What Makes Online Content Viral?," *Journal of Marketing Research* 49, no. 2 (2012), doi: https://doi.org/10.1509/jmr.10.0353. Jonah Berger, "Arousal Increases Social Transmission of Information," *Psychological Science* 22, no. 7 (2011), doi: https://doi.org/10.1177/0956797611413294.

Page 2768 of 3957

Law that arousal is required to motivate behavior and (b) social psychological theories exploring the individual benefits of sharing information with a larger group.

The Yerkes-Dodson Law is the idea that there is a normal distribution (bell-curve) relationship between performance and arousal.[113] At very low levels of arousal, individuals will not engage in tasks. At very high levels of arousal, individuals are so stimulated that they also cannot engage in tasks. There is an optimal level of arousal, near the midpoint, at which an individual will maximally perform. The research described regarding emotional arousal and sharing of information supports portions of the Yerkes-Dodson law.[114] Low-emotional arousal is not as associated with information sharing as higher levels are. However, we are unaware of researchers specifically testing for the bell-curve relationship regarding information sharing (i.e., are there levels of emotional arousal where individuals will no longer be inclined to share information?).

There are multiple social benefits served by sharing information among group members. Sharing emotional information with others can increase social bonding or increase the perception of similarity among group members, both of which can strengthen a community.[115] However, these social benefits also motivate other behaviors to protect the group and group identity. Brady, Crockett, and Van Bavel note that, when group identities are threatened from individuals inside or outside the group (through challenging information), those who more strongly associate with the group are more likely to express or share emotional information.

Implications of emotionally arousing content for disinformation

The relevance of emotions and arousal to the likelihood of information sharing is an important key for understanding the spread of disinformation. Research suggests that a reader is more likely to share false information if it arouses him or her. A recent study exploring 126,000 tweets found that the false content shared was more novel and inspired fear, disgust, or surprise while the true information shared inspired anticipation, sadness, joy, and trust.[116] In this study, false content inspired emotions that were more arousing than emotions inspired by

[113] Robert M. Yerkes and John D. Dodson, "The Relation of Strength of Stimulus to Rapidity of Habit-Formation," *Journal of Comparative Neurology and Psychology* 18 (1908).

[114] Bruce E. Kaufman, "Emotional Arousal as a Source of Bounded Rationality," *Journal of Economic Behavior and Organization* 38, no. 135-144 (1999), doi: 10.1016/S0167-2681(99)00002-5.

[115] William J. Brady, M. J. Crockett, and Jay J. Van Bavel, "The MAD Model of Moral Contagion: The Role of Motivation, Attention, and Design in the Spread of Moralized Content Online," *Perspectives on Psychological Science* 15, no. 4 (2020), doi: 10.1177/1745691620917336.

[116] Vosoughi, Roy, and Aral, "The Spread of True and False News Online."

Page 2769 of 3957

true content. In addition, they found that bots were as likely to share true information as false information and that those who shared false information were less likely to be influencers (e.g., fewer followers, less active on social media, less time on Twitter, and less likely to be verified) than those who shared true information. Of interest, this article explored the extent to which false and true information spread and found that an individual instance of true content rarely reached more than 1,000 people, whereas the false content routinely reached 1,000 to 100,000 people. The authors conclude that "the greater likelihood of people retweeting falsity more than truth is what drives the spread of false news, despite network and individual factors that favor the truth."[117]

It is possible that multiple psychological principles, activated at the same time, can increase the likelihood that disinformation is absorbed or shared. Kaufman builds on the Yerkes-Dodson Law to describe how higher levels of emotional arousal can interfere with cognitive processes (e.g., short-term memory, organizing thoughts, and rational thinking).[118] This suggests that if something is highly arousing, it might increase the likelihood that a person would process the information using automatic thinking.

What can we do about it?

Our literature review did not produce many insights into combating the effects of emotion and arousal on disinformation. Indeed, the articles that discuss the topic primarily describe the phenomenon in field and laboratory settings, but do not explore ways to counter the effect. However, the literature strongly indicates that emotional and arousing content are more likely to be shared, and Russia has tended to favor disinformation stories on topics known to be highly emotional and arousing to US citizens, such as race relations.

Given that disinformation is, by definition, constructed, it can be constructed to contain emotional or arousing messages. Several of the ideas to combat the absorption and spread of disinformation have been discussed in the previous sections. Inoculation, discussed to combat multiple psychological principles that can facilitate disinformation, could be applied to combating emotional and arousing messages. Making people aware of the effect of emotional/arousing information on beliefs and behaviors can give them tools to respond more accurately. Increasing controlled processing through friction or nudging could also help combat emotional and arousing disinformation. Providing cues to think more deeply about information on suspect websites might prime individuals to be more skeptical of emotional/arousing information they receive.

[117] Vosoughi, Roy, and Aral, "The Spread of True and False News Online."

[118] Kaufman, "Emotional Arousal as a Source of Bounded Rationality."

Page 2770 of 3957

Summary

Understanding how false information spreads is the first step toward containing it. We described four major psychological principles that research demonstrates are related to the absorption and spread of disinformation.

The first psychological principle relates to how people **initially process information**. Our "processing capacity" is limited, so we cannot deeply attend to all new information. We take mental shortcuts to incorporating new information, and those shortcuts can open us up to mistakes. To the extent that we do not process information as deeply as we should, disinformation can be construed as true information.

The second psychological principle, called **cognitive dissonance**, describes the discomfort we feel when we are confronted with two competing ideas. We are motivated to reduce the dissonance by changing one attitude, removing (ignoring) the contradictory information, discounting the importance of contradictory information, or increasing the importance of compatible information. If disinformation supports our initial beliefs or creates less dissonance than true information, we are more likely to believe the disinformation.

The third psychological principle describes the role **group membership, beliefs, and novelty** play in absorbing and sharing disinformation. We are more likely to share information with people we identify with (i.e., consider members of our group) when we believe the information is true and when it is novel or urgent.

The fourth psychological principle describes the **role of emotion and arousal** in our sharing of disinformation. Research demonstrates that we pay more attention to information that makes us feel positively or that arouses us to act. That means we are more likely to share information if we feel awe, amusement, or anxiety than if we feel sadness or contentment.

Further we also summarized the research on countering the effect of disinformation through the psychological principles described. Several techniques discussed could be used to counter disinformation absorption that results from more than one psychological principle. Specifically, preventive inoculation and encouraging deeper, analytic thinking could shield a person from the effects of disinformation. Researchers recommend that disinformation containment policies should emphasize behavioral interventions that confront psychological mechanisms to dissuade the spread of disinformation rather than solely focusing only on bots and algorithms. [119]

[119] Vosoughi, Roy, and Aral, "The Spread of True and False News Online."

Page 2771 of 3957

Conclusion

Brett Horvath, the president of Guardians.ai, argues that "disinformation is not the weaponization of knowledge"; rather, he says, "it's the weaponization of cognition." He further points out that "a coherent strategy…has to be built on principles: What are you defending, and what are you attacking?"[120] As such, we contend that the threat posed by disinformation cannot be met solely with technological and political solutions; the psychological principles that facilitate its absorption and spread must also be considered.

Human brains allow us to organize information and respond to it efficiently, but cognitive mechanisms are not infallible. As the research we have cited makes clear, disinformation weaponizes normal and necessary cognitive mechanisms by exploiting their vulnerabilities. But despite their susceptibility to disinformation, cognitive mechanisms present a potential path forward. To date, much has been written about how to respond technologically and politically to disinformation, but far less has been written about how we might respond psychologically to such manipulation. Identifying the best paths forward in this space requires first developing an understanding of the psychological mechanisms that make disinformation effective. As noted throughout this report, preventive inoculation and encouraging deeper, analytic thinking are frequently discussed in the literature as ways to protect against disinformation. Additional research is necessary to determine effective ways to integrate these two techniques into individual-level cognition and community-level intervention, especially in online environments. A more targeted approach may be possible if we explore the four psychological mechanisms being exploited to spread disinformation: initial information processing, cognitive dissonance, GBN, and emotional arousal.

Ultimately, solutions that consider technological and political factors alone cannot sufficiently diminish the large-scale absorption and spread of disinformation. Because disinformation primarily affects the mind, a multipronged response that includes evidence-based psychological interventions will be critical to the work of countering this growing threat.

[120] Robert Ackerman, "Cyber-Driven Disinformation Is Here to Stay," Signal, Sept. 5, 2019, https://www.afcea.org/content/cyber-driven-disinformation-here-stay.

Page 2772 of 3957

Glossary

Psychological Terms	Definitions
Alertness	A heightened awareness to the effects of disinformation that can prevent disinformation from being absorbed.
Analytic thinking	Deliberate, controlled, thoughtful evaluation of new information that can prevent disinformation from being absorbed.
Belief-disconfirmation paradigm	After a group commits to a belief that can clearly be proven false, the social circumstances of learning the truth have a large effect on group members' acceptance or denial of that truth.
Cognitive dissonance	Dissonance theory describes how people are influenced to either accept or reject beliefs, and the arguments/information that accompany those beliefs. It posits that people feel uncomfortable when they have to reconcile conflicting information.
Dual process theory	The foundation for understanding the two ways we process information. The first process, called automatic, requires very little effort and is fast, efficient, and "cognitively cheap." The second process, called controlled, is slower, more cognitively involved, and requires deliberate attention.
Effort-justification paradigm	When someone has to undergo an unpleasant experience or exert a lot of effort to join a group, their commitment to that group will be higher than for groups that do not demand an unpleasant initiation or increased effort to join.
Free-choice paradigm	People will emphasize the good aspects of a choice that they freely chose. Once someone has made a choice, dissonance is likely to be activated. There will be more dissonance if the choice is difficult and less dissonance if the choice is easy.
Friction	Friction occurs when something is difficult to process and can be created by asking questions that make others process information more deliberately (e.g., asking, "what makes you say that?"). It is the opposite of fluency and can prevent disinformation from being absorbed.
Group, Belief, Novelty (GBN) Model	The theory posits that we accept and share information more readily when it comes from a group of people we know (G), it appeals to what "our group" believes (B), and when we think it is new (N).

Page 2773 of 3957

Psychological Terms	Definitions
Heuristics	Mental shortcuts we use to make sense of the world. Heuristics are developed through previous experience and connections we make between similar pieces of information.
Illusory truth effect	When familiarity with something gives the illusion that it is more accurate, inadvertently increasing someone's belief in that information.
Induced-compliance paradigm	When someone is paid to say something that they do not believe, their belief will change to reflect what they have outwardly said. This is particularly true when the reward offered is small, and less so if the reward is large.
Initial information processing	Our brains employ mental shortcuts in an effort o process information as efficiently as possible, which can make us vulnerable to mistakes.
Inoculation	To provide awareness of possible disinformation and the effects of disinformation so others can recognize it when confronted by it later. This can prevent disinformation from being absorbed.
Information fluency	A person's ability to process information. This increases when information is clear and easy to understand.
Negative emotion	Emotions that make people feel bad. Examples include anxiety, fear and sadness.
Norms-consistency paradigm	People are more likely to accept and defend information that is consistent with their previous norms and actions.
Nudge	To provide subtle cues for an encouraged behavior. This can prevent disinformation from being absorbed.
Positive emotion	Emotions that make people feel good. Examples include, awe, amusement, and contentment.
Primacy and recency effect	The tendency for people to remember information that is presented first (primacy) or presented most recently (recency).
Skepticism	The awareness of possible hidden agendas and a personal desire to understand the evidence. This can prevent disinformation from being absorbed.
Therapeutic inoculation	Providing awareness of disinformation that a person has already experienced to attempt to remove that disinformation and mitigate its effect on future beliefs and behavior.
Yerkes-Dodson Law	The theory that there is a normal distribution (bell-curve) relationship between performance and arousal. At very low levels of arousal, an individual will not engage in tasks. At very high levels of arousal, the individual is so stimulated that they also cannot engage in tasks.

Page 2774 of 3957

Figures

Figure 1. Twitter post showing the Columbian Chemicals plant explosion 1
Figure 2. Twitter post asking Oregon senator Jeff Merkley about the Columbian Chemicals plant explosion 2
Figure 3. Twitter account posting a fake CNN homepage showing the story of the Columbian Chemicals plant explosion 3
Figure 4. Taxonomy of disinformation, misinformation, and mal-information 9
Figure 5. Russian disinformation regarding US Ambassador Tefft 12
Figure 6. US Embassy response to Russian disinformation regarding US Ambassador Tefft 13

Page 2775 of 3957

Tables

Table 1. Psychological principles relevant for disinformation adoption and spread.....25
Table 2. Dual process theory.....26
Table 3. Disinformation prevention mechanisms for initial information processing.....31
Table 4. Cognitive dissonance paradigms.....36
Table 5. Key components of using dissonance for inoculation.....41
Table 6. Using components of the GBN model to counter disinformation.....46
Table 7. Examples of positive and negative emotions that differ on level of arousal.....49

Page 2776 of 3957

References

Altmeyer, Bob. "The Other Authoritarian Personality." *Advances in Experimental Social Psychology* 30 (1998): 47-91. doi: https://doi.org/10.1016/S0065-2601(08)60382-2.

"The American Ambassador to Russia John F. Tefft Walked at an Opposition Rally in Maryino." Посол США в России Джон Ф. Тефт прогулялся на митинге оппозиции в Марьино. Twitter. Sept. 20, 2015. https://twitter.com/rentvchannel/status/645658877426593792.

Aronson, Elliot. "Dissonance Theory: Progress and Problems." In *Theories of Cognitive Consistency: A Sourcebook*, edited by Robert P. Abelson, Elliot Aronson, William J. McGuire, Theodore M. Newcomb, Milton J. Rosenberg, and Percy H. Tannenbaum. Chicago: Rand-McNally, 1968.

———. "The Return of the Repressed: Cognitive Dissonance Theory Makes a Comeback." *Psychological Inquiry* 3, no. 4 (1992): 303-311. doi: 10.1207/s15327965pli0304_1.

Aronson, Elliot, and Diane Bridgeman. "Jigsaw Groups and the Desegregated Classroom: In Pursuit of Common Goals." *Personality and Social Psychology Bulletin* 5, no. 4 (1979): 438-446. doi: https://doi.org/10.1177/014616727900500405.

Asser, Martin. "What the Muhammad Cartoons Portray." BBC. Jan. 2, 2010. http://news.bbc.co.uk/2/hi/middle_east/4693292.stm.

Bago, Bence, David G. Rand, and Gordon Pennycook. "Fake News, Fast and Slow: Deliberation Reduces Belief in False (But Not True) News Headlines." *Journal of Experimental Psychology: General* 149, no. 8 (Aug. 2020): 1608-1613. doi: 10.1037/xge0000729.

Bail, Christopher, Brian Guay, Emily Maloney, Aidan Combs, D. Sunshine Hillygus, Friedolin Merhout, Deen Freelon, and Alexander Volfovsky. "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017." *PNAS: Proceedings of the National Academy of Sciences of the United States of America* 117, no. 1 (2020): 243-250. Accessed Feb. 3, 2021. https://www.pnas.org/content/117/1/243.

Beckett, Lois. "Misinformation 'Superspreaders:' Covid Vaccine Falsehoods Still Thriving on Facebook and Instagram." *The Guardian*. Jan. 6, 2021. Accessed Feb. 3, 2021. https://www.theguardian.com/world/2021/jan/06/facebook-instagram-urged-fight-deluge-anti-covid-vaccine-falsehoods.

Begg, Ian Maynard, Ann Anas, and Suzanne Farinacci. "Dissociation of Processes in Belief: Source Recollection, Statement Familiarity, and the Illusion of Truth." *Journal of Experimental Psychology: General* 121, no. 4 (1992): 446-458. doi: https://doi.org/10.1037/0096-3445.121.4.446.

Berger, Jonah. "Arousal Increases Social Transmission of Information." *Psychological Science* 22, no. 7 (2011): 891-893. doi: https://doi.org/10.1177/0956797611413294.

Berger, Jonah, and Katherine L. Milkman. "What Makes Online Content Viral?". *Journal of Marketing Research* 49, no. 2 (2012): 192-205. doi: https://doi.org/10.1509/jmr.10.0353.

Blake, Aaron. "A New Study Suggests Fake News Might Have Won Donald Trump the 2016 Election." *The Washington Post*. Apr. 3, 2018. Accessed Feb. 1, 2021. https://www.washingtonpost.com/news/the-fix/wp/2018/04/03/a-new-study-suggests-fake-news-might-have-won-donald-trump-the-2016-election/.

Bordia, Prashant, and Nicholas DiFonzo. "Psychological Motivations in Rumor Spread." In *Rumor Mills: The Social Impact of Rumor and Legend*, edited by Gary Allen Fine, Veronique Campion-Vincent, and Chip Heath. NY: Aldine Press, 2005.

Brady, William J., M. J. Crockett, and Jay J. Van Bavel. "The MAD Model of Moral Contagion: The Role of Motivation, Attention, and Design in the Spread of Moralized Content Online." *Perspectives on Psychological Science* 15, no. 4 (2020): 978-1010. doi: 10.1177/1745691620917336.

Page 2777 of 3957

Brady, William J., Ana P. Gantman, and Jay J. Van Bavel. "Attentional Capture Helps Explain Why Moral and Emotional Content Go Viral." *Journal of Experimental Psychology: General* 149, no. 4 (2020): 746-756.

Brooking, Emerson, and Suzanne Kianpour. *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century.* Atlantic Council. 2020. Accessed Feb. 1, 2021. https://www.atlanticcouncil.org/wp-content/uploads/2020/02/IRAN-DIGITAL.pdf.

Brooks, Bernard P., Nicholas DiFonzo, and David S. Ross. "The GBN-Dialogue Model of Outgroup-Negative Rumor Transmission: Group Membership, Belief, and Novelty." *Nonlinear Dynamics, Psychology, and Life Sciences* 17, no. 2 (2013): 269-293.

Buchanan, Tom. "Why Do People Share False Information Online? The Effects of Message and Viewer Characteristics on Self-Reported Likelihood of Sharing Social Media Disinformation." *PLoS ONE* 15, no. 10 (2020): 1-33. doi: 10.5255/UKDA-SN-854297.

Carnegie, Dale. *How to Win Friends and Influence People*. New York: Simon & Schuster, 1936.

Castello, Thomas H., Shauna M. Bowes, Sean T. Stevens, Irwin D. Waldman, Arber Tasimi, and Scott O. Lilienfeld. "Clarifying the Structure and Nature of Left-Wing Authoritarianism." *Journal of Personality and Social Psychology* (2021 pre-print). doi: doi 10.31234/osf.io/3nprq.

Chaiken, Shelly, and Yaacov Trope. *Dual-Process Theories in Social Psychology*. New York: Guilford Press, 1999.

Chen, Adrian. "The Agency." *New York Times Magazine*. June 2, 2015. Accessed Feb. 2, 2021. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Cialdini, Robert B. *Influence: Science and Practice*. 4th ed. Boston: Allyn and Bacon, 2001.

"Columbian Chemicals Plant Explosion Hoax." Know Your Meme. 2014. Accessed Feb. 4, 2021. https://knowyourmeme.com/memes/columbian-chemicals-plant-explosion-hoax.

Compton, Josh. "Prophylactic Versus Therapeutic Inoculation Treatments for Resistance to Influence." *Communication Theory* 30, no. 3 (2020): 330-343. doi: https://doi.org/10.1093/ct/qtz004.

Compton, Josh, and Bobi Ivanov. "Untangling Threat During Inoculation-Conferred Resistance to Influence." *Communication Reports* 25 (2012): 1-13. doi: 10.1080/08934215.2012.661018.

Cook, John, Stephan Lewandowsky, and Ulrich K. H. Ecker. "Neutralizing Misinformation Through Inoculation: Exposing Misleading Argumentation Techniques Reduces Their Influence." *PLoS ONE* 12, no. 5 (2017). doi: https://doi.org/10.1371/journal.pone.0175799.

Cook, Sarah. "Welcome to the New Era of Chinese Government Disinformation." *The Diplomat*. May 11, 2020. Accessed Feb. 1, 2021. https://thediplomat.com/2020/05/welcome-to-the-new-era-of-chinese-government-disinformation/.

Crawford, Krysten. "Stanford Study Examines Fake News and the 2016 Presidential Election." Stanford News. Jan. 18, 2017. Accessed Feb. 2, 2021. https://news.stanford.edu/2017/01/18/stanford-study-examines-fake-news-2016-presidential-election/.

Davis, Lauren C. "The Flight from Conversation." *The Atlantic*. Oct. 7, 2015. http://www.theatlantic.com.

DiFonzo, Nicholas, Jason W. Beckstead, Noah Stupak, and Kate Walders. "Validity Judgments of Rumors Heard Multiple Times: The Shape of the Truth Effect." *Social Influence* 11 (2016): 22-39. doi: https://doi.org/10.1080/15534510.2015.1137224.

DiFonzo, Nicholas, and Prashant Bordia. "How Top Professionals Handle Hearsay: Corporate Rumors, Their Effects, and Strategies to Manage Them." *Public Relations Review* 26 (2000): 173-190.

———. "Rumor and Prediction: Making Sense (But Losing Dollars) in the Stock Market." *Organizational Behavior and Human Decision Processes* 71 (1997): 329-353.

———. *Rumor Psychology: Social and Organizational Approaches*. Washington D.C.: American Psychological Association, 2007. doi: https://doi.org/10.1037/11503-000.

Ecker, Ulrich K. H., Stephan Lewandowsky, Briony Swire, and Darren Chang. "Correcting False Information in Memory: Manipulating the Strength of Misinformation Encoding and its Retraction." *Psychonomic Bulletin & Review* 18 (2011): 570-578. doi: 10.3758/s13423-011-0065-1.

Page 2778 of 3957

Ecker, Ulrich K. H., Stephan Lewandowsky, and David T. W. Tang. "Explicit Warnings Reduce But Do Not Eliminate the Continued Influence of Misinformation." *Memory and Cognition* 38 (2010): 1087-1100. doi: 10.3758/MC.38.8.1087.

"Edgar Allan Poe—'The Balloon Hoax'." The Edgar Allan Poe Society of Baltimore. Last updated July 15, 2020. https://www.eapoe.org/works/info/pt049.htm.

Fazio, Lisa K. "Pausing to Consider Why a Headline Is True or False Can Help Reduce the Sharing of False News." *Harvard Kennedy School (HKS) Misinformation Review* 1, no. 2 (2020).

Festinger, Leon. *A Theory of Cognitive Dissonance*. Evanston, IL: Row, Peterson, 1957.

Fiske, Susan T., and Shelly E. Taylor. *Social Cognition: From Brains to Culture*. 3rd ed. London: SAGE Publishing, 2016.

Freedman, Alix M. "Rumor Turns Fantasy Into Bad Dream." *The Wall Street Journal*. May 10, 1991, 1991.

Gareev, Makhmut A. "Anticipate Changes in the Nature of War: Every Era Has Its Own Kind of Military Conflict, and its Own Constraints, and its Own Special Biases." Voyenno-Promyshlennyy Kuryer Online. Jun. 5, 2013.

Gerasimov, Valery V. "The Value of Science is Foresight." Ценность науки в предвидении. VPK. ВПК. Feb. 26, 2013. Accessed Feb. 1, 2021. https://vpk-news.ru/articles/14632.

———. "Vectors of the Development of Military Strategy." Векторы развития военной стратегии. Krasnaya Zvezda. Красная звезда. Mar. 4, 2019. Accessed Feb. 1, 2021. http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1.

Harmon-Jones, Eddie, ed. *Cognitive Dissonance: Reexamining a Pivotal Theory in Psychology*. Washington, DC: American Psychological Association, 2019. doi: https://doi.org/10.1037/0000135-000.

Horowitz, Donald L. *The Deadly Ethnic Riot*. Berkeley, CA: Univeristy of California Press, 2001.

"IRGC (Islamic Revolutionary Guard Corps)." Counter Extremism Project. Accessed Feb. 3, 2021. https://www.counterextremism.com/threat/irgc-islamic-revolutionary-guard-corps.

Jackson, Dean. "Issue Brief: How Disinformation Impacts Politics and Publics." National Endowment for Democracy. May 29, 2018. Accessed Feb. 2, 2021. https://www.ned.org/issue-brief-how-disinformation-impacts-politics-and-publics/.

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus, and Giroux, 2011.

Kahneman, Daneil, and Amos Tversky. "On the Psychology of Prediction." *Psychological Review* 80, no. 4 (1973): 237-251.

Kaminska, Izabella. "A Lesson in Fake News from the Info-Wars of Ancient Rome." *Financial Times*. Jan. 17, 2017. Accessed Feb. 3, 2021. https://www.ft.com/content/aaf2bb08-dca2-11e6-86ac-f253db7791c6.

Kaufman, Bruce E. "Emotional Arousal as a Source of Bounded Rationality." *Journal of Economic Behavior and Organization* 38, no. 135-144 (1999). doi: 10.1016/S0167-2681(99)00002-5.

Kliman, Daniel, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt, and Carisa Nietsche. *Dangerous Synergies.* CNAS. 2020. Accessed Feb. 1, 2021. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Dangerous-Synergies-May-2020-DoS-Proof.pdf?mtime=20200506164642&focal=none.

Kurlantzick, Joshua. "How China Ramped Up Disinformation Efforts During the Pandemic." Council on Foreign Relations. Sept. 10, 2020. Accessed Feb. 2, 2021. https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic.

Lee, Doowan. "The United States Isn't Doomed to Lose the Information Wars." *Foreign Policy*. Oct. 16, 2020. Accessed Feb. 3, 2021. https://foreignpolicy.com/2020/10/16/us-election-interference-disinformation-china-russia-information-warfare/.

Li, Cong. "Primacy or Recency Effect? A Long-Term Memory Test of Super Bowl Commercials." *Journal of Consumer Behavior* 9, no. 1 (2009): 32-44.

Page 2779 of 3957

Lin, Wei-Kuo, and Michael Pfau. "Can Inoculation Work Against the Spiral of Silence? A Study of Public Opinion on the Future of Taiwan." *International Journal of Public Opinion Research* 19, no. 2 (2007): 155-172. doi: 10.1093/ijpor/edl030.

Mayo, Ruth. "Cognition Is a Matter of Trust: Distrust Tunes Cognitive Processes." *European Review of Social Psychology* 26 (2015): 283-327. doi: https://doi.org/10.1080/10463283.2015.1117249.

McBride, Megan, Zack Gold, and Kasey Stricklin. *Social Media Bots: Implications for Special Operations Forces.* CNA. DRM-2020-U-028199-Final. Sept. 2020. Accessed Feb. 2, 2021. https://www.cna.org/CNA_files/PDF/DRM-2020-U-028199-Final.pdf.

McGuire, William. "Resistance to Persuasion Conferred by Active and Passive Prior Refutation of Same and Alternative Counterarguments." *Journal of Abnormal Psychology* 63, no. 2 (1961): 326-332.

Mikkelson, David. "Did Keanu Reeves Say Hollywood Elites Use the 'Blood of Babies' to Get High?". Snopes. Nov. 22, 2017. Accessed Feb. 1, 2021. https://www.snopes.com/fact-check/keanu-reeves-blood-drinking/.

Milkman, Katherine L., and Jonah Berger. "The Science of Sharing and the Sharing of Science." *Proceedings of the National Academies of Science* 111 no. Supplement 4 (2013): 13642-13649. doi: 10.1073/pnas.1317511111.

Mosleh, Mohsen, Gordon Pennycook, Antonio A. Arechar, and David G. Rand. "Cognitive Reflection Correlates with Behavior on Twitter." *Nature Communications* 12, no. 921 (2021).

Murdock, Bennet B., Jr. "The Serial Position Effect on Free Recall." *Journal of Experimental Psychology* 64, no. 5 (1962): 482-488. doi: https://doi.org/10.1037/h0045106.

Murphy, Jamie, Charles Hofacker, and Richard Mizerski. "Primacy and Recency Effects on Clicking Behavior." *Journal of Computer-Mediated Communication* (2020): 522-535.

Nemr, Christina, and William Gangware. *Weapons of Mass Distraction.* Park Advisors. 2019. Accessed Feb. 2, 2021. https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

Nossal, Gustav J. "Vaccination." In *Encyclopedia of Life Sciences*. Hoboken, NJ: Wiley, 1999. www.els.net.

Pellegrino, Bianca. "People Famous For Doing Things They Didn't Do." ListVerse. Sept. 8, 2019. https://listverse.com/2019/09/08/top-10-people-famous-for-doing-things-they-didnt-do/.

Pennycook, Gordon, and David G. Rand. "Lazy, Not Biased: Susceptibility to Partisan Fake News Is Better Explained by Lack of Reasoning than by Motivated Reasoning." *Cognition* 188 (July 2019): 39-50. doi: https://doi.org/10.1016/j.cognition.2018.06.011.

Pennycook, Gordon, Jonathan McPhetres, Yunhao Zhang, Jackson G. Lu, and David G. Rand. "Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy Nudge Intervention." *Psychological Science* 31, no. 7 (2020). doi: https://doi.org/10.1177/0956797620939054.

Pfau, Michael, Kyle J. Tusing, Ascan F. Komer, Waipeng W. Lee, Linda C. Godbold, Linda J. Penaloza, Violet S. Yang, and Hong, Yah-Huei "Enriching the Inoculation Construct: The Role of Critical Components in the Process of Resistance." *Human Communication Research* 24, no. 2 (1997): 187-215. doi: 10.1111/j.1468-2958.1997.tb00413.x.

Roiser, Martin, and Carla Willig. "The Strange Death of the Authoritarian Personality: 50 Years of Psychological and Political Debate." *History of the Human Sciences* 15, no. 4 (2002): 71-96. doi: 10.1177/952695102015004682.

Rosnow, Ralph L., James L. Esposito, and Leo Gibney. "Factors Influencing Rumor Spreading: Replication and Extension." *Language and Communication* 8, no. 29-42 (1988).

Saaty, T. L., and Müjgan Sagir Özdemir. "Why the Magic Number Seven Plus or Minus Two." *Mathematical and Computer Modelling* 38 (2003): 233-244. doi: 10.1016/S0895-7177(03)90083-5.

Page 2780 of 3957

Schmaltz, Rodney, and Scott Lilenfeld. "Hauntings, Homeopathy, and the Hopkinsville Goblins: Using Pseudoscience to Teach Scientific Thinking." *Frontiers in Psychology* 5 (2014): 1-5. doi: https://doi.org/10.3389/fpsyg.2014.00336.

Schreck, Carl. "Photoshop Wars: U.S. Ambassador 'Attends' Russian Opposition Rally...and the Moon Landing." Radio Free Europe/Radio Liberty. Sept. 21, 2015. Accessed Feb. 3, 2021. https://www.rferl.org/a/russia-photoshop-us-ambassador-tefft-opposition-rally-ren-tv/27260885.html.

Shane, Tommy. "The Psychology of Misinformation: How to Prevent It." First Draft News. July 27, 2020. https://firstdraftnews.org/latest/the-psychology-of-misinformation-how-to-prevent-it/.

———. "The Psychology of Misinformation: Why We're So Vulnerable." First Draft News. June 30, 2020. https://firstdraftnews.org/latest/the-psychology-of-misinformation-why-were-vulnerable/.

Stricklin, Kasey. "Why Does Russia Use Disinformation?". Lawfare. Mar. 29, 2020. Accessed Feb. 2, 2021. https://www.lawfareblog.com/why-does-russia-use-disinformation.

Swire, Briony, and Ulrich K. H. Ecker. "Misinformation and Its Correction: Cognitive Mechanisms and Recommendations for Mass Communications." In *Misinformation and Mass Audiences*, edited by Brian Southwell, Emily A. Thorson, and Laura Sheble. Austin: University of Texas Press, 2018.

Swire, Briony, Ulrich K. H. Ecker, and Stephan Lewandowsky. "The Role of Familiarity in Correcting Inaccurate Information." *Journal of Experimental Psychology: Learning, Memory, and Cognition* 43, no. 12 (2017): 1948-1961. doi: 10.1037/xlm0000422.

Thaler, Richard H., and Cass R. Sunstein. *Nudge: Improving Decisions about Health, Wealth and Happiness*. New Haven, CT: Yale University Press, 2008.

Turkle, Sherry. *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York: Basic Books, 2011.

———. *The Empathy Diaries: A Memoir*. New York: Penguin Publishing, 2021.

———. *Life on the Screen: Identity in the Age of the Internet*. New York: Touchstone, 1997.

———. *Reclaiming Conversation: The Power of Talk in the Digital Age*. New York: Penguin Books, 2015.

Unkelbach, Christian. "Reversing the Truth Effect: Learning the Interpretation of Processing Fluency in Judgments of Truth." *Journal of Experimental Psychology: Learning, Memory, and Cognition* 33, no. 1 (2007): 219-230. doi: 10.1037/0278-7393.33.1.219.

"US Ambassador to Russia John F. Tefft Is Sent to Opposition Rally in Maryino." Посла США в России Джона Ф. Теффта отправили на митинг оппозиции в Марьине. Ren.TV. Sept. 20, 2015. http://ren.tv/novosti/2015-09-20/posla-ssha-v-rossii-dzhona-f-teffta-otpravili-na-miting-oppozicii-v-marine.

Vosoughi, Soroush, Deb Roy, and Sinan Aral. "The Spread of True and False News Online." *Science* 359, no. 6380 (2018): 1146-1151. https://science.sciencemag.org/content/359/6380/1146.

Woodsome, Kate, Danielle Kunitz, and Joy Sharon Yi. "Our Political Divide Is Dangerous. A Neuroscientist and Political Scientist Explain Why." *Washington Post*. Dec. 24, 2020.

Yerkes, Robert M., and John D. Dodson. "The Relation of Strength of Stimulus to Rapidity of Habit-Formation." *Journal of Comparative Neurology and Psychology* 18 (1908): 459-482.

Zakem, Vera, Megan McBride, and Kate Hammerberg. *Exploring the Utility of Memes for U.S. Government Influence Campaigns.* CNA. DRM-2018-U-017433-Final. 2018. https://www.cna.org/cna_files/pdf/DRM-2018-U-017433-Final.pdf.

Page 2781 of 3957

This report was written by CNA's Strategy, Policy, Plans, and Programs Division (SP3).

SP3 provides strategic and political-military analysis informed by regional expertise to support operational and policy-level decision-makers across the Department of the Navy, the Office of the Secretary of Defense, the unified combatant commands, the intelligence community, and domestic agencies. The division leverages social science research methods, field research, regional expertise, primary language skills, Track 1.5 partnerships, and policy and operational experience to support senior decision-makers.

CNA is a not-for-profit research organization that serves the public interest by providing in-depth analysis and result-oriented solutions to help government leaders choose the best course of action in setting policy and managing operations.

Dedicated to the Safety and Security of the Nation

DRM-2021-U-029337-1Rev-2

3003 Washington Boulevard, Arlington, VA 22201
www.cna.org ● 703-824-2000

PERSEREC

Technical Report 05-6
May 2005

Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers

Suzanne Wood
Consultant to Northrop Grumman Mission Systems

Kent S. Crawford
Eric L. Lang
Defense Personnel Security Research Center

Approved for Public Distribution:
Distribution Unlimited.

Research Conducted by
Defense Personnel Security Research Center

Technical Report 05-6 **May 2005**

Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers

Suzanne Wood
Consultant to Northrop Grumman Mission Systems

Kent S. Crawford
Eric L. Lang
Defense Personnel Security Research Center

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD·MM·YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
31-05-2005	Technical	2002-2005

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Suzanne Wood, Kent S. Crawford, Eric L. Lang	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	8. PERFORMING ORGANIZATION REPORT NUMBER TR 05-6
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	10. SPONSORING/MONITOR'S ACRONYM(S) 11. SPONSORING/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

13. SUPPLEMENTARY NOTES

14. ABSTRACT

PERSEREC recently conducted a study of supervisor and coworker reporting of security-related information. Explanations were offered by security managers and by focus group participants as to why many security-related behaviors are under-reported. The main problem is that people are hesitant to report suitability behaviors, such as excessive drinking, because they are not able to see a direct link between the particular human problem and national security. Consequently, PERSEREC developed a clear, succinct list of behaviors that could pose a potential threat to national security and thus should be reported if observed. Members of various counterintelligence agencies in the government reviewed and edited this list. It has since been included in the new DoD Instruction 5240.6 *Counterintelligence Awareness, Briefing, and Reporting Programs* as Enclosure 3. In addition, PERSEREC developed a brochure based on these items as an educational tool to help DoD components and other departments that have need of security education materials on supervisor and coworker reporting or for counterintelligence briefings.

15. SUBJECT TERMS
Supervisor reporting; coworker reporting; counterintelligence indicators

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF REPONSIBLE PERSON
Unlimited Distribution				57	James A. Riedel, Director
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER *(Include area code)* 831-657-3000

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Preface

PERSEREC recently conducted a study of supervisor and coworker reporting of information of security concern. In response to our probing for answers as to why security-related behaviors are under-reported, interviewees and participants in focus groups said that policies were written too broadly for them to implement. The participants also said that they were very willing to report serious behaviors that clearly related to counterintelligence or security, but much less willing to report on suitability types of behaviors, such as excessive drinking and personal problems, because they were not able to see the direct link between the human problem and national security. They would prefer that these personal troubles be handled through employee assistance programs or other monitored treatment programs.

In response to these research findings, PERSEREC developed a list of Counterintelligence Reporting Essentials (CORE) that contained items that were primarily behavioral and clearly linked to counterintelligence and security risk. Working with the counterintelligence community, PERSEREC honed the list to 16 items. These 16 items were included as Enclosure 3 in the new DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs*.

In addition, PERSEREC created a CORE brochure that can be disseminated throughout the counterintelligence and security communities. The brochure briefly discusses the rationale for developing the CORE list, describes potential uses by security professionals, and lists the specific behaviors that should be reported. The behaviors fall under the headings, Recruitment, Information Collection, Information Transmittal, and Suspicious Behaviors.

We believe the CORE list—as a new policy enclosure and an easy-to-read brochure—responds directly to the concerns of clearance holders in a way that is likely to improve security awareness and overall reporting of security-relevant behaviors.

James A. Riedel
Director

Page 2790 of 3957

Page 2791 of 3957

Acknowledgements

The authors would like to express their appreciation to a number of people who helped with this research. Thanks to Troy Sullivan and Windell Courson, staff members at the Department of Defense Counterintelligence Directorate, Office of the Under Secretary of Defense (Intelligence), who worked with the authors in deciding which of PERSEREC's reportable behaviors would be included as an Enclosure to the new DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs.*

PERSEREC's original CORE list had circulated in October 2002 among the staff of the Joint Counterintelligence Evaluation Office (JCEO) under Mary Griggs. JCEO then distributed the list to members of the DoD Investigative Working Group (IWG), representing Army Military Intelligence, Air Force Office of Special Investigations, Defense Intelligence Agency, Defense Security Service, National Security Agency, Naval Criminal Investigative Service, and the National Reconnaissance Office, and to a number of counterintelligence personnel at the Counterintelligence Field Activity (CIFA). We are grateful to these people for their helpful comments and suggestions. Many thanks also to Virginia Kirk at JCEO for her administrative and logistical assistance.

Page 2792 of 3957

x

Executive Summary

Background

In January 2003, the Defense Personnel Security Research Center (PERSEREC) published a report of a study that examined the supervisor and coworker reporting requirement within the Department of Defense's (DoD) personnel security program (Wood & Marshall-Mies, 2003). The study dealt with self-initiated reporting, when a person would see a subordinate or colleague behaving inappropriately and report the behavior to Security. One of the aims of the study was to better understand the prevalence of workplace reporting, the kinds of behaviors that are reported, and the reasons people may not report. To this end, researchers interviewed 45 security managers and management personnel in 20 DoD and non-DoD federal agencies who described the reporting rate as very low, perhaps reflecting an under-reporting of relevant behaviors. They offered a series of explanations as to why people may not report, including cultural resistance; negative perceptions of reporting; lack of knowledge and experience of the system among security officers, supervisors, and the workforce; and unclear relationships between Security, employee assistance programs, and other functions.

The PERSEREC study also included several focus groups with supervisors and employees at various federal agencies to learn participants' views and recommendations concerning reporting. Focus group participants made it clear that they are willing to report egregious behaviors that they believe pose a likely threat to national security. They simply want to know precisely what such behaviors are. Wording of policy, in their opinion, is amorphous and confusing. All participants without exception said that they would seldom report certain gray-area behaviors that they describe as too personal ("the more private things," as one put it). Such behaviors may include emotional or mental, financial, alcohol and drugs, and marital problems, and unusual personal conduct. Research suggested that participants are reluctant to report these behaviors because they cannot see a link between the behavior and national security; in other words, they are unlikely to be convinced of the security relevance of personal problems. They may also be reluctant because they do not trust the system to deal with the reports equitably and also may fear possible reprisals to themselves as so-called whistleblowers.

In an attempt to end confusion about what should always be reported, the PERSEREC study recommended the development of a list of egregious behaviors that are closely connected to counterintelligence (CI) and security. The list would not include behaviors of a suitability or reliability nature since the research showed that supervisors and coworkers have said they would be unlikely to report such matters.

The present report documents the rationale for preparing the list and describes the processes by which it was developed and its eventual inclusion as Enclosure 3 in the new DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs*.

Page 2794 of 3957

Method

Research comprised the following steps: (1) comparison of major CI policy documents; (2) review of other source documents; (3) development of a draft Counterintelligence Reporting Essentials (CORE) list of behaviors that must be reported; (4) presentation of the draft CORE list for review and editing by CI experts; (5) introduction of the final CORE list into DoD policy; and (6) promulgation and implementation of the final CORE list, through the Defense Security Service (DSS) and other CI entities, for use in security and education programs and CI briefings.

Policy Review and Review of Other Source Documents

The various key policy documents that concern the reporting of CI and security-related behaviors were compared and contrasted, exploring areas of overlap, specificity, and authoritative procedures, i.e., whether one policy superseded another. Other documents and publications that have been developed by DoD, intelligence community agencies, and PERSEREC in the area of CI awareness and education were also reviewed. Examination of these documents provided background, context, and a pool of information from which PERSEREC researchers could draw as they developed the draft CORE list.

Development and Evaluation of Draft CORE List of Behaviors

PERSEREC researchers proceeded to pull together a draft CORE list of behaviors that are observable and may be associated with potential risk to national security. This became known as the CORE list.

The draft CORE list was evaluated by staff at the Joint Counterintelligence Evaluation Office (JCEO), the DoD Investigative Working Group (IWG), and by the Counterintelligence Field Activity (CIFA). The list was then reviewed by staff at the DoD Counterintelligence Directorate in the Office of the Under Secretary of Defense (Intelligence).

Introduction of Draft CORE List into DoD Instruction 5240.6

The 16 items in the final CORE list were added as an Enclosure to the revision of DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs*.

Implementation of PERSEREC's Brochure in the Field

PERSEREC developed a separate brochure that includes the 16 original PERSEREC CORE list items, along with eight others added by the DoD Counterintelligence Directorate. This brochure, which explains the rationale for the list and its potential uses, is attached to this report as a pdf file and is detachable for use in the field.

Page 2795 of 3957

Recommendation

DoD should distribute the PERSEREC brochure to CI and security agencies for their review and possible implementation. Possible uses include security education briefings of various sorts (e.g., initial, refresher, and CI awareness). By concentrating on direct CI- and security-related behavior, personnel in the field are likely to develop a better understanding of exactly what to report and a greater commitment to reporting it.

Page 2797 of 3957

Table of Contents

Background 1

Method 1

Policy Review 2

Review of Other Source Documents 6

Development of Draft CORE List of Behaviors 7

Evaluation of Draft CORE List by Counterintelligence Experts 8

Introduction of Draft CORE List Items into DoD Instruction 5240.6 9

Implementation of CORE Brochure in the Field 10

Recommendation 11

References 13

Appendices

Appendix A: Department of Defense Instruction 5240.6 (August 7, 2004) A-1

**Appendix B: COUNTERINTELLIGENCE REPORTING ESSENTIAL (CORE)
A Practical Guide for Reporting Counterintelligence and Security Indicators** B-1

Page 2798 of 3957

Page 2799 of 3957

Background

PERSEREC in 2003 published a report that studied self-initiated reporting, where supervisors and co-workers person observe suspicious behavior by a fellow worker (usually in the workplace) and report it to a supervisor or security official (Wood & Marshall-Mies, 2003).

During the course of the study, PERSEREC staff learned from several sources—extensive literature reviews, headquarters management personnel, and people working in the field—that, despite formal policies requiring employees to report security-related behaviors, they do so only rarely. Yet employees in the field are not averse to reporting genuine security infractions. In fact, under appropriate conditions, they are quite willing to act as eyes and ears for the government. They are simply confused about precisely what is important enough to report. Many government workers anguish over reporting gray-area behaviors they do not consider to be clearly connected to security. They say the policies are written too broadly for the average person in the field. One supervisor, echoing the opinion of many, said, "We need a clear communication of what is mandatory to report." A coworker complained, "You can't ask people to do something if you don't define it…We need more definitions. How do we know which behaviors are OK and which are not?"

One of the study recommendations, therefore, was that PERSEREC, in collaboration with counterintelligence (CI) professionals, develop a clear, succinct list of behaviors that could pose a potential threat to national security and thus should be reported if observed. This list, to be known as the Counterintelligence Reporting Essentials (CORE) list, would contain behavioral examples to clarify what is considered egregious or potentially critical to national security. Use of the CORE list should then facilitate reporting of truly significant behaviors. Behaviors that raise questions about reliability, the gray-area behaviors that interviewees said they would be less willing to report, would be handled by supervisors through counseling, employee assistance programs, or other monitored treatment programs. The goal was to produce a relevant and useful CORE list, which, through adoption as policy, could be employed to improve reporting requirements and security education programs.

Method

The research methodology to produce, review, and implement the CORE list required six steps: (1) comparison of major CI policy documents; (2) review of other source documents; (3) development of a draft CORE list of behaviors that must be reported; (4) presentation of the list to CI experts for review and editing; (5) introduction of the CORE list into Department of Defense (DoD) policy; and (6) promulgation and implementation, through the Defense Security Service (DSS) and other CI entities, for use in security and education programs and in CI briefings.

Page 2800 of 3957

Policy Review

The purpose of this section is to report our review of all of the different policy documents related to supervisor and coworker reporting and to compare and contrast the requirements of various entities with regard to this subject. PERSEREC researchers reviewed the policies, Directives, and Executive Orders that concern the reporting of CI- and security-related behaviors. The review explored areas of overlap, specificity, and authoritative procedures, i.e., whether one policy superseded another.

The Clinton administration's Presidential Decision Directive PDD/NSC-12, *Security Awareness and Reporting of Foreign Contacts* (August 5, 1993) requires that government employees report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which illegal or unauthorized access is sought to classified or otherwise sensitive information, or the employee is concerned that he or she may be the target of actual or attempted exploitation by a foreign entity.

Executive Order 12968 (August 4, 1995) states in Sec. 6.2(a) that employees should protect classified information from unauthorized disclosure; report all contacts with persons, including foreign nationals, who seek to obtain classified information; report all violations of security regulations to appropriate security officials; and comply with all other security requirements of the order. It adds in Sec. 6.2(b): "Employees are also encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security."

Title 50, USC, Chapter 23, Subchapter 1, Sec. 797, lays out the penalties for violating security regulations at a variety of government facilities and under a variety of circumstances. Such a violation will constitute a misdemeanor and carry with it, upon conviction, a fine not to exceed $5,000 or imprisonment for not more than one year, or both.

The Director of Central Intelligence Directive (DCID) 6/4, *Personnel Security Standards* (July 2, 1998), lists (Annex E, 6 [a] – [m]) several general categories of behavior that are reportable if observed in the workplace. These are similar to the adjudicative guidelines (in the DoD Directive 5200.2-R) except that they do not include the brief behavioral descriptions that appear in the adjudicative guidelines. The categories, which—like the adjudicative guidelines—mix CI, security and reliability issues, are listed below. Only two—(b) and (c)—are strictly related to CI issues.

(a) Involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate the overthrow or alteration of the United States Government by unconstitutional means.

(b) Foreign influence concerns/close personal association with foreign nationals.

(c) Foreign citizenship or foreign monetary interests.

(d) Sexual behavior that is criminal or reflects a lack of judgment or discretion.

(e) Unwillingness to comply with rules and regulations or to cooperate with security processing.

(f) Unexplained affluence or excessive indebtedness.

(g) Alcohol abuse.

(h) Illegal or improper drug use/involvement.

(i) Apparent mental or emotional disorder(s).

(j) Criminal conduct.

(k) Noncompliance with security requirements.

(l) Engagement in outside activities that could cause a conflict of interest.

(m) Misuse of information technology systems.

The 1996 DoD Instruction 5240.6 (*Counterintelligence [CI] Awareness and Briefing Program*) (July 16, 1996) differed significantly from the DCID 6/4. DoD Instruction 5240.6 is the fundamental, workhorse instruction for CI awareness and briefing programs for DoD. (For an analysis of the new DoD Instruction 5240.6, please see pp. 9-10 below.)

In the 1996 DoD Instruction 5240.6, the 13 reportable items from DCID 6/4 were described only briefly and included items that were not strictly CI-related, e.g., sexual behavior, alcohol abuse, illegal or improper drug use/involvement, apparent mental or emotional disorders. While several items were quite specific, e.g., behaviors such as contacts with foreign intelligence or terrorist organizations, requests for unauthorized access to classified or unclassified controlled information, contacts with known or suspected foreign intelligence officers, and contacts with foreign diplomats, the instruction went on to list (at 6.1.2) an amalgam of behaviors, strung together in one sentence and describing 10 broad areas that lack specificity and are often repetitive of themselves. "…DoD personnel who have information about activities pertaining to espionage, terrorism, unauthorized technology transfer, sabotage, sedition, subversion, spying, treason, unauthorized release of classified or unclassified controlled information, or unauthorized instructions into automated information systems."

The military services published their own instructions, based on the 1996 DoD Instruction 5240.6. The Air Force's AFI71-101V4, *Counterintelligence* (August 1, 2000), closely mirrors the 1996 DoD Instruction 5240.6, as does the Navy's SECNAVINST 3875.1A *Counterintelligence and Awareness Briefing Program* (February 19, 1999).

Page 2802 of 3957

The Army, however, expands considerably on reporting requirements in its AR 381-12 *Military Intelligence Subversion and Espionage Directed Against the U.S. Army (SAEDA)* (January 15, 1993). In Chapter 3, *Reporting Requirements*, it addresses three areas: *SAEDA Incidents*, *Additional Matters of CI Interest*, and *Indicators of Espionage*. The segment on SAEDA incidents describes the incidents and situations that must be reported, these items reflecting the old DoD 5240.6 but in much more detail. The next section, *Additional Matters of CI Interest*, expands greatly the reportable behaviors. These include, for example, the discovery of listening devices; unauthorized absence of Department of the Army (DA) personnel with high-level clearances; reports of attempted or actual suicide; COMSEC insecurities; assassination (or attempts) of anyone by terrorists or agents of foreign powers; defection, or attempted or threatened defections; detention of personnel by a foreign government with interests inimical to those of the US; impersonation of DA intelligence personnel; willful compromise of the identify of US intelligence personnel engaged in clandestine intelligence and CI activities; and incidents in which foreign countries offer employment to US personnel involved in the development of nuclear weapons.

The third section of AR 381-12, *Indicators of Espionage*, lists 19 behaviors that may be indicative of espionage, although the regulation stresses that while a single indicator by itself does not necessarily mean that a person is engaged in espionage, it must be reported. This list is reproduced below:

(a) Any attempt to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities or attempting to obtain information for which the person has no authorized access or need to know.

(b) Unauthorized removed of classified materials from work area.

(c) Extensive use of copy, FAX or computer equipment to reproduce or transmit classified material that may exceed job requirements.

(d) Repeated or unrequired work outside normal duty hours, especially unaccompanied.

(e) Obtaining witness signatures on classified document destruction forms when witness did not observe the destruction.

(f) Bringing unauthorized cameras, recording devices, computers or modems into areas where classified data is stored, discussed, or processed.

(g) Unexplained or undue affluence, including sudden purchases of high-value items where no logical income source exists. Attempts to explain wealth by reference to inheritance, luck in gambling, or some successful business venture.

Page 2803 of 3957

(h) Opening several bank accounts containing substantial sums of money where no logical income source exists.

(i) Free spending or lavish display of wealth which appears beyond normal income.

(j) Sudden reversal of financial situation or sudden repayment of large debts or loans.

(k) Correspondence with persons in countries of special concern.

(l) Unreported contact with officials of countries of special concern.

(m) Frequent or unexplained trips of short duration to foreign countries.

(n) Attempts to offer extra income from an outside endeavor to personnel with sensitive jobs or to entice them into criminal situations that could lead to blackmail.

(o) Homesteading or repeatedly requesting extensions to tours of duty in one assignment or location, especially when the assignment offers significant access to sensitive information or the job is not desirable.

(p) Repeated involvement in security violations.

(q) Joking or bragging about working for a foreign intelligence service.

(r) Visits to a foreign embassy, consulate, trade, or press office.

(s) Business dealings with nationals or firms of countries of concern.

In summary, DoD Instruction 5240.6, flowing from higher-level policies such as a Presidential Decision Directive and an Executive Order, lays out the basic requirement for CI awareness and briefing programs in the DoD. Air Force and Navy wrote instructions that closely parallel the DoD instruction; the Army elaborated on the instruction, providing more details and specifics. Requirements vary somewhat from one entity to another. PERSEREC staff decided that a short, succinct list of reportable behaviors is needed rather than having supervisors, coworkers, and agencies deal with the plethora of different approaches and degrees of specificity found in the different policies.

Page 2804 of 3957

Review of Other Source Documents

Having completed the policy review, PERSEREC staff reviewed a selection of publications and documents that have been developed by DoD, intelligence community agencies and PERSEREC in the area of counterintelligence awareness and education. These would provide the context and information required to construct PERSEREC's draft CORE list.

DSS published in January 1998 a For Official Use Only (FOUO) document, "Recognition of Potential Counterintelligence Issues." The document was intended to aid the facility security officers of cleared U.S. defense contractors in recognizing potential CI issues.

PERSEREC's *Employees' Guide to Security Responsibilities* has a section on CI indicators.[1] This contains 23 items grouped into five categories: (1) potential motivation, (2) potential indicators of information collection, (3) potential indicators of information transmittal, (4) potential indicators of illegal income, and (5) other potential indicators. (The Guide also has a list of security and suitability behaviors, organized according to the 13 adjudicative guidelines, e.g., alcohol consumption, allegiance to the United States, criminal conduct, drug involvement, etc.)

DoD 5220.22-M, *National Industrial Security Program Operating Manual* (January 1995), Section 1-300 General, under *Reporting Requirements*, states that contractors are required to report certain events that have an impact on the status of the facility clearance, impact on the status of an employee's personnel clearance, affect proper safeguarding of classified information, or indicate classified information has been lost or compromised. Contractors are required to establish such internal procedures as are necessary to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the facility security officer, the FBI, or other Federal authorities as required by the Manual, the terms of a classified contract, and U.S. law. The manual states that contractors must provide complete information to enable the authorities to ascertain whether classified information is adequately protected. Contractors must submit reports to the FBI, and to their local security officials. This appears to be the only place in the National Industrial Security Program Operating Manual (NISPOM) where reporting requirements are mentioned.

DSS publishes an annual brochure for security professionals, CI personnel, and cleared contractors, *Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed Against the U.S. Defense Industry.* The brochure is designed to help employees recognize suspicious contacts. The most frequent information-gathering method employed by foreign entities is simply to request information from individuals working in U.S. defense industry science and technology programs. The brochure lists indicators to watch for and appropriate security countermeasures to apply. Other methods include inappropriate conduct during visits;

[1]For more detail, see the *Employees' Guide to Security Responsibilities* on the Web at www.dss.mil/training/securityawareness.htm.

Page 2805 of 3957

suspicious work offers; international exhibits, conventions and seminars; joint ventures/joint research; foreign acquisition of technology and companies; co-opting former employees; and targeting cultural commonalities. For each of these methods, DSS provides a list of indicators and recommended security countermeasures.

The following agency brochures and booklets were also reviewed:

- CIA orientation briefing, "Reporting of Security-Relevant Behavior Requirements"
- CIA brochure, "Why We Care: A Guide for Understanding Suitability and CI Indicators" (FOUO)
- DIA brochure, "Plenty of Excuses But No Good Reasons"
- DIA brochure, "Countering Espionage"
- DISA Newcomers' Briefing
- DSS's "Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed against the U.S. Defense Industry"
- DOE brochure, "Counterintelligence in our Changing World"
- DOE brochure, "Clues to Spotting a Spy"
- FBI "Security Handbook"
- Navy "Security Awareness Chronicle"
- NCIS list, "Indicators of Espionage"
- NIMA "MSSR," unclassified video briefing on espionage, recruitment, security, reporting requirements, etc.
- NSA booklet, "Foreign Intelligence Recruitment Approaches"
- State Department's booklet, "Counterintelligence for the 1990s and Beyond"

Each agency mentioned above had its own perspective on the subject of CI awareness programs, producing guides, learning tools, manuals, studies, handbooks, brochures and booklets that contain all the indicators and behaviors that agencies have considered to be of CI concern. Review of the above documents provided background and a pool of information from which PERSEREC researchers could draw as they prepared the draft CORE list. Researchers were able to cull items from the above publications and re-arrange them in a more systematic way that would make sense to employees in the field.

Development of Draft CORE List of Behaviors

Having reviewed the various policies and related materials listed above and compared and contrasted the strengths and weaknesses of each in terms of clarity and level of detail, PERSEREC researchers developed from the documents a list that included behaviors that should be reported when observed because they are genuine security violations or have serious CI significance. Researchers focused on behavioral items that clearly reflect security and CI risk. Items that were too vague, non-behavioral (e.g., that

required an observer to intuit another person's state of mind), or not clearly associated with a security risk were eliminated.

The draft CORE list was developed in a series of steps, each step building on the previous one. As we sequentially reviewed the documents listed below we added new items not covered in the previous documents until we reached a saturation point where we had captured all items that fell within our selection criteria, i.e., behaviors that are observable and may be associated with a risk to national security. The aim was to construct a list that was simple, short, effective, and credible to the reader. Below are listed the steps we followed in constructing the draft CORE list.

(1) Reviewed DCID 6/4 (13 adjudication guidelines).

(2) Compared DCID 6/4 with DoD Instruction 5240.6 "Counterintelligence Awareness and Briefing Program."

(3) Compared the above two documents with SAEDA regulations and unclassified briefing, "Indicators."

(4) Then added items from PERSEREC's "Employees' Guide to Security Responsibilities."

(5) Then reviewed assorted agency brochures and booklets to see what reportable behaviors might have been missed.

(6) Incorporated all the behaviors culled from the above materials into one list, using as the selection criterion the fact that the behavior clearly should be reported because it is a CI- or security-related violation. The draft CORE list was then carefully reviewed by a panel of five additional researchers at PERSEREC who attempted to eliminate any items that were essentially non-behavioral (e.g., mostly required judgment calls on the part of the potential reporter).

Having developed a draft CORE list, it was important to have it evaluated by professional CI experts.

Evaluation of Draft CORE List by Counterintelligence Experts

In October 2002, the draft CORE list was circulated among the staff of the Joint Counterintelligence Evaluation Office (JCEO) for their review. In turn, JCEO distributed the list to members of the DoD Investigative Working Group (IWG) and to a number of retired FBI officials working for the Counterintelligence Field Activity (CIFA). These individuals provided editorial and substantive comments on the draft CORE list, and their responses were incorporated. The list was then reviewed in April 2003 by CI personnel in the DoD Counterintelligence Directorate under the Office of the Under Secretary of Defense (Intelligence) (OUSD[I]). Directorate staff reviewed the items and made

valuable changes to some. Of PERSEREC's original 30 items, the CI staff advised PERSEREC to reject three, either because the items were not supported by policy or because items raised legal concerns. PERSEREC staff subsequently eliminated these three and eliminated an additional item because it duplicated another. A few items were combined.

Introduction of Draft CORE List into DoD Instruction 5240.6

PERSEREC reviewed an early draft of the new DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs*, dated April 21, 2003, for potential coordination with the CORE list. PERSEREC staff members worked with DoD Counterintelligence Office staff who wrote the instruction and wanted to include PERSEREC's draft CORE list into the new instruction. The instruction was promulgated August 7, 2004.

The instruction, in Item 6 *Procedures*, adds a new section (6.1.) that discusses awareness and briefing programs. It then describes in 6.1.3. the kinds of information that must be included in CI briefings: information about early detection of espionage and other suspected foreign intelligence and terrorist activities; comprehensive tailored threat information focusing on foreign intelligence, terrorism and other threats; information about the DoD anomalies program;[2] and reporting responsibilities and procedures. In Item 6.2, *Reporting Requirements*, the new instruction states (at 6.2.1) that DoD personnel "shall report information pursuant to E.O. 12968 and DoD 5200.2-R…concerning security violations and other information with potentially serious security significance regarding someone with access to classified information employed in a sensitive position." The new instruction refers the reader to an Enclosure 3, where specific behaviors that must be reported are listed. This is an extremely important device that provides the reader explicit examples of reportable behavior.

Item 6.2.2 states "DoD personnel shall expeditiously report any contacts or circumstances that could pose a threat to the security of U.S. personnel, DoD resources, and classified national security information…or controlled unclassified information…" These are relatively vague terms, but then 6.2.3 proceeds to list several explicit counterintelligence circumstances in which contacts must be reported. These include requests of people for unauthorized access to classified information; when contacts may indicate that DoD personnel may be targets for exploitation; contacts with intelligence officers from any country; contacts where information is received about terrorism, espionage, sabotage, subversion, or other intelligence activities; intrusions into U.S. automated information systems; contacts with foreign government interests that may be reportable under separate procedures (e.g., for attaches or arms control negotiators); and other situations where personnel hold sensitive positions and may be required to inform

[2] Pursuant to White House Memorandum, *Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies*, August 23, 1996 and ASD(C3I) Memorandum, *Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies*, October 15, 1996.

Page 2808 of 3957

their commanders of the nature of any intended contact with a foreign diplomatic establishment. For the full wording on the above items, please see Item 6.2, *Reporting Requirements*, on pp. 6-7 of the new instruction.

The new DoD Instruction 5240.6 is creative and forward-looking in that it sets out a specific and explicit set of CI behaviors that should be reported and then refers the reader to Enclosure 3 where a further set of behaviors is listed. Prompted by the CI Directorate's review of PERSEREC's draft CORE, this is the first time that such a list has been included in any such instruction.

DoD Instruction 5240.6, Enclosure 3, contains 14 items taken directly from PERSEREC's CORE list of 16 items. These are behaviors that are clear violations and must be reported immediately; no judgment is required of the person reporting. The CI Directorate added other items to Enclosure 3. These additions were the kinds of items that had initially been rejected by researchers at PERSEREC who recognized such items as potentially security-relevant but: (1) were open to different interpretations that might have little bearing on security, or (2) were behaviors that could not normally be known to a supervisor or coworker. These additional items, several borrowed from the Army's SAEDA list, included volunteering for assignments beyond the normal scope of responsibilities; use of copy machines, faxes or computers to transmit materials that may exceed job requirements; working outside normal duty hours; unexplained or undue affluence; sudden reversal of a bad financial situation or repayment of large debts; attempts to entice DoD personnel into situation that could place them in a compromising position; attempts to place DoD personnel under obligation through special treatment; and short trips to foreign countries or travel within the US for reasons that appear unusual or inconsistent with a person's interests or financial means. Counterintelligence Directorate staff included these items because they have been previously mentioned in policy and have thus traditionally been part of a set of behaviors of possible security concern.

Implementation of CORE Brochure in the Field

After PERSEREC's CORE list was included in policy, PERSEREC transformed it into a brochure for use in the field. The brochure is designed for distribution to DoD components and other departments and agencies that have a need for security education materials and educational tools in the area of supervisor and coworker reporting. It contains the rationale for creating the CORE list so that people using it in the field will understand why items are included. Reportable behaviors are then presented in three major categories: (1) recruitment, (2) information collection, and (3) information transmittal. A fourth section contains a number of discretionary items, i.e., behaviors that are worth noting if one observes them. This fourth section in the brochure is labeled Suspicious Behaviors and is included because the items have long been covered in policy. (Please see the PERSEREC brochure at Appendix B.)

Page 2809 of 3957

Recommendation

DoD should distribute the CORE brochure and its developmental rationale to CI and security agencies for possible implementation. Potential uses include security education briefings of various sorts (e.g., initial, refresher, and CI awareness) and distribution to cleared personnel. By concentrating on direct CI- and security-related behavior, personnel in the field are likely to develop a better understanding of exactly what to report and a greater commitment to reporting it.

Page 2810 of 3957

Page 2811 of 3957

References

Wood, S., & Marshall-Mies, J.C. (2003). *Improving supervisor and coworker reporting of information of security concern* (PERS-TR-02-3). Monterey, CA: Defense Personnel Security Research Center.

Page 2812 of 3957

Page 2813 of 3957

Appendix A

Department of Defense Instruction 5240.6 (August 7, 2004)

Page 2814 of 3957

Page 2815 of 3957

Department of Defense

INSTRUCTION

NUMBER 5240.6
August 7, 2004

USD(I)

SUBJECT: Counterintelligence (CI) Awareness, Briefing, and Reporting Programs

References: (a) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness and Briefing Program," July 16, 1996 (hereby canceled)
(b) Presidential Decision Directive/NSC No.12,[1] "Security Awareness and Reporting of Foreign Contacts," August 5, 1993
(c) DoD Directive 5240.2, "DoD Counterintelligence (CI)," May 22, 1997
(d) Executive Order 12829, "National Industrial Security Program," January 6, 1993
(e) through (y), see enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues reference (a), implements reference (b) within the Department of Defense (DoD), and establishes procedures for conducting and administering DoD counterintelligence awareness, briefings and reporting as required by reference (c).

1.2. Provides procedures for the handling of other threat information affecting the security of DoD personnel, information, resources, installations, and operations.

1.3. Reaffirms the requirement for a foreign intelligence and international terrorist threat awareness and briefing programs for DoD military, civilian employee, and contractor personnel.

[1] Authorized users may contact the CI Directorate, DUSD(CI&S), USD(I), Room 3C260, Pentagon for a copy.

Page 2816 of 3957

2. APPLICABILITY AND SCOPE

This Instruction applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. DoD contractor personnel with security clearances for their briefing and reporting requirements as specified under E.O. 12829 (reference (d)), (hereafter referred to collectively as "the DoD contractors").

2.3. Active and Reserve military personnel, DoD civilian employees, and DoD contractors (hereafter collectively referred to as "the DoD personnel").

3. DEFINITIONS

Definitions for this Instruction are in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. The DoD personnel report any contact information or circumstances that could pose a threat to the security of U.S. personnel, DoD or other U.S. resources, and classified national security information (hereafter referred to as "classified information"), or controlled unclassified information under E.O. 12958, DoD Directive 5230.24, DoD 5400.7-R, and DoD Directive 5210.83 (references (e) through (h)) to an appropriate authority. Judicial and/or administrative action may be taken when DoD personnel fail to report such required information.

4.2. The DoD personnel shall receive periodic briefings on the threats posed by foreign intelligence services, international terrorists, computer intruders and unauthorized disclosures, and individual reporting responsibilities. This shall include insider threats and the crimes of spying and treason.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)) shall oversee the DoD Counterintelligence (CI) awareness, briefing, and reporting programs and ensure:

5.1.1. The Deputy Under Secretary of Defense (Counterintelligence and Security) (DUSD(CI&S)) shall establish and sustain the DoD CI awareness, briefing, and reporting programs.

5.1.2. The Director, Counterintelligence, under the DUSD(CI&S), shall:

5.1.2.1. Recommend policy on CI awareness, briefing, and reporting programs to the DUSD(CI&S) and the USD(I).

5.1.2.2. Provide oversight to the DoD CI Program.

5.1.2.3. Participate in DoD and national-level forums concerning CI awareness, briefing, and reporting programs.

5.1.2.4. Serve as the staff point of contact within OSD for issues related to CI awareness, briefing, and reporting programs.

5.1.3. The Director, Counterintelligence Field Activity (CIFA), under the DUSD(CI&S), shall:

5.1.3.1. Manage and provide functional oversight of the Department's CI awareness, briefing, and reporting programs.

5.1.3.2. Brief the USD(I) on significant CI investigative referrals received pursuant to this Instruction in accordance with DoD Directive 5105.67 (reference (i)).

5.1.3.3. Recommend policy changes through the DUSD(CI&S) to the USD(I).

5.1.3.4. Provide additional training to Component CI personnel on the skills required for the CI awareness, briefing, and reporting programs.

5.1.3.5. Represent the Department with other Government and management agencies regarding implementation of all DoD CI matters pursuant to reference (i).

5.1.4. The Director, Defense Security Service, under the DUSD(CI&S), shall recommend changes to DoD 5220.22-M (reference (j)) to the DUSD(CI&S), to implement this Instruction within cleared defense contractor facilities.

5.2. The Heads of the DoD Components shall:

5.2.1. Develop and implement CI briefing, awareness, and reporting programs within their organizations.

5.2.2. Promptly report any CI information developed from these programs to their organic or lead CI agency and to the CIFA pursuant to USD(I) Memorandum, "Reporting Significant Counterintelligence Activity," July 19, 2003 (reference (k)).

5.2.3. Establish time-sensitive reporting procedures pursuant to paragraph 6.3., below, for the DoD personnel during official or non-official overseas travel.

5.2.4. Ensure Component CI agencies report CI information through the Portico system.

5.2.5. Ensure Component CI agency CI information is appropriately documented in the Portico system. Information collected responsive to validated collection requirements shall be published via Intelligence Information Report on the Portico system.

5.3. The Director, Defense Intelligence Agency, shall, in addition to the responsibilities listed in paragraph 5.2., above, and in coordination with the Director, Joint Staff, develop and implement CI awareness, briefing, and reporting programs for the Chairman, Joint Chiefs of Staff.

5.4. Defense Agencies with organic CI organizations shall:

5.4.1. Ensure reported information regarding contractor personnel is referred to the Defense Security Service (DSS) and the Federal Bureau of Investigation (FBI).

5.4.2. Ensure reported information regarding military or DoD civilian personnel is referred to the appropriate Military Department CI agency or the FBI, as appropriate. Any information reported to the FBI shall also be reported to the CIFA pursuant to DoD Instruction 5240.4 (reference (l)).

5.5. The Secretaries of the Military Departments shall:

5.5.1. Ensure Department CI agencies refer reported information regarding contractor personnel to the DSS and the FBI.

5.5.2. Refer reported information regarding DoD civilian employees to the FBI for possible CI investigative or operational action where the Department does not otherwise have investigative authority. Any information reported to the FBI shall also be reported to the CIFA pursuant to reference (l).

6. PROCEDURES

6.1. Awareness and Briefing Programs

6.1.1. The DoD awareness and briefing programs shall promote threat and reporting awareness responsibility, enable DoD personnel to identify CI threats, and the reporting of suspicious situations and incidents to appropriate authorities.

6.1.2. Threat awareness may be enhanced through a variety of methods, including but not limited to publications, posters, live presentations, and recorded media.

6.1.3. CI Briefings shall include:

6.1.3.1. Information about early detection of espionage and other suspected foreign intelligence and international terrorist activities to include the crimes of sabotage, subversion, treason, and spying.

6.1.3.2. Comprehensive, tailored threat information focusing on foreign intelligence, international terrorism, and other threats to include insider threats relevant to the DoD Component's mission, functions, activities and locations.

6.1.3.3. Information addressing the DoD anomalies program pursuant to White House Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," August 23, 1996 and Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," October 15, 1996 (references (m) and (n)), which remain in effect.

6.1.4. Briefings shall be presented at or near the time of initial entry or hire and thereafter at least every 12 months. More frequent briefing intervals should be instituted if conditions warrant. Some DoD Component organizations or personnel may require more frequent briefings predicated on the nature of their duties.

6.1.5. Briefings should be presented by the Component CI agency when feasible. If the servicing Component CI agency is not used, the briefings should be coordinated with them for content and accuracy.

6.1.6. Briefings conducted pursuant to this Instruction do not satisfy the requirement of DoD Directive 2000.12 (reference (o)).

6.2. Reporting Requirements

6.2.1. The DoD personnel shall report information pursuant to E.O. 12968 and DoD 5200.2-R (references (p) and (q)) concerning security violations and other

information with potentially serious security significance regarding someone with access to classified information or who is employed in a sensitive position. Examples of information or observed behaviors that should be reported are listed in enclosure 3.

6.2.2. Pursuant to this Instruction, the DoD personnel shall expeditiously report any contacts or circumstances that could pose a threat to the security of U.S. personnel, DoD resources, and classified national security information or controlled unclassified information to an appropriate DoD authority.

6.2.2.1. Appropriate authorities for active duty and Reserve military personnel and DoD civilians and DoD contractors working in DoD Component facilities include security officers, supervisors, commanders, and organic or lead CI agencies. Security officers, supervisors, and commanders shall expeditiously refer any information they receive pursuant to this Instruction to their supporting CI agency.

6.2.2.2. Appropriate authorities for DoD contractors at cleared contractor facilities shall include Facility Security Officers, Military Department CI Agencies, the FBI, or the DSS pursuant to reference (l).

6.2.3. The DoD personnel shall report contacts pursuant to the following situations:

6.2.3.1. A request by anyone, regardless of nationality, for unauthorized access to classified information under DoD 5200.1-R (reference (r)); controlled unclassified information under references (f), (g), and DoD Directive 5230.25 (reference (s)); or information systems containing such information.

6.2.3.2. Contact with an individual, regardless of nationality, under circumstances that suggest the DoD personnel may be the target of an attempted exploitation by a foreign intelligence service or international terrorist organization.

6.2.3.3. Contact with a known or suspected intelligence officer from any country.

6.2.3.4. Contact with anyone receiving information of planned, attempted, actual, or suspected international terrorism, espionage, sabotage, subversion, or other intelligence activities against the Department of Defense, other U.S. facilities, U.S. organizations, or U.S. citizens.

6.2.3.5. Actual or attempted unauthorized access into U.S. automated information systems and/or unauthorized transmissions of classified or controlled unclassified information over on-line computer services and telephones.

6.2.3.6. Close and continuing associations with foreign nationals may also be reportable under Director of Central Intelligence Directive (DCID) 6/1, reference (t) and DCID 6/4, reference (u).

6.2.3.7. In addition to the aforementioned reporting requirements, personnel who occupy positions designated by their DoD Component as sensitive shall apprise their commanders or supervisors of the nature and purpose of any intended contact with any foreign diplomatic establishment whether in the United States or abroad.

6.3. Sanctions. The DoD personnel who fail to report information required by this Instruction may be subject to judicial and/or administrative action under applicable law and regulations, including the Uniform Code of Military Justice (reference (v)), and other applicable sections of the United States Code.

6.4. Other

6.4.1. DoD acquisition program personnel working with Critical Program Information pursuant to DoD Directive 5200.39 (reference (w)) shall notify their servicing security personnel of all projected foreign travel. Such personnel shall receive foreign intelligence threat briefings and anti-terrorism briefings prior to overseas travel.

6.4.2. The DoD personnel with access to Sensitive Compartmented Information (SCI) pursuant to DCID 1/20 (reference (x)) incur special security obligations that include advance foreign travel notification for official and/or unofficial travel and defensive travel briefings.

7. EFFECTIVE DATE

This Instruction is effective immediately.

Stephen A. Cambone
Under Secretary of Defense for Intelligence

Enclosures - 3
- E1. References, continued
- E2. Definitions
- E3. Examples of Reportable Employee Behaviors

E1. ENCLOSURE 1

REFERENCES, continued

(e) Executive Order 12958, "Classified National Security Information," April 17, 1995
(f) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
(g) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
(h) DoD Directive 5210.83, "Department of Defense Unclassified Nuclear Information (DoD UCNI)," November 15, 1991
(i) DoD Directive 5105.67, "Department of Defense Counterintelligence Field Activity (DoD CIFA)," February 19, 2002
(j) DoD 5220.22-M, "National Industrial Security Program Operating Manual," January 1999
(k) Under Secretary of Defense (Intelligence) Memorandum, "Reporting Significant Counterintelligence Activity," July 19, 2003
(l) DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," September 22, 1992
(m) White House Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," August 23, 1996[2]
(n) Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," October 15, 1996[3]
(o) DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003
(p) Executive Order 12968, "Access to Classified Information," August 2, 1987
(q) DoD 5200.2-R, "Personnel Security Program," January 1987
(r) DoD 5200.1-R, "DoD Information Security Program," January 16, 1997
(s) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984
(t) Director of Central Intelligence Directive 6/1, "Security Policy for Sensitive Compartmented Information and Security Policy Manual," March 1, 1995[4]
(u) Director of Central Intelligence Directive 6/4, "Personnel Security Standards," July 2, 1998[5]
(v) Section 801-940, Chapter 47, of title 10, United States Code, "Uniform Code of Military Justice"
(w) DoD Directive 5200.39, "Security, Intelligence and Counterintelligence Support to Acquisition Program Protection," September 10, 1997

---

[2] Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.
[3] Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.
[4] Available to authorized users via DoD Secure Internet Protocol Route Network (SIPRNET).
[5] Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.

(x) Director of Central Intelligence Directive 1/20, "Security Policy Concerning Travel and Assignment of Personnel With Access to Sensitive Compartmented Information (SCI)," December 29, 1991[6]

(y) Sections 792-799, Chapter 37 of title 18, United States Code

[6] Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.

E2. ENCLOSURE 2

DEFINITIONS

E2.1. DEFINED TERMS

E2.1.1. Anomalies. Foreign power activity or knowledge suggesting foreign knowledge of U.S. national security information, processes or capabilities.

E2.1.2. Classified Information. Information requiring protection in the interest of national security, classified "TOP SECRET, SECRET, or CONFIDENTIAL" according to reference (x).

E2.1.3. Contact. Any form of meeting, association, or communication in person; by radio, telephone, letter, computer; or other means, regardless of who initiated the contact for social, official, private, or other reasons.

E2.1.4. Controlled Unclassified Information. Data bearing distribution limitation statements such as "For Official Use Only" in accordance with reference (g) and other information marked under references (f) and (g).

E2.1.5. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

E2.1.6. Counterintelligence Investigations. Are conducted to prove or disprove an allegation of espionage or other intelligence activities, such as sabotage, assassination, or other national security crimes conducted by or on behalf of a foreign government, organization, or person or international terrorists. CI investigations may establish the elements of proof for prosecution or administrative actions, provide a basis for CI operations, or validate the suitability of personnel for access to classified information. CI investigations are conducted against individuals or groups for committing major security violations, as well as failure to follow Defense Agency and Military Department directives governing reporting contacts with foreign citizens and out-of-channel requests for defense information. CI investigations provide military commanders and policymakers with information used to eliminate security vulnerabilities and otherwise improve the security posture of threatened interests.

E2.1.7. Defensive Travel Briefings. Formal advisories alerting personnel of the potential for harassment, exploitation, provocation, capture, or entrapment while traveling. These briefings, based on actual experience when available, include

information on courses of action helpful in mitigating adverse security and personnel consequences and advise of passive and active measures that personnel should take to avoid becoming targets or inadvertent victims as a consequence of hazardous travel.

E2.1.8. DoD Component CI Organizations. The organic CI elements of the Army, the Navy, the Air Force, the Marine Corps, the Joint Staff, the Combatant Command Staffs, the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the Defense Security Service, the Defense Threat Reduction Agency, and the Missile Defense Agency and the CIFA.

E2.1.9. Espionage. Defined under Sections 792-799, Chapter 37, title 18, United States Code (reference (y)) and Article 106a, Uniform Code of Military Justice (UCMJ) (reference (v)).

E2.1.9.1. Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies during war or peace.

E2.1.9.2. Reference (y) makes it an offense to gather, with the requisite intent or belief, national defense information, by going on, entering, flying over, or obtaining access by any means to any installation or place used by the United States for national defense. The method of gathering that information is immaterial.

E2.1.9.3. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense, which he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it may be punished under reference (y).

E2.1.9.4. Anyone entrusted with or having lawful possession or control of information about national defense, who through gross negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of that trust may be punished under reference (y).

E2.1.9.5. If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of reference (y).

E2.1.10. Foreign Diplomatic Establishment. Any embassy, consulate, or interest section representing a foreign country.

E2.1.11. Lead CI Agency. A Military Department CI Agency that has been designated by the USD(I) to provide defined levels of CI support to one or more of the DoD Components.

E2.1.12. Military Department CI Agencies. The Military Department CI Agencies include the U.S. Army Counterintelligence, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

E2.1.13. National Security. A collective term encompassing both national defense and foreign relations of the United States.

E2.1.14. Portico. A program managed by the CIFA to provide automation support, through web-enabled software hosted on a robust infrastructure, to the DoD CI Community. Portico enables CI enterprise business processes; facilitates information sharing, and coordination across DoD Services and Agencies; and provides management tools for each CI functional area, as well as supporting tools and services for managing the CI process in the functional areas of Collection; Investigations; Analysis and Production; Operations; and CI Functional Services.

E2.1.15. Sabotage. An act or acts with the intent to injure or interfere with, or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises or utilities to include human or natural resources, under reference (y).

E2.1.16. Spying. During wartime, any person who is found lurking as a spy or acting as a spy in or about any place, vessel or aircraft, within the control or jurisdiction of any of the Armed Forces or in or about any shipyard, any manufacturing or industrial plant, or any other place or institution engaged in work in aid of the prosecution of the war by the United States, or elsewhere.

E2.1.17. Subversion. An act or acts inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, of discipline, of the Military Forces of the United States.

E2.1.18. Terrorism. The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

E2.1.19. Treason. Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason (see Section 2831 of title 18, U.S. Code, reference (y)).

E2.1.20. Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

E3. ENCLOSURE 3

EXAMPLES OF REPORTABLE EMPLOYEE BEHAVIORS

E3.1. LIST OF REPORTABLE EMPLOYEE BEHAVIORS

E3.1.1. Unauthorized contact with an individual who is known or suspected of being associated with a foreign intelligence, security, or terrorist organization.

E3.1.2. Illegal activity, conduct or requests for participation in illegal activities or other conduct that might make someone susceptible to blackmail or result in a security violation.

E3.1.3. Reading or discussing classified or controlled unclassified information in an unauthorized location, such as while using public transportation.

E3.1.4. Attempts to obtain classified or other protected information in any format to which the requesting person does not have authorized access.

E3.1.5. Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.

E3.1.6. Unauthorized possession and/or operation of cameras, recording devices, computers, or modems in areas wherein classified information and data are stored, discussed, or processed.

E3.1.7. The existence or use of any unauthorized listening or surveillance devices in sensitive or secure areas.

E3.1.8. Keeping classified material at home or any other unauthorized place.

E3.1.9. Acquiring access to classified or unclassified automated information systems without proper authorization.

E3.1.10. Transmitting classified material over unclassified FAX or computer.

E3.1.11. Seeking to obtain access to sensitive information inconsistent with present duty requirements.

E3.1.12. Removing classified or controlled unclassified material from work areas without appropriate authorization by any means.

E3.1.13. Improperly removing security classification markings from documents.

E3.1.14. Discussing classified information on a non-secure, unencrypted telephone.

E3.1.15. Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities.

E3.1.16. Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified material that may exceed job requirements.

E3.1.17. Repeated or un-required work outside of normal duty hours, especially unaccompanied.

E3.1.18. Unexplained or undue affluence, including sudden purchases of high value items (i.e., real estate, stocks, vehicles, or vacations) where no logical income source exists. Attempts to explain wealth by reference to inheritance, luck in gambling, or some successful business venture.

E3.1.19. Sudden reversal of a bad financial situation or repayment of large debts.

E3.1.20. Attempts to entice DoD personnel into situations that could place them in a compromising position.

E3.1.21. Attempts to place DoD personnel under obligation through special treatment, favors, gifts, money or other means.

E3.1.22. Short trips to foreign countries or travel within the United States to cities with foreign diplomatic activities for reasons that appear unusual or inconsistent with a person's interests or financial means.

Page 2831 of 3957

Appendix B

COUNTERINTELLIGENCE REPORTING ESSENTIALS (CORE)

A Practical Guide for Reporting Counterintelligence and Security Indicators

Page 2832 of 3957

Page 2833 of 3957

COUNTERINTELLIGENCE REPORTING ESSENTIALS (CORE)

A Practical Guide for Reporting Counterintelligence and Security Indicators

Defense Personnel Security Research Center (PERSEREC)

Page 2834 of 3957

INTRODUCTION

Supervisors and coworkers are the first line of defense against espionage. The government relies on you to protect national security by reporting any behavior that you observe that may be related to a potential compromise of classified information. You are encouraged, sometimes obliged, by Executive Order, Presidential Decision Directive and U.S. Code, as well as by DoD Directives, Regulations, Instructions, to report such behaviors. However, judgment calls are often required by the potential reporter, and this often leads to indecision or choosing not to report anything.

Therefore, presented below is a focused list of serious counterintelligence- and security-related behaviors that, if observed or learned about, should be reported immediately to appropriate counterintelligence or security authorities. All these behaviors are serious and require little or no speculation.

Upon receiving your report, a security professional will follow up with appropriate verification. If you are at all uncertain, it is better to err on the side of reporting than not. The counterintelligence and security people will know how to handle your report.

The list of behaviors is not intended to be exhaustive. You should report any additional observed behaviors that may parallel or exceed the concerns listed in this brochure.

The brochure can be used by supervisors, coworkers, and security professionals in initial and refresher briefings and in counterintelligence briefings. By concentrating on direct counterintelligence- and security-related behavior, personnel in the field are likely to develop a better understanding of exactly what to report and a greater commitment to reporting it.

If you want only the CORE items,
print the last four pages of this document.

Page 2835 of 3957

BACKGROUND

The Defense Personnel Security Research Center (PERSEREC) conducted research on how employees with clearance access understand the requirements to report suspicious behavior that they observe.*

Finding: Supervisors and coworkers are willing to report on behaviors that have a clear connection to security, such as transmitting classified documents to unauthorized personnel, but they are unwilling to report on colleagues' personal problems, such as alcohol abuse. Because it was difficult to discern which reporting requirements were clearly related to security, there was very little reporting.

Outcome: PERSEREC, in collaboration with counterintelligence professionals, developed a clear, succinct list of "Coworker Reporting Essentials" (CORE) behaviors that could pose a possible threat to national security and thus should be reported if observed. The draft CORE was reviewed and edited by counterintelligence professionals at the Counterintelligence Field Activity (CIFA), and was coordinated by the DoD Investigative Working Group (IWG).

PERSEREC also coordinated with the DoD Counterintelligence Directorate in the Office of the Under Secretary for Defense (Intelligence), who included the PERSEREC CORE list in DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs.*

*Wood, S., & Marshall-Mies, J.C. (2003). Improving supervisor and coworker reporting of information of security concern. Monterey, CA: Defense Personnel Security Research Center.

Page 2836 of 3957

COUNTERINTELLIGENCE REPORTING ESSENTIALS (CORE)

If you become aware of any of the following behaviors or activities, you should report them to your security officer or supervisor. These behaviors are derived from the DoD Instruction 5240.6 *Counterintelligence Awareness, Briefing, and Reporting Programs.*

RECRUITMENT

Foreign intelligence entities are on the lookout for people who can be solicited to commit espionage against the U.S. At the same time, willing would-be spies often approach foreign intelligence operatives on their own initiative, thus volunteering for recruitment. It is a major task of counterintelligence to intercept these relationships. The recruitment cycle requires, first, that contact be established between the foreign intelligence agency and the potential spy, whether by direct recruitment or by volunteering. While the recruitment relationship almost always involves contacts with foreigners, an already-committed U.S. spy may approach you or a colleague on the job for recruitment into espionage.

Reportable Behaviors

- you become aware of a colleague having contact with an individual who is known to be, or is suspected of being, associated with a foreign intelligence, security, or terrorist organization.

- you discover that a colleague has not reported an offer of financial assistance by a foreign national other than close family.

- you find out that a colleague has failed to report a request for classified or unclassified information outside official channels to a foreign national or anyone without authorization or need to know.

- you become aware of a colleague engaging in illegal activity or if a colleague asks you to engage in any illegal activity.

Page 2837 of 3957

INFORMATION COLLECTION

Before classified or other kinds of sensitive materials can be passed to a foreign intelligence agency, they must be collected. They can simply be stolen (e.g., paper placed in a briefcase and taken out of the office), photographed, collected via computers, or obtained through eavesdropping or other surveillance devices. The computer age, with its e-mail and database capabilities, has offered new opportunities to potential spies for collecting data. While technical countermeasures can control some situations, it is up to coworkers to watch for and, if possible, identify breaches in the system that allow classified and sensitive information to be collected for espionage purposes.

Reportable Behaviors

- . . a colleague asks you to obtain classified or other protected information in any format to which the person does not have authorized access.

- . . a colleague asks you to witness signatures for destruction of classified information when you did not observe the destruction.

- . . you observe a colleague operating unauthorized cameras, recording devices, computers, or modems in areas where classified data are stored, discussed, or processed.

- . . you become aware of the existence of any listening or surveillance devices in sensitive or secure areas.

- . . you find out that a colleagues has been keeping classified material at home or any other unauthorized place.

- . . you discover a colleague acquiring access to classified or unclassified automated information systems without authorization.

- . . you observe a colleague seeking to obtain access to sensitive information inconsistent with present duty requirements.

Page 2838 of 3957

INFORMATION TRANSMITTAL

In former days the transmittal of classified or sensitive information took the form of stealing documents and physically handing them to the foreign intelligence agent. In addition, spies could photocopy paper materials, smuggle materials out in briefcases, even illicitly take photographs in the workplace. Nowadays, there are many more opportunities to transmit information. With the advent of e-mail, faxes, and other technological capabilities, it is possible to transmit large quantities of information without being immediately caught. Coworkers must be aware of this problem and, if an illicit transmission is detected, report it directly and immediately to the designated cognizant counterintelligence or security authorities.

Once a relationship with a foreign intelligence agent is established and information begins to flow, illicit trips abroad by the recruited spy usually follow (meetings are easier to arrange abroad than in the U.S.). These journeys are often concealed by the person and the foreign contact is not reported. If you learn of such journeys or contacts, you should report.

Reportable Behaviors

- you see someone removing classified material from the work area without appropriate authorization, either by physically taking it home or on travel, or by e-mailing or faxing it out of the office. The same rule applies for other protected materials, such as export-controlled or proprietary items.

- you observe a colleague using unclassified FAX or computer to transmit classified material.

- you observe a person improperly removing the classification markings from documents.

- you hear a colleague discussing classified information on a nonsecure telephone.

- you become aware that people with TS/SCI or contractors with a reporting requirement have attempted to conceal any work-related foreign travel and any personal foreign travel.

Page 2839 of 3957

SUSPICIOUS BEHAVIORS

The new DoD Instruction 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs* (August 7, 2004) lists an additional series of eight items that, while not exactly clear-cut violations, have been traditionally considered behaviors that may well be connected to counterintelligence and security problems. These behaviors do require some degree of judgment before reporting. Often you might not know about them directly but only by hearsay. Often they may easily carry plausible alternative explanations. They are included here with the caveat that they do require a judgment call before reporting. If you are at all uncertain, it is better to report the behavior than to make no report at all.

> Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities.

> Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified material that may exceed job requirements.

> Repeated or un-required work outside of normal duty hours, especially unaccompanied.

> Unexplained or undue affluence, including sudden purchases of high value items (e.g., real estate, stocks, vehicles, or vacations) where no logical income source exists. Attempt to explain wealth by reference to inheritance, luck in gambling, or some successful business venture.

> Sudden reversal of financial situation or sudden repayment of large debts or loans.

>Attempts to entice DoD personnel into situations that could place them in a compromising position.

> Attempts to place DoD personnel under obligation through special treatment, favors, gifts, money, or other means.

>Short trips to foreign countries or travel within the United States to cities with foreign diplomatic activities for reasons that appear unusual or inconsistent with a person's interests or financial means.

Page 2840 of 3957

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

UNDERSTANDING THE ROLE OF OVERT AND COVERT ONLINE COMMUNICATION IN INFORMATION OPERATIONS

by

Boyan I. Dimitrov

March 2022

Thesis Advisor: Timothy C. Warren
Second Reader: Shannon C. Houck

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
UNDERSTANDING THE ROLE OF OVERT AND COVERT ONLINE COMMUNICATION IN INFORMATION OPERATIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Boyan I. Dimitrov

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This thesis combines regression, sentiment, and social network analysis to explore how Russian online media agencies, both overt and covert, affect online communication on Twitter when North Atlantic Treaty Organization (NATO) exercises occur. It explores the relations between the average sentiment of tweets and the activities of Russia's overt and covert online media agencies. The data source for this research is the Naval Postgraduate School's licensed Twitter archive and open-source information about the NATO exercises timeline. Publicly available lexicons of positive and negative terms helped to measure the sentiment in tweets. The thesis finds that Russia's covert media agencies, such as the Internet Research Agency, have a great impact on and likelihood for changing the sentiment of network users about NATO than do the overt Russian media outlets. The sentiment during NATO exercises becomes more negative as the activity of Russian media organizations, whether covert or overt, increases. These conclusions suggest that close tracking and examination of the activities of Russia's online media agencies provide the necessary base for detecting ongoing information operations. Further refining of the analytical methods can deliver a more comprehensive outcome. These refinements could employ machine learning or natural language processing algorithms that can increase the precision of the sentiment measurement probability and timely identification of trolls' accounts.

14. SUBJECT TERMS
information operations, social media, Russian media outlets, Russia's covert online activity, IRA, Internet Research Agency, sentiment analysis, Twitter

15. NUMBER OF PAGES
79

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Page 2843 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2844 of 3957

Approved for public release. Distribution is unlimited.

UNDERSTANDING THE ROLE OF OVERT AND COVERT ONLINE COMMUNICATION IN INFORMATION OPERATIONS

Boyan I. Dimitrov
Podpolkovnik, Bulgarian Air Force
Master of Radio and Television Engineering , Air Force Academy, Bulgaria, 1999
MIB, "St. Cyril and St. Methodius" University of Veliko Tarnovo, Bulgaria, 2011

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2022

Approved by: Timothy C. Warren
Advisor

Shannon C. Houck
Second Reader

Carter Malkasian
Chair, Department of Defense Analysis

Page 2845 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2846 of 3957

ABSTRACT

This thesis combines regression, sentiment, and social network analysis to explore how Russian online media agencies, both overt and covert, affect online communication on Twitter when North Atlantic Treaty Organization (NATO) exercises occur. It explores the relations between the average sentiment of tweets and the activities of Russia's overt and covert online media agencies. The data source for this research is the Naval Postgraduate School's licensed Twitter archive and open-source information about the NATO exercises timeline. Publicly available lexicons of positive and negative terms helped to measure the sentiment in tweets. The thesis finds that Russia's covert media agencies, such as the Internet Research Agency, have a great impact on and likelihood for changing the sentiment of network users about NATO than do the overt Russian media outlets. The sentiment during NATO exercises becomes more negative as the activity of Russian media organizations, whether covert or overt, increases. These conclusions suggest that close tracking and examination of the activities of Russia's online media agencies provide the necessary base for detecting ongoing information operations. Further refining of the analytical methods can deliver a more comprehensive outcome. These refinements could employ machine learning or natural language processing algorithms that can increase the precision of the sentiment measurement probability and timely identification of trolls' accounts.

Page 2847 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2848 of 3957

TABLE OF CONTENTS

I. INTRODUCTION....1

II. LITERATURE REVIEW....5
- A. INFORMATION OPERATIONS AND SOCIAL MEDIA....5
- B. METHODS OF STUDYING INFORMATION OPERATIONS....11

III. INFORMATION WARFARE: THE BEAR AND THE DRAGON....15
- A. INFORMATION CONFRONTATION, INFORMATION WARFARE, AND INFORMATION OPERATIONS....15
- B. SOCIAL MEDIA IN INFORMATION WARFARE....20

IV. RESEARCH METHODS....29
- A. HYPOTHESES....29
- B. DATA AND METHODS....29
  - 1. Datasets....29
  - 2. Sentiment Analysis and Text Processing of Social Media Data....30
  - 3. Network Topography Measures....31
  - 4. Dependent Variables....31
  - 5. Independent Variables....32
  - 6. Control Variables....33
- C. REGRESSION ANALYSIS....34

V. REGRESSION RESULTS....35
- A. RUSSIAN ONLINE INFLUENCE ON SOCIAL MEDIA SENTIMENT....35
  - 1. Findings....35
  - 2. Analysis of the Findings....38
- B. NETWORK MEASURES AND RUSSIAN ONLINE INFLUENCE....42
  - 1. Analysis of the Findings....44
- C. DISCUSSION....46

VI. CONCLUSIONS....51

LIST OF REFERENCES....55

Page 2849 of 3957

INITIAL DISTRIBUTION LIST 61

Page 2850 of 3957

LIST OF FIGURES

Figure 1. IRA and Russian Media Tweets vs. Sentiment in the NATO Conversation 39

Figure 2. Substantive Effects of IRA and Russian Media Tweets on the Probability of Positive and Negative Sentiment 40

Figure 3. NATO Exercises and IRA Tweets vs. Probability of Positive Sentiment 41

Figure 4. NATO Exercises and Distance to Russia vs. Probability of Positive Sentiment 42

Figure 5. NATO Exercises and IRA Tweets vs. Network Size 44

Figure 6. NATO Exercises, IRA Tweets, and Russian Media Tweets vs. Degree Centralization 45

Figure 7. NATO Exercises, IRA Tweets, and Russian Media Tweets vs. Clustering Coefficient 46

Figure 8. Russian Military Exercises and Distance to Russia vs. Probability of Positive Sentiment 49

Page 2851 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Sentiment Regression Models: Goodness of Fit 35

Table 2. Sentiment Regression Models: Base Terms 36

Table 3. Sentiment Regression Models: Multiplicative Interaction Terms 38

Table 4. Network Regression Models 43

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2854 of 3957

LIST OF ACRONYMS AND ABBREVIATIONS

AIC	Akaike's Information Criteria
BIC	Bayesian Information Criteria
BLM	Black Lives Matter
GDP	Gross Domestic Product
IO	Information Operation
IRA	Internet Research Agency
IRC	Information-Related Capabilities
LDA	Latent Dirichlet Allocation
MAE	Mean Absolute Error
MoDRF	Ministry of Defence of the Russian Federation
NATO	North Atlantic Treaty Organization
NPS	Naval Postgraduate School
ORA	Organizational Risk Analyzer
RMSE	Root Mean Squared Error

Page 2855 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2856 of 3957

ACKNOWLEDGMENTS

This thesis would not be possible without the tireless work of the teachers and instructors from the Defense Analysis Department of the Naval Postgraduate School. I am particularly grateful to my advisors Professor T. Camber Warren and Professor Shannon Houck, for their dedication and patience during my research. In addition, I am also thankful to the people in the International Graduate Program Office for the exceptional support that they provide for the international students.

Page 2857 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2858 of 3957

I. INTRODUCTION

In recent years, social media has become significantly important as a source of information and means of communication. Many people worldwide have an account on at least one social media platform. Such platforms created a new environment, which enormously simplified exchanging ideas, messages, and knowledge. However, it also becomes a channel for manipulation, deception, and proliferation of extremist and radical ideologies. The popularity of such online services creates opportunities for state and non-state actors to manipulate a society's values and beliefs. The online media platforms become both a target and source of information campaigns to manipulate public perception. Governments worldwide work actively to develop online capabilities for influence to strengthen their power and accomplish their political agendas. Examples of such influence are the Russian government's online campaign against Ukraine in 2014[1] and campaigns by ISIS[2] and the Taliban[3] using social media to communicate their messages to target audiences.

These examples also demonstrate that the main actors in information operations operate overtly or covertly when influencing the targeted audiences. Official media agencies or journalists known for their affiliation to such outlets can openly deliver part of the narratives in such operations. However, this affiliation can affect their credibility and diminish the effects of the information operation. In contrast, media organizations that use covert methods can avoid being attributed to the source of the campaign, primarily by using fake online accounts. Therefore, they can infiltrate different communities to affect their online communication. Most importantly, they do not just push narratives that are in line

[1] Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (October 2017): 8–11, https://doi.org/10.1177/0163443716686672; Yevgeniy Golovchenko, Mareike Hartmann, and Rebecca Adler-Nissen, "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation," *International Affairs* 94, no. 5 (September 1, 2018): 2, https://doi.org/10.1093/ia/iiy148.

[2] Imran Awan, "Cyber-Extremism: Isis and the Power of Social Media," *Society* 54, no. 2 (April 2017): 5, https://doi.org/10.1007/s12115-017-0114-0.

[3] Vincent Bernatis, "The Taliban and Twitter: Tactical Reporting and Strategic Messaging," *Perspectives on Terrorism* 8, no. 6 (2014): 6, http://www.jstor.org/stable/26297291.

Page 2859 of 3957

with the official position of their state or organization. They can employ more aggressive methods and deliberately disseminate misleading, false, or divisive information to create in the targeted society disorientation and social confrontation. Consequently, both overt and covert media organizations significantly contribute to the overall effect of information operations. Their role in such activities needs exploring and constant monitoring to employ proper countermeasures. National security agencies need to develop the capacity to counter such online information campaigns. Successful and efficient counteraction depends on the reliable identification of the sources of information attacks, their target audiences, and their strategic messages.

However, researchers usually employ a single analytical method when exploring online information operations. For example, some of the most common methods include temporal analysis, data mining, or social network analysis.[4] This lack of an integrated approach delivers only partial results about the overall picture in the information campaign and prevents proper countermeasure planning. Thus, this thesis demonstrates that combining statistical analysis, social network analytic tools, text mining, and sentiment analysis can improve this approach. It shows that these methods provide the necessary results to build models that can explore the role of the different actors in information operations. This thesis's more comprehensive approach can increase the probability of timely identification of ongoing information operations, their audiences, main actors' probable location(s), and contribution to the overall effect of the operation. This research has great potential for improvement by adding new methods to the analysis. For example, machine learning algorithms can increase the precision of sentiment measurement. Additionally, dynamic network analysis and natural language processing can identify the most important topics in the online conversation and who contributes to these topics.

This thesis focuses on the online conversation on Twitter about the North Atlantic Treaty Organization (NATO), by examining the effects of military exercises over the

[4] Kai Shu et al., *Fake News Detection on Social Media: A Data Mining Perspective*, vol. 19, 2017, https://arxiv.org/pdf/1708.01967.pdf; Xinyi Zhou et al., "Fake News: Fundamental Theories, Detection Strategies and Challenges," in *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining* (WSDM '19: The Twelfth ACM International Conference on Web Search and Data Mining, Melbourne VIC Australia: ACM, 2019), 836–37, https://doi.org/10.1145/3289600.3291382.

2013–2014 time period. It explores the relations between the average sentiment of messages in this online conversation and the activities of Russia's overt and covert online media agencies. The thesis's most important findings are that the messages generated by Russia's covert agencies have a more substantial impact on the probability of sentiment change than those of the overt Russian media. Furthermore, the study finds that both the overt and the covert Russian actors more effectively influence positive rather than negative sentiments. Nevertheless, the evidence also shows that sentiment during NATO exercises becomes more negative as the activity of Russian covert media organizations increases. Furthermore, this thesis finds that during NATO exercises the trend toward negative sentiments increases if the sender's location is closer to the borders of the Russian Federation. Finally, this study also finds that activity by the Internet Research Agency (IRA), a covert Russian social media influencer agency, and Russian media during NATO exercises increases the daily network size of users engaged in the NATO conversation, and this network becomes more interconnected. When NATO exercises occur, Russian media activities tend to increase the centralization of the daily network. By contrast, the IRA seems to operate as a more "egalitarian" network of small teams with a similar number of ties.

Page 2861 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2862 of 3957

II. LITERATURE REVIEW

A. INFORMATION OPERATIONS AND SOCIAL MEDIA

The major actors on the international political stage, such as the United States, Russia, and China, have similar views about confrontation that unfolds in the form of information. Whether they define it as an information operation or information warfare, its primary goals are to influence the adversary's political and military leadership's decision-making process, reduce the enemy's morale, and tarnish the population's confidence in its leaders and institution. All three countries acknowledge that this type of confrontation has multidimensional characteristics because it targets physical, informational, and cognitive aspects of the information environment. The Joint Chiefs of Staff's JP3-13 provides details the U.S. concept of information operations,[5] while I. N. Panarin presents the Russian view and provides that country's definitions for information warfare (*Russ. informacionnoe protivoborstvo*) and its primary goals.[6] In turn, Paul Charon and Jean-Baptist Jeangène Vilmer[7] provide extensive details about China's concept of information operations, examine multiple case studies, and explain how Beijing studies and exploits the lessons learned from the Russian and U.S. military campaigns. In addition to the work of Charon and Jeangène Vilmer, Nathan Beauchamp-Mustafaga and Michael Chase[8] and Elsa Kania[9] can provide complementary insight into the Chinese concept of "the Three Warfares"—psychological warfare, public opinion warfare, and legal warfare.

---

[5] The Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, JP 3-13 (Washington, DC: Joint Chief of Staff, 2012), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

[6] I. N. Panarin, *Informatsionnaia Voina i Geopolitika*, [Information Warfare and Geopolitics] Velikii Put′ (Moskva: Pokolenie, 2006).

[7] Paul Charon and Jean-Baptist Jeangène Vilmer, *Chinese Influence Operations: A Machiavellian Moment* (Paris, France: Ministry for the Armed Forces, Institute for Strategic Research, 2021), https://www.irsem.fr/report.html.

[8] Nathan Beauchamp-Mustafaga and Michael S. Chase, *Borrowing a Boat Out to Sea: The Chinese Military's Use of Social Media for Influence Operations*, Policy Papers (Washington, DC: Johns Hopkins University School of Advanced International Studies, 2019).

[9] Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief* 16, no. 13 (August 2016), https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/.

Page 2863 of 3957

Researchers examining the organization and capabilities of the Russian media propaganda machine explain that it has overt and covert components. The former encompasses the vast network of media outlets and news agencies whose editorial policies are under the Kremlin's direct control.[10] Monica Hanley and Andrey Kuzichkin provide valuable details about the organization of the Russian media landscape, the major media holding companies, and who owns them. The authors show that these media networks receive funds from some of the largest Russian state or private corporations such as Gazprom, VneshTorgBank, and Severstal. The authors also describe the specialized administrative structures that support the Russian media operations and the role of the Russian presidential administration in this process.

Similarly, Tod Helmus finds that the Kremlin uses its nexus of media companies in congruence with covert assets such as online trolls and bots.[11] He explores the difference in Moscow's tactics in the countries close to its borders and those far away. In the 'far abroad' states, Helmus observes that the Kremlin identifies radical or extremist groups from the conservative or liberal spectrum, tries to reinforce their extreme political views, and then provokes a conflict between them. In contrast, in the 'near abroad,' the targets are typically Russian ethnic and language minorities, Orthodox religious communities, or those with a shared memory about historical events.[12] In this light, Vasile Rotaru examines Moscow's "soft power" in the countries bordering Russia and provides details on the potential role of such groups in Russian influence operations.[13]

---

[10] Monica Hanley and Andrey Kuzichkin, *Russian Media Landscape:Structures, Mechanisms, and Technologies of Information Operations* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2021), https://stratcomcoe.org/publications/russian-media-landscape-structures-mechanisms-and-technologies-of-information-operations/215.

[11] Todd C. Helmus, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Research Report (Rand Corporation), RR-2237-OSD (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR2237.html.

[12] Helmus, 14–22.

[13] Vasile Rotaru, "Forced Attraction?: How Russia Is Instrumentalizing Its Soft Power Sources in the 'Near Abroad,'" *Problems of Post-Communism* 65, no. 1 (January 2, 2018): 37–48, https://doi.org/10.1080/10758216.2016.1276400.

Page 2864 of 3957

The covert component of the Russian information operation capabilities includes groups such as the IRA that have used concealed actions to disseminate disinformation or employ divisive tactics among their target audiences. These IRA activities have attracted the attention of the scientific community worldwide. In particular, two events have primarily captured the researchers' focus: the 2016 U.S. presidential elections and the protest movement #BlackLivesMater (BLM).

Ahmer Arif et al.[14] demonstrate that during the BLM protests, the IRA used "Twitter and other online platforms to infiltrate politically active online communities." An important finding is that the IRA agents focused their efforts to manipulate the pro-BLM audience and those against the protest movement. Moreover, the Russian trolls' activities went beyond simply spreading disinformation on social media, as they were able to "connect to the cultural narratives, stereotypes, and political positions" of their target audiences." The authors point out that the IRA activities rely on three different components. The first is "the affordances of the online environment," or the inherent characteristics of Twitter and the other social media that define how the users use them. The second is "the social structures and behaviors of the online crowd," or the targeted audience's subgroups, hierarchy, or leaders and how they interact with each other. The third is "the improvised performances of agents that seek to leverage that crowd," or the actual actions to influence the target audience.

Similar findings are presented by Darren Linvill and Patrick Warren, who categorize IRA accounts into five general types: Right Troll, Left Troll, News Feed, Hashtag Gamer, and Fearmonger.[15] These authors observe that "within each type, accounts were used consistently, but the behavior across types was different, both in terms of

[14] Ahmer Arif, Leo Graiden Stewart, and Kate Starbird, "Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse," *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (November 2018): 1–27, https://doi.org/10.1145/3274289.

[15] Darren L. Linvill and Patrick L. Warren, "Troll Factories: Manufacturing Specialized Disinformation on Twitter," *Political Communication* 37, no. 4 (February 2020): 447–67, https://doi.org/10.1080/10584609.2020.1718257.

Page 2865 of 3957

'normal' daily behavior and in how they responded to external events."[16] They compare the Internet Research Agency's organization to industrial enterprises that use "interchangeable parts" with specialized functions to achieve political goals.

Philip Howard et al. reveal how the IRA's activities sought to polarize U.S. society during the 2016 presidential election by engaging primarily far-conservative and far-liberal communities on social media. Specifically, the authors used qualitative and quantitative analysis to demonstrate that IRA operations targeted "African American voters to boycott elections or follow the wrong voting procedures" and incited "extreme right-voters to be more confrontational." [17]

Congressional hearings questioning social media companies' officials[18] regarding the Kremlin meddling in the U.S. election process and court indictments against IRA-linked individuals[19] also provide an important source of detailed information about the IRA's structure, leadership, and activities. During the hearings, a Twitter representative revealed that more than 47% of the IRA accounts were automated. In addition, he confirmed that Russian media company RT purchased ads that promoted election-related content that Twitter identified as being "inflammatory or low-quality."[20] The court indictment details the IRA's owners, management, departments, activities, and budget.

---

[16] Linvill and Warren, 447.

[17] Philip N. Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012–2018," *Oxford, UK: University of Oxford, Computational Propaganda Research Project, 2019*, October 2019, 48, https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs.

[18] *Russia Investigative Task Force: Testimony before Permanent Select Committee on Intelligence*, 115th Cong. (2017) (statement of Sean J. Edgett Acting General Counsel, Twitter, Inc), accessed February 4, 2022, https://docs.house.gov/meetings/IG/IG00/20171101/106558/HHRG-115-IG00-Wstate-EdgettS-20171101.pdf.

[19] The U.S. vs. The Internet Research Agency LLC, 1:18-cr-00032-DLF, filed February 16, 2018, https://www.justice.gov/file/1035477/download.

[20] *Russia Investigative Task Force: Testimony before Permanent Select Committee on Intelligence*, 115th Cong. (2017) (statement of Sean J. Edgett Acting General Counsel, Twitter, Inc), https://docs.house.gov/meetings/IG/IG00/20171101/106558/HHRG-115-IG00-Wstate-EdgettS-20171101.pdf, 13.

Page 2866 of 3957

Information operations have different manifestations, and they often result in "distraction, distortion, dismay, and disruption"[21] in the public perceptions of specific communities or the society in a given country as a whole. David Beskow and Kathleen Carley's research demonstrates that these activities could be message-driven or network-driven.[22] Message-driven and network-driven activities differ in their targets. The former aims at a public perception by spreading inaccurate or divisive information.[23] The latter aims to affect group dynamics by manipulating the target's social ties. For example, network-driven messages focus on removing a group's less radical opinion to transform it into a polarized echo chamber.[24] As a result, the main goal of the researchers studying information operations is to examine the dynamics of these processes and "to classify adversarial actors and their activities, assess and predict their impact, and design effective strategies for intervention and building the resilience of online communities."[25]

In addition, studies of information operations conducted through the internet agree that the dissemination of disinformation or fake news is their most recognizable feature, and how to detect them is the central question that needs an answer. The researchers approach this problem from different perspectives. For example, the data-oriented approach explores online communication by analyzing messages and their social context. Knowledge perspective fake-news detection compares verified news articles to knowledge

---

[21] Ben Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It," *Central European Policy Institute* 15 (2015), https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

[22] David M. Beskow and Kathleen M. Carley, "Social Cybersecurity: An Emerging National Security Requirement," *Military Review*, March-April (2019), https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MA-2019/Beskow-Carley-Social-Cyber.pdf.

[23] W. Lance Bennett and Steven Livingston, "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions," *European Journal of Communication* 33, no. 2 (April 2018): 122–39, https://doi.org/10.1177/0267323118760317; Mejias and Vokuev, "Disinformation and the Media."

[24] R. Kelly Garrett, "Echo Chambers Online?: Politically Motivated Selective Exposure among Internet News Users," *Journal of Computer-Mediated Communication* 14, no. 2 (January 2009): 265–85, https://doi.org/10.1111/j.1083-6101.2009.01440.x; Elmie Nekmat, "Prosocial vs. Trolling Community on Facebook: A Comparative Study of Individual Group Communicative Behaviors," *International Journal of Communication* 12 (2018): 1–22, http://ijoc.org.

[25] Joshua Uyheng et al., "Interoperable Pipelines for Social Cyber-Security: Assessing Twitter Information Operations during NATO Trident Juncture 2018," *Computational and Mathematical Organization Theory* 26, no. 4 (December 2020): 3, https://doi.org/10.1007/s10588-019-09298-1.

Page 2867 of 3957

in a trustworthy database.[26] The knowledge perspective fake-news detection method compares verified news articles to knowledge in a trustworthy database, while style-based detection captures "the differences in writing styles between fake and accurate news."[27] Another approach, the propagation perspective, explores the dissemination path of the news and indirectly detects fake news by assessing the credibility of the headlines, publishers, comments, and users.

Data mining, machine learning, and natural language processing methods are the major tools in implementing these approaches. Each tool differs from the others in its strategies, datasets, and techniques.[28] They are described in more detail in the following section of this thesis.

Other researchers correctly observe that combining these approaches may yield better results. Joshua Uyheng et al.[29] put the concept of social cyber-security and interoperability at the center of their work. Social cyber-security is "a multidisciplinary and multimethodological field that studies how to preserve the Internet as a free and open space for the exchange of information." [30] Carley and Beskow further examine how technology change and decentralization of information flow enables the emergence of social cyberthreats.[31] They explain that "technology has waived the requirement for physical proximity to influence society; and, the decentralization of information flows has reduced the cost of entry."[32]

---

[26] Kai Shu et al., *Fake News Detection on Social Media: A Data Mining Perspective*, vol. 19, 2017, https://arxiv.org/pdf/1708.01967.pdf.

[27] Xinyi Zhou et al., "Fake News: Fundamental Theories, Detection Strategies and Challenges," in *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining* (WSDM '19: The Twelfth ACM International Conference on Web Search and Data Mining, Melbourne VIC Australia: ACM, 2019), 837, https://doi.org/10.1145/3289600.3291382.

[28] Zhou et al., "Fake News."

[29] Uyheng et al., "Interoperable Pipelines for Social Cyber-Security."

[30] Kathleen M. Carley et al., "Social Cyber-Security," in *Social, Cultural, and Behavioral Modeling*, ed. Robert Thomson et al., vol. 10899, Lecture Notes in Computer Science (Cham, Switzerland: Springer International Publishing, 2018), https://doi.org/10.1007/978-3-319-93372-6_42.

[31] Beskow and Carley, "Social Cyber-Security."

[32] Beskow and Carley, 122.

Page 2868 of 3957

The analysis of "online content polluters, such as bots and trolls,"[33] has an important place in the field of social cyber-security. They both spread aggressive or disruptive messages. It should be noted that in contrast to trolls who are humans, bots are automated accounts.[34] The success of these "online polluters" has both technological and sociopsychological aspects. Thus, social cyber-security researchers have to combine methods in both computational social sciences.

Several prior Naval Postgraduate School (NPS) theses have also focused on social media to study influence in the information environment. For example, Eric Chan explored Russian influence operations and the historical background of IRA activity.[35] Meanwhile, James Morales provided valuable information on how to use tweets' sentiment analysis for assessing the anti-American mood in Pakistan and Japan. Particularly interesting is his study on how public perceptions change due to U.S. exercises in Japan.[36] Greg Selph et al. examine the relation between the civil conflicts in Nigeria, the Philippines, and Pakistan and the change in sentiment of tweets. The authors provide a valuable assessment of the significance of sentiment analysis for studying social media.[37]

B. METHODS OF STUDYING INFORMATION OPERATIONS

The most frequently used methods for analyzing information operations are dynamic network analysis, natural language processing, and machine learning. Machine

---

[33] Kyumin Lee, Brian David Eoff, and James Caverlee, "Seven Months with the Devils: A Long-Term Study of Content Polluters on Twitter," in *Fifth International AAAI Conference on Weblogs and Social Media*, Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media (College Station, TX: Texas A&M University, 2011), 8; Emilio Ferrara, *Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election* (Los Angeles, CA: University of Southern California, Information Sciences Institute, 2017), 33, https://ssrn.com/abstract=2995809.

[34] David M. Beskow and Kathleen M. Carley, "It's All in a Name: Detecting and Labeling Bots by Their Name," *Computational and Mathematical Organization Theory* 25, no. 1 (March 2019): 24–35, https://doi.org/10.1007/s10588-018-09290-1.

[35] Elvis M. Chan, "Fighting Bears and Trolls: An Analysis of Social Media Companies and U.S. Government Efforts to Combat Russian Influence Campaigns during the 2020 U.S. Elections" (master's thesis, Naval Postgraduate School, 2021), 25–59, http://hdl.handle.net/10945/68309.

[36] James Morales, "Assessing Anti-American Sentiment through Social Media Analysis" (master's thesis, Naval Postgraduate School, 2016), 45, http://hdl.handle.net/10945/51587.

[37] Gregory R. Selph, Michael H. Crain, and Andrew Anderson, "Measuring Sentiment Response to Collective Violence through Social Media" (master's thesis, Naval Postgraduate School, 2018), 26, http://hdl.handle.net/10945/66275.

learning algorithms are very efficient in the automatic identification of fake accounts and bots in online conversations.[38] These algorithms are applied to aggregated datasets to discover patterns in bots' messaging behavior or relationships with other social network nodes. Uyheng et al. claim that "given a reasonably large dataset of a labeled bot and non-bot accounts, predictive models can be trained to discriminate between each type of account with decent accuracy ($\geq$ 90%) across various contexts."[39] Other studies demonstrate that detecting trolling and opinion manipulation in news community forums and Twitter can use online messages' textual features.[40] When studying online information operations, another critical task is identifying the topics or central messages of the targeted conversations. Techniques such as topic modeling allow researchers to capture the core ideas and reveal critical aspects of a disinformation campaign. For example, the Latent Dirichlet Allocation (LDA) algorithm can extract topics from a corpus of texts using natural language processing.[41] Finally, dynamic network analysis provides quantitative methods to test hypotheses about users' influence in an online conversation. It analyzes how their characteristics and behavior change over time and how they interact. For example, on Twitter, the study of users' features and their ties (how they retweet, reply, or are mentioned) can deliver "more complex insights into online discourse."[42]

Uyheng et al.[43] convincingly demonstrate that these methods can discover patterns in Twitter users' behavior attributed to online information campaigns during NATO

---

[38] Fred Morstatter et al., "Is the Sample Good Enough? Comparing Data from Twitter's Streaming API with Twitter's Firehose," *ICWSM 2013*, June 2013, http://arxiv.org/abs/1306.5204; SiHua Qi, Lulwah AlKulaib, and David A. Broniatowski, "Detecting and Characterizing Bot-Like Behavior on Twitter," in *Social, Cultural, and Behavioral Modeling: 11th International Conference, SBP-BRiMS 2018 Washington, DC, USA, July 10–13, 2018 Proceedings 123*, n.d.

[39] Uyheng et al., "Interoperable Pipelines for Social Cyber-Security," 3.

[40] Carley et al., "Social Cyber-Security"; Todor Mihaylov, Georgi Georgiev, and Preslav Nakov, "Finding Opinion Manipulation Trolls in News Community Forums," in *Proceedings of the Nineteenth Conference on Computational Natural Language Learning* (Proceedings of the Nineteenth Conference on Computational Natural Language Learning, Beijing, China: Association for Computational Linguistics, 2015), 310–14, https://doi.org/10.18653/v1/K15-1032.

[41] David M. Blei, Andrew Ng, and Michael Jordan, "Latent Dirichlet Allocation," *Journal of Machine Learning Research* 3 (January 2003): 22.

[42] Kathleen M. Carley et al., "Toward an Interoperable Dynamic Network Analysis Toolkit," *Decision Support Systems* 43, no. 4 (August 2007): 1324–47, https://doi.org/10.1016/j.dss.2006.04.003.

[43] Uyheng et al., "Interoperable Pipelines for Social Cyber-Security," 5.

Page 2870 of 3957

exercises. They apply LDA to determine what topics are prevalent in Twitter communication when NATO exercises occur and how they change over time. Next, the researchers explore the features of Twitter accounts to classify them as bots or not. For this purpose, they use a random forest machine learning model such as Bothunter.[44] In parallel, the authors employ different neural networks trained on a dataset of user descriptions for role identification (e.g., if the users are news agencies, reporters, and others) and for location prediction. In the end, they use an Organization Risk Analyzer (ORA) for individual and network drill-down to identify influential users, characterize the Twitter conversation's overall structure, and visualize the results. Uyheng et al.'s approach shows that combining computational tools can better analyze information operations in social media, as this approach can gain more complex insights into participants and their messages than single tools can.

Nonetheless, these results could be improved further by integrating different analytical tools or methods, such as sentiment analysis (especially in languages other than English), regression analysis, and network topology metrics' calculation. The change in the sentiment of tweets can play the role of a dependent variable in regression models to establish which factors have a statistically significant influence. The calculation of different topology metrics of the users' social network can reveal how its characteristics, such as centralization or interconnectedness, change under specific factors. This thesis complements the earlier analysis of the Russian covert and overt media agencies' role in influencing the information environment during NATO exercises in Europe. It combines regression, sentiment, and social network analyses to determine systematically how significant political-military events such as Allied exercises affect social media users' perceptions.

[44] David M. Beskow and Kathleen M. Carley, *Bot-Hunter: A Tiered Approach to Detecting & Characterizing Automated Activity on Twitter*, Xx (Pittsburgh, PA: Carnegi Mellon University, 2018), 1, https://www.researchgate.net/publication/326606376_Bot-hunter_A_Tiered_Approach_to_Detecting_Characterizing_Automated_Activity_on_Twitter.

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2872 of 3957

III. INFORMATION WARFARE: THE BEAR AND THE DRAGON

A. INFORMATION CONFRONTATION, INFORMATION WARFARE, AND INFORMATION OPERATIONS

The development of information technologies has led many military and political leaders worldwide to value the significance of influence and control over the information environment. Moreover, the widely accepted understanding is that this influence and control can go beyond its traditional force multiplier role in conventional military operations and become central in non-military confrontation.

In the United States, the Department of Defense defines information operations as disruptive actions aimed at the decision-making process of potential adversaries. These actions include employing information-related capabilities (IRC) to gain advantages in the information environment's three distinct dimensions: physical, informational, and cognitive.[45] JP 3-13 further specifies that the IRCs affect the ability of the targeted individual or group "to collect, process, or disseminate information before and after decisions are made."[46] Beyond the offensive aspect, information operations incorporate defensive actions as well. By employing IRC, the information operations aim to protect their own forces in the three-dimensional information environment from hostile activities that can undermine their own chain of command and the decision-making process. Thus, in its essence, an information operation seeks to change the adversary's situational awareness and diminish its information capabilities, in order to ultimately disrupt the adversary's decision-making process.

The Russian political elite, the military, and the academic community attach equally high importance to the process of influence and confrontation in the information environment. As the Chief of General Staff of the Russian Armed Forces, General Valery Gerasimov, points out that information warfare creates wide asymmetric opportunities to

[45] The Joint Chiefs of Staff, *JP 3-13*, 3.

[46] The Joint Chiefs of Staff, I–3.

Page 2873 of 3957

reduce the enemy's combat potential.[47] In Russian documents on the topic, these activities are part of the broader concept of information warfare (*informacionnoe protivoborstva, Russ. информационное противоборство*). Igor Panarin postulates that the main goals of information warfare are to undermine the information security of the hostile state; to damage the integrity (stability) of its governmental and military control system; and to effectively influence the information provided to its leadership, political elite, and the systems that form the public's opinion, perception, and decision making. Panarin states that the ultimate goal of every state in information warfare is to achieve information superiority in the world information environment. Although he does not define the distinct dimensions of the information environment, he distinguishes two types of information warfare—technical and psychological. The first refers to the situation in which the targeted systems exchange and process information, and the latter focuses on the political elite's and public's cognitive capabilities and the alteration of public opinion. However, this differentiation demonstrates that the Russian concept also recognizes that information warfare can target different dimensions—physical or cognitive.[48]

The Ministry of Defense of the Russian Federation shares this definition. It specifies that, in wartime, information resources and capabilities become specific means to suppress enemy activity and deprive it of the opportunity to resist.[49] The Russian military leadership also recognizes the multidimensional character of information warfare. It can have both physical and informational-psychological impacts on the adversary's force. The former is the destruction of the enemy's information, radio-electronic, and computer networks, and the latter is the psychological influence on the population and the personnel of the armed forces of the opposing sides. The Russian concept incorporates both defensive and offensive aspects that must be considered in their unity. As both Panarin and the

---

[47] Valery Gerasimov, "The Science's Value is in the Prediction." *Military Industrial Courier* no. 8(476), 02/27-03/05/2013, https://vpk-news.ru/sites/default/files/pdf/ VPK_08_476.pdf, accessed February 1, 2022.

[48] Panarin, *Informatsionnaia Voina i Geopolitika [Information Warfare and Geopolitics]*, 172.

[49] *Enciclopedia of the Ministry of Defence of the Russian Federation*, s.v. "information warfare," accessed February 1, 2022, https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary.

military experts underline, it is equally important to protect one's own decision-making process and to influence the adversary's command and control system in information warfare.

The contemporary Russian information warfare concept uses and adapts the Soviet Union's "active measures" such as *dezinformatsiya* or the intentional spread of disinformation or false, inaccurate, and controversial information to mislead the target audience and shape adversaries' public opinion.[50] Arif et al. point out that such strategies are "ideologically fluid," and thus they are suitable to sow discord among very diverse political groups. They involve "harnessing existing public discontent by amplifying reductive social interpretations that confirm existing beliefs, support desired conclusions, or prompt certain strong emotions regarding groups of people and events."[51]

Beijing has carefully analyzed the campaigns of the United States in the Gulf War, Kosovo, Iraq, Afghanistan, and Ukraine, and what role information operations played in them.[52] It uses these lessons learned to adjust and update its concept for information warfare. The foundation of modern Beijing's concept are the theories of "Unrestricted War" and the "Three Warfares." The former posits that, in future conflict, the state has to implement "all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests."[53] The latter is part of so-called "political warfare," which includes the integrated usage of psychological warfare, public opinion warfare, and legal warfare. These three warfare types constitute "a discursive power over an adversary—that is, the power to control

---

[50] More details about Soviet disinformation campaigns can be found in Ladislav Bittman, *The KGB and Soviet Disinformation: An Insider's View* (Washington, DC: Pergamon-Brassey's, 1985); Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes information, Culture and Money* (New York: Institute of Modern Russia, 2014); and Alvin A. Snyder, *Warriors of Disinformation: American Propaganda, Soviet Lies, and the Winning of the Cold War: An Insider's Account* (New York: Arcade Publishing, 2014.

[51] Arif, Stewart, and Starbird, "Acting the Part," 3.

[52] Beauchamp-Mustafaga and Chase, *Borrowing a Boat Out to Sea*, 34–36.

[53] Liang Qiao and Xiangsui Wang, *Unrestricted Warfare*, 2nd ed. (Wuhan, China: Chongwen, 2011), 41.

Page 2875 of 3957

perceptions and shape narratives that advance Chinese interests and undermine those of an opponent."[54]

Beauchamp-Mustafaga and Chase explain that public opinion warfare includes using "various media means and information resources" to "create a favorable public opinion environment for political initiative and military victory.[55]" This type of warfare has a relatively permanent nature and occurs both in wartime and peacetime. It finds expression in "long-term infiltration into the objects of the society and culture's deep structure, changing the awareness and conviction of the enemy masses."[56] Charon et al. specify that China's general idea of public opinion refers to the terms "public emotion" and "public opinion." The first term is "subjective interpretation of certain social realities,"[57] and therefore, it is an individual's perception. At the same time, the second emphasizes "the socio-political attitudes generated by social interactions, and thus it is the collective majority opinion."[58] Hence, control over public opinion is inextricably tied with control over public emotions. Charon and Jeangène Vilmer describe the core of public opinion warfare as the "cognitive orientation of the masses, to excite their emotions and to constrain their behavior."[59]

Beauchamp-Mustafaga and Chase point out that there is a difference between public opinion warfare and psychological warfare. The latter is "more focused and concentrated in wartime."[60] According to their analysis of strategic documents of the People's Liberation Army, Charon and Jeangène Vilmer assert that Beijing distinguishes four types of psychological warfare: "coercion," "mystification," "division," and "defense."[61] The first seeks to force the adversary to adopt a particular behavior; the

---

[54] Beauchamp-Mustafaga and Chase, *Borrowing a Boat Out to Sea*, 8.

[55] Beauchamp-Mustafaga and Chase, 9.

[56] Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," 2.

[57] Charon and Jeangène Vilmer, *Chinese Influence Operations*, 30.

[58] Charon and Jeangène Vilmer, 30.

[59] Charon and Jeangène Vilmer, 48.

[60] Beauchamp-Mustafaga and Chase, *Borrowing a Boat Out to Sea*, 8–9.

[61] Charon and Jeangène Vilmer, *Chinese Influence Operations*, 49–50.

second spreads confusion and misleads; the third uses the adversary's weaknesses and domestic disagreements to hinder its decision-making process, ruin fighters' morale, and diminish public confidence. The fourth protects one's own troops' morale from the enemy's influence.[62] Related to psychological warfare is the concept for "cognitive domain operations." As Beauchamp-Mustafaga and Chase explain, China considers these operations as the next step in the evolution of warfare, "moving from the natural and material domains—land, maritime, air, even electromagnetic—into the ephemeral, namely the human mind."[63] Such operations target the enemy's cognitive thinking and decision-making processes with the means of psychological warfare to disrupt. Their ultimate goal is to achieve "mind superiority."[64]

The third component of the "Three Warfares" concept, legal warfare, corresponds to the strategic use of the law. Its essence is to exploit the legal provisions of international and national laws to provide legitimacy for Chinese demands or policies.[65] Its goal is to "attain normative superiority" that can justify the use of force during a conflict, or when confrontation ends "to retain any gains or to claim its due."[66]

The "Three Warfares" concept demonstrates that China, like the United States and Russia, also sees information warfare as a multidimensional phenomenon and recognizes the importance of operations in the information and cognitive dimensions. Beijing combines contemporary theories such as cognitive-domain operations, discursive power, and political warfare with older concepts such as "active measures," which China inherited from its historical ties with the former Soviet Union. This combination, together with the lessons learned from its main allies and adversaries, allows China to adapt its strategies and doctrines successfully to exploit the benefits and weaknesses of today's information environment.

---

[62] Charon and Jeangène Vilmer, 49.

[63] Beauchamp-Mustafaga and Chase, *Borrowing a Boat Out to Sea*, 10.

[64] Charon and Jeangène Vilmer, *Chinese Influence Operations*, 31.

[65] Charon and Jeangène Vilmer, 31.

[66] Charon and Jeangène Vilmer, 51.

In conclusion, all three major actors in the international political system adopt strategies and develop capabilities to gain an advantage over the information environment. As described in the literature just reviewed, the ultimate goals of information operations are to hinder the decision-making process of the adversary's political leadership and military commanders, affect the morale of the population and armed forces of the hostile nation, and protect a country's own forces and political system from malicious influence. Thus, information operations have both defensive and offensive aspects.

A common understanding is that the information environment has different dimensions that define two specific directions of confrontation. The first targets the physical dimension and the technical systems that transmit, receive, and store information; the second aims at psychological impacts on the target audience by manipulating the information and cognitive dimensions. In recent years, with the increase in online connectivity and rapid expansion of social media such as Facebook, Instagram, and Twitter, the latter dimension has grown more significant.

B. SOCIAL MEDIA IN INFORMATION WARFARE

This section explores the main characteristics of the information operations conducted on social media, and on Twitter in particular, by the adversaries of the United States and NATO. Although the previous chapter makes clear that China has significant capabilities and ambitions to dominate the global information environment, until recently, Beijing's focus has been predominantly on influencing its close neighborhood (Hong Kong, Taiwan), the Pacific region, and North America. This thesis, however, focuses primarily on the activities of various entities connected to the Russian Federation as they relate to the possible effects of hostile information operations conducted during NATO exercises in Europe. Samantha Bradshaw and Philip Howard point out that the social media information environment is complex and constantly evolving. In this environment, various actors pursue their political goals by creating and disseminating narratives designed to provoke a specific reaction in the targeted audience. At the same time, these audiences also are a diverse community, and they react differently to these narratives. Often, they

Page 2878 of 3957

contribute to the further development of the narrative by adding links to other content such as video, pictures, or music.[67]

Various Russian companies and organizations are involved in social media information operations. Some of them operate openly, such as the television channel RT (formerly Russia Today) and the news agency Sputnik, while others work covertly, such as the IRA. This combination allows the Kremlin to run "large-scale and complex information operations" with actors "at varying levels of attribution."[68]

The overt companies comprise a vast network that connects to domestic and foreign audiences through online channels on different social media platforms and at the same time creates more traditional content for TV channels, newspapers, and news agencies. These two forms of communication cannot be entirely separated because the traditional media products are also disseminated online.[69] A 2021 report by the NATO Center of Excellence for Strategic Communication reveals that the RT news service is central in Moscow's information operations. This news service was created in 2005 under Russia Today's brand, but later it changed its name to RT. The non-profit organization ТВ-Новости/TV-News controls RT; however, RT's funding comes entirely from the Russian state budget. In 2020, the subsidy to TV-News was more than 360 million U.S. dollars. Around 83% of these funds are dedicated to media content production. Margarita Simonyan has been in charge of the main editorial office of RT since 2005.[70] She and her husband have tight connections to members of the presidential administration, such as its First Deputy Chief of Staff, Alexei Gromov. He is one of RT's creators and maintains the Kremlin's control over the work of the largest newspapers, television channels, and news agencies.[71] RT also has a YouTube channel, which was the first "to reach 1 billion views … and later it was

---

[67] Philip N. Howard and Samantha Bradshaw, "The Global Organization of Social Media Disinformation Campaigns," *The Journal of International Affairs, SIPA* 71 (September 2018): 9, https://jia.sipa.columbia.edu/global-organization-social-media-disinformation-campaigns.

[68] Helmus, *Russian Social Media Influence*.

[69] Helmus, 26.

[70] Hanley and Kuzichkin, *Russian Media Landscape*, 22.

[71] Hanley and Kuzichkin, 11.

also the first to reach 10 billion views."[72] In addition, RT has a vast network of Twitter accounts in different languages, such as @RT_COM, @RT_America, @RTUKnews, @de_rt_com, and @RTarabic_Bn. Each of these accounts has between several thousand and several million followers. Simonyan herself has 531.7 thousand Twitter followers. In a congressional hearing, one Twitter official testified that "@RT_COM and @RT_America together spent $516,900 in advertising in 2016. As a result, they were able to promote 1,912 Tweets and generate approximately 192 million impressions[73] across all ad campaigns.[74]

Another Russian media group with significant input into information operations is Rossiya Segodnya. It is state-owned, and in 2020 the company received 100 million U.S. dollars from the state budget.[75] Rossiya Segodnya is a holding company that controls influential media outlets such as RIA Novosti, Sputnik, InoSMI, Baltnews, and others. These news agencies publish their information products on various online platforms, including Twitter.

Russia's network of existing official media channels significantly contributes to Moscow's capability to organize and conduct information operations. Its main contributions are to receive legally directed funds from the Russian state for media production and to operate legally in different countries. In addition to creating content in several different languages, this arrangement helps such media outlets to access broad audiences. As Hanley and Kuzichkin point out, RT and Sputnik use this opportunity and customize their media products "depending on the audience and the strategic objective."[76] The authors explain that for its Latin American audience RT produces leftist content in the

[72] Hanley and Kuzichkin, 22.

[73] Twitter defines impressions as viewing the content of the tweet. For details see *Russia Investigative Task Force: Testimony before Permanent Select Committee on Intelligence*, 3.

[74] *Russia Investigative Task Force: Testimony before Permanent Select Committee on Intelligence*, 13.

[75] Hanley and Kuzichkin, *Russian Media Landscape*, 25.

[76] Hanley and Kuzichkin, 9.

Page 2880 of 3957

Spanish language, while its products for Eastern European countries emphasize national or historical ties to Russia or praise the strength of the Russian economy.[77]

Complementing these public media organizations, the Kremlin's information operations arsenal has companies that use covert methods, including fake accounts and divisive and fake information posting. A notorious example is the Internet Research Agency, a Russian corporation based in Saint Petersburg. Various authorities and scientists have revealed the corporation's interference in the 2016 U.S. Presidential election[78] and the Black Lives Matter movement's protests.[79] According to Howard et al., the IRA has been using Twitter since 2009. The initial focus was on the Russian audience, and the tweets were primarily in the Russian language. The company began targeting English-speaking users at a slow pace in 2013. By the beginning of 2014, however, its engagement with English-speaking users had increased and grew significantly by the end of the year.[80]

Although the company had direct links to the Russian government, the IRA primarily received funding for its operations from two companies, Concord Management and Consulting and Concord Catering. Both were under the control of Nikolay Prigozhin,[81] who is also the owner of Wagner (a private military company) and has close connections to the Kremlin elite.[82] The IRA's activities also received funding as part of a large interference operation named "Project Lakhta" that targeted audiences in the United States and Russia, France, and other countries. As of 2016, the IRA's monthly budget was over 1.25 million U.S. dollars.[83]

---

[77] Hanley and Kuzichkin, 9.

[78] *The U.S. vs the Internet Research Agency LLC*, 1:18-cr-00032-DLF.

[79] Arif, Stewart, and Starbird, "Acting the Part."

[80] Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012–2018," 10.

[81] *The U.S. vs the Internet Research Agency* at 6–7.

[82] Nathaniel Reynolds, *Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group*, *The Return of the Global Russia* (Washington, DC: Carnegie Endowment for International Peace, 2019), 9–12, https://carnegieendowment.org/files/GlobalRussia_NateReynolds_Vagner.pdf.

[83] *The U.S. vs. the Internet Research Agency* at 7.

The IRA's organizational structure was complex, and it had hundreds of employees "ranging from creators of fictitious personas to technical and administrative support."[84] The company had management and specialized graphic design, data analysis, search engine optimization, finance, information technology, and translation departments. The latter allowed its operators to post information on social media in different languages and expand its global reach.[85] The IRA's staff members worked two 12-hour shifts to match regular users' activity in different time zones, as they did during the 2016 U.S. presidential election. Their tasks were "to create social media accounts that appeared to be operated by U.S. persons…[and]… create political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements."[86] The employees were very productive: they created 36,746 accounts related to the 2016 presidential election. They posted approximately 1.4 million election-related tweets from September through November 2016, and these tweets received approximately 288 million impressions.[87] The IRA's management was responsible for receiving and evaluating the impact of the organization's online social media operations and the size of the online U.S. audiences reached through IRA's posts. They measured "different types of engagement with the posts (such as likes, comments, and reposts), changes in audience size, and other metrics."[88]

These Russian organizations, both the overt and covert ones, involved in information operations have the capability to engage global audiences on various social media platforms and in different geographical locations. Online, such organizations operate on Twitter, Facebook, Instagram, and geographically, they can influence audiences both far and near their borders.[89] However, these targeted social groups in the 'far abroad' and

---

84 *The U.S. vs. the Internet Research Agency* at 6.

85 *The U.S. vs. the Internet Research Agency* at 6.

86 *The U.S. vs. the Internet Research Agency* at 14.

87 *Russia Investigative Task Force: Testimony before Permanent Select Committee on Intelligence*, 10.

88 *The U.S. vs. the Internet Research Agency* at 15.

89 Helmus, *Russian Social Media Influence*, 32–39.

Page 2882 of 3957

'near abroad' have different characteristics, forcing the Kremlin to adapt its influence strategies.

The so-called 'near abroad' includes the former Soviet republics and most East European states. Such countries usually have sizable Russian minorities, Russian-speaking citizens, or groups that share common memories or interpretations of history. These communities are both targets and conduits of Russian "soft power" and influence.[90] Moscow's most important narratives in these countries include tropes about traditional (Russian) conservative values, such as family and orthodoxy, a shared fear of violent revolutions, and the West's betrayal and moral degradation.[91]

In contrast to the 'near abroad,' Russian information operations in the 'far abroad' countries focus on radical political groups, social movements, and religious groups. Andrew Weisburd, Clint Watts, and Jim Berger argue that Moscow's information campaigns fall into four categories: political, financial, social, and conspiracy. The political and financial campaigns aim to slander political leaders, undermine governmental institutions' credibility, or erode trust in the financial system or experts. The social objectives of such operations seek to "undermine the fabric of society."[92] Finally, the dissemination of conspiracy theories promotes images of "global calamity while questioning the expertise of anyone who might calm those fears."[93]

Ben Nimmo formulates four specific tactics that the Kremlin uses to achieve these goals: dismiss, distort, dismay, and distract. The dismiss tactics deny the truth of the facts that contradict Moscow's narratives or tarnish the credibility of the source of these facts. The distorted tactics mix cherry-picked facts, lies, and disinformation. Since the ultimate goal is to sow doubts in the designated audiences, the truthfulness of the dismissed facts or blatant falsehood of the distorted message is not essential. All these tactics need only to

---

[90] Rotaru, "Forced Attraction?," 3–10.

[91] Helmus, *Russian Social Media Influence*, 10.

[92] Andrew Weisburd, Clint Watts, and Jim Berger, "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy," War on the Rocks, November 6, 2016, https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

[93] Weisburd, Watts, and Berger.

Page 2883 of 3957

disorient the targeted population or social groups. The dismay tactics intimidate and induce fear and anxieties in the audience, usually through harassment and personal threats. Finally, the distraction techniques turn the "attention away from the activities of Russia and its allies by launching accusations elsewhere."[94] Overall, as Peter Pomerantsev and Michael Weiss observe, "the aim of this new propaganda is not to convince or persuade, but to keep the viewer hooked and distracted, passive and paranoid, rather than agitated to action."[95]

Linvill and Warren explored the implementation of these tactics by the IRA from June 19, 2015, to December 31, 2017, and "identified five categories of IRA-associated Twitter handles, each with unique patterns of behaviors."[96] These categories are Right Troll, Left Troll, News Feed, Hashtag Gamer, and Fearmonger. The Right Troll accounts posted nativist and right-leaning populist messages. The Left Troll handles published "socially liberal messages, with an overwhelming focus on cultural identity."[97] The News Feed accounts "overwhelming presented themselves as the U.S. local news aggregators,"[98] while the Hashtag Gamer handles promoted hashtag games, some of which had socially or politically divisive hashtags. The fifth category, Fearmonger trolls, posted news about crisis events, usually fabricated. The authors observed that Left and Right Trolls were more active than the other types, but their activity varied significantly on a day-to-day basis. The News Feed accounts tweeted at a relatively consistent rate throughout the explored period. By contrast, the Hashtag Gamer handles were "very active during and after the election season, but by the summer of 2017, they [were] nearly silent."[99] All five troll types changed their behavior under specific political circumstances. For example, when John Podesta's email was leaked to the press for the first time (8:30 pm UTC on October 7,

---

[94] Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It."

[95] Peter Pomerantsev and Michael Weiss, *The Menace of Unreality:How the Kremlin Weaponizes Information, Culture and Money* (New York, NY: The Institute of Modern Russia, 2014), 11, https://www.almendron.com/tribuna/wp-content/uploads/2015/08/The_Menace_of_Unreality_Final.pdf.

[96] Linvill and Warren, "Troll Factories," 451.

[97] Linvill and Warren, 452.

[98] Linvill and Warren, 452.

[99] Linvill and Warren, 453.

Page 2884 of 3957

2016), the News Feeds trolls continued to post messages at their regular low rate. Meanwhile, the Hashtag Gamers' activity which was very high in the late hours of October 5, 2016, went silent in the following days. In contrast, the Left and Right trolls became active on October 6, 2016, and tweeted at a high rate until October 7, 2016.[100]

In conclusion, the Russian Federation has the capability to organize and implement online information operations through its covert and overt assets. RT news network and Sputnik news agency are among the most powerful tools in the Russian online arsenal. Under the Kremlin's strict control, they deliver and popularize narratives to their vast audience in countries in the near and the far abroad. Additionally, Moscow has created companies that use covert techniques to engage carefully selected social groups in order to manipulate their perceptions and emotions. In such cases, the main goal is to sow distrust, disorient targeted groups' value systems, and amplify social divisions. An example of this type of covert organization is the Internet Research Agency, which had hundreds of employees, and its leadership had close connections to the Kremlin's political elite. Studies of the IRA's activities and tactics revealed possible patterns in its operations on Twitter. Most importantly, research has delineated the types of accounts that IRA operators used for their tasks. These accounts revealed distinct posting behaviors and shared specific information.

Russia's overt and covert organizations have developed a global reach and can target audiences in various languages. Typically, in the 'near abroad' countries, the target is local Russian-speaking communities, Russian ethnic minorities, and other groups that share cultural, historical, or religious identity with Russia. For these audiences, Moscow's narratives include positive interpretations of the Russian political and cultural model and negative depictions of the Western political, financial, and social systems. The 'far abroad' narratives aim at damaging social cohesiveness and confidence in institutions. Since their goal is to reinforce the most radical opposing opinions, they may also include positive and negative messages regarding a particular topic.

---

[100] Darren L. Linvill and Patrick L. Warren, *Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building* (Clemson, SC: Clemson University, 2018), 11, http://pwarren.people.clemson.edu/Linvill_Warren_TrollFactory.pdf.

Page 2885 of 3957

The next chapter details the research methods used in this thesis to examine user activity on one particular social media platform, Twitter, between July 2013 and August 2014, to identify factors related to IRA and Russian media efforts specifically influencing sentiments in tweets about NATO.

Page 2886 of 3957

IV. RESEARCH METHODS

A. HYPOTHESES

This research examines one year of user activity on Twitter from July 2013 to August 2014. The purpose is to identify the significant factors that influence sentiments related to tweets on a particular topic—in this case, all tweets in which the text included the acronym NATO.

The first hypothesis is that the overall sentiment in the online conversation on NATO will become more negative if there is an increase in IRA and Russian media activity (Hypothesis 1). The second hypothesis is that while NATO exercises are occurring the sentiment of the online conversation related to NATO will become more negative as the activity of Russian media organizations, whether covert or overt, increases. Third, this thesis hypothesizes that the change in sentiment during NATO exercises will be more negative in a country closer to the borders of the Russian Federation (Hypothesis 3). Fourth, this thesis also hypothesizes that IRA and Russian media activity during NATO exercises will increase the size of the daily user network for the NATO conversation, and that network will become more centralized and interconnected (Hypothesis 4).

B. DATA AND METHODS

To test the hypotheses formulated in Section A this thesis examines specific datasets and applies different methods, such as regression and sentiment analysis, text mining, and social network analysis.

1. Datasets

This thesis uses the NPS-licensed Twitter archive as the primary data source. It contains a random sample of ten percent of the tweets posted globally between August 1, 2013, and July 31, 2014.

A search query was constructed based on the acronym NATO (in the English, French, Chinese, and Cyrillic alphabets) and a list of handles connected to IRA and Russian online media outlets. The U.S. House of Representatives Permanent Select Committee on

Page 2887 of 3957

Intelligence published these handles in June 2018.[101] The query's results are stored in two datasets. In the first, the results are aggregated in "country-date" units. In the second dataset, each row represents a separate tweet with its text, and each message is represented as a "point" at a latitude/longitude/time location.

2. Sentiment Analysis and Text Processing of Social Media Data

Social media sentiment analysis relies on dictionaries containing words with predetermined positive or negative sentiment scores. In this research, two separate sentiment lexicons[102] are used, one with negative words and one with positive words. These dictionaries are in the English language; therefore, the text of every tweet needs translation before further processing.

Since this research dataset contains information about the tweet's language, the initial dataset was split into smaller sub-datasets according to the tweet's language. The result was 45 distinct sub-datasets organized by "tweet ID" and "text." These sub-datasets were translated using the Google Translate website at the next stage. After translation, each tweet's text went through text processing, including tokenization and cleaning of redundant symbols and words such as punctuation signs, special characters, or symbol combinations (e.g., @, RT, and URLs).

Next, cleaned tokens (words) were compared to the content of the positive and negative dictionaries. Depending on which lexicon contained a match for a word, each word received a sentiment score accordingly. Each word's score was calculated with Formula 1 to distinguish between a positive and a negative sentiment:

$$S_{word} = Positive\ score - Negative\ score \quad (1)$$

Words with a positive sentiment were coded as 1, and the negative as -1. If there was no match or the word was found in both dictionaries, the sentiment score was 0 or neutral.

---

101 *The Internet Research Agency's Handles as of June 2018*, U.S. House of Representatives Permanent Select Committee on Intelligence (Washington, DC, 2018), https://intelligence.house.gov/uploadedfiles/ira_handles_june_2018.pdf.

102 Minqing Hu and Bing Liu, *Mining and Summarizing Customer Reviews*, Research Track Paper (Chicago, IL: University of Illinois at Chicago, 2004).

Page 2888 of 3957

Finally, the overall sentiment of the tweet was calculated using Formula 2 as the sum of the sentiment scores of its tokens:

$$S_{tweet} = \sum_{i=1}^{n} S_{word_i} \quad (2)$$

3. Network Topography Measures

After the sentiment score of the tweets was calculated, edge lists were created for every day in the research period. Two Twitter accounts have a tie between them if one of them retweeted, mentioned, or quoted the other's tweet. The attribute list includes username, language, followers, country name, date when the user tweeted, and two flags indicating whether the user was an IRA member or a Russian official media outlet. Using R-package "igraph,"[103] it was possible to calculate the network size, density, local clustering coefficient, and degree centralization score for all users in 365 social networks.

4. Dependent Variables

The mean sentiment of the tweets in the NATO conversation (as defined earlier) was the dependent variable used to test Hypotheses 1 through 3. It is aggregated to a "country-date" unit of analysis. It is an ordered categorical variable with three levels. The first corresponds to negative sentiment, the second to neutral sentiment, and the third to positive sentiment.

Other dependent variables based on network structure, such as network size, local clustering coefficient, and degree centralization, were used to test Hypothesis 4. The network size is based on the number of accounts in the network. It provides information on how many users participated in the explored NATO online conversation. The change in network size during the research period can provide information on how the network of participants was growing or shrinking.[104] The local clustering coefficient is an interconnectedness measure known as average ego-network density. It provides

[103] Gabor Csardi and Tamas Nepusz, "The Igraph Software Package for Complex Network Research," *InterJournal Complex Systems* (2006): 1695, https://igraph.org.

[104] Daniel Cunningham, *Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis* (Lanham, MD: Rowman & Littlefield, 2016), 86.

Page 2889 of 3957

information on how interconnected the actors of the ego network are.[105] The degree centralization score "uses the variation of the actor's [degree] centrality within the network to measure the level of centralization."[106] If the degree centralization is high, the users' degree centrality scores significantly vary. Therefore, if the score is high, one or a few accounts are significantly more active than the others.[107]

5. Independent Variables

The independent variables cover five categories: spatial effects, network topography, levels of online activity, and the dates of NATO and Russian military exercises.

The distance to the Russian border is the only spatial variable. It represents the shortest distance between the Russian state border and every tweet's location, measuring 0 for tweets originating inside Russia.

Edge density, the only social network topography measure, is an independent variable in the models that test Hypotheses 1 through 3. It introduces information about the behavior of daily user accounts into the model. Its change reflects the emergence or disappearance of the network's ties (as defined earlier).

The Twitter-related variables count the number of tweets originating from IRA or Russian overt accounts by day.

Finally, the exercise-related variables provide information measuring the dates on which NATO or Russian military exercises occurred, coded as 1 for the dates of the exercises and 0 for all other dates. Jan Brzezinski and Nicholas Varangis summarized NATO and Russian military activity over this period, and provided information about their timeline, location, and participants.[108] There were four NATO military drills in Eastern

---

[105] Cunningham, 100.

[106] Cunningham, 87.

[107] Cunningham, 87.

[108] Jan J. Brzezinski and Nicholas Varangis, "The NATO-Russia Exercise Gap," *Atlantic Council* (blog), February 23, 2015, https://www.atlanticcouncil.org/blogs/natosource/the-nato-russia-exercise-gap/.

Page 2890 of 3957

Europe and Scandinavia in the research period. "Steadfast Jazz" took place in Poland and Lithuania (November 2–9, 2013), Norway hosted "Cold Response" (March 7–21, 2014), Estonia hosted "Spring Storm 14/Steadfast Javelin I" (May 5–23, 2014), and "Saber Strike 2014" took place in the Baltic States (June 9–20, 2014). The Russian Federation had three large-scale exercises in the research period. They took place in the Western Military District (Zapad-13, September 17–26, 2013), in the Western and Central Military Districts (February 26–March 3, 2014), and the Central Military District (June 21–28, 2014).

6. Control Variables

The control variables in the tested model are the total number of tweets, the country's population, gross domestic product per capita, political regime type, and access to the internet.

Gross domestic product (GDP) per capita and population provide information about the relative size and prosperity of each country. Access to the Internet provides information about the degree to which the population can use online media as a source of information. The World Bank Development Indicators[109] are the source of these three variables.

The political regime variable is derived from the Polity5 Project dataset.[110] The model uses the revised combined polity score (Polity2), adapted for time-series analysis. It ranges from 10 (strongly democratic) to -10 (strongly autocratic). Introducing this variable in the model provides an opportunity to examine how the ruling regime or the type of government influences the effectiveness of online information operations.

The total number of tweets variable provide information about the overall daily activity in Twitter

[109] World Bank, "World Development Indicator," accessed February 27, 2022, https://datatopics.worldbank.org/world-development-indicators/.

[110] Center for Systemic Peace, "Polity5 Project, Political Regime Characteristics and Transitions, 1800–2018," April 23, 2020, https://www.systemicpeace.org/inscrdata.html.

C. REGRESSION ANALYSIS

The initial analysis presented here utilizes ordered logit regression models. Its goal is to test the formulated hypotheses concerning the relationship among online sentiments, military exercises, and the activity of Russian overt and covert agents. The regression analysis tests four different models. It starts with a simple additive form and gradually introduces different multiplicative interaction terms. These terms examine different relations among the independent variables in accordance with the formulated Hypotheses 1 to 3. A log transformation is applied to all independent variables in the model except *NATO Exercise*, *Russian Exercise*, and *Political Regime* in order to reduce the skew in their values. The full version of the sentiment model is as follows:

$$
\begin{aligned}
\text{Sentiment} = \; & \beta_0 + \beta_1 \text{NATO Exercise} + \beta_2 \text{Russian Exercise} + \beta_3 \text{IRA Tweets} \\
& + \beta_4 \text{Distance to Russia} + \beta_5 \text{Russian Media Tweets} + \beta_6 \text{Edge Density} \\
& + \beta_7 \text{Political Regime} + \beta_8 \text{GDP} + \beta_9 \text{Population} \\
& + \beta_{10} \text{Access to Internet} + \beta_{11} \text{Total Tweets} \\
& + \beta_{12} (\text{Russian Exercise} * \text{Distance to Russia}) + \beta_{13} (\text{NATO Exercise} * \text{Distance to Russia}) \\
& + \beta_{14} (\text{Russian Exercise} * \text{IRA Tweets}) + \beta_{15} (\text{NATO Exercise} * \text{IRA Tweets}) \\
& + \beta_{16} (\text{Political Regime} * \text{IRA Tweets}) + \beta_{17} (\text{NATO Exercise} * \text{Russian Media Tweets})
\end{aligned}
$$

In addition, six log-linear models are used to test Hypothesis 4. Each pair of models tests a different dependent variable—network size, degree centralization, or clustering coefficient—with the first model providing a baseline additive specification and the second model including multiplicative interaction terms. The full version of each model is given by:

$$
\begin{aligned}
\text{Network Metric} = \; & \beta_0 + \beta_1 \text{IRA Tweets} + \beta_2 \text{Russian Media Tweets} + \beta_3 \text{Distance to Russia} + \beta_4 \text{NATO Exercise} \\
& + \beta_5 \text{Political Regime} + \beta_6 \text{GDP} + \beta_7 \text{Population} + \beta_8 \text{Access to Internet} + \beta_9 \text{Total Tweets} \\
& + \beta_{10} (\text{NATO Exercise} * \text{IRA Tweets}) \\
& + \beta_{11} (\text{NATO Exercise} * \text{Russian Media Tweets}) \\
& + \beta 2 (\text{Political Regime} * \text{IRA Tweets})
\end{aligned}
$$

Page 2892 of 3957

V. REGRESSION RESULTS

A. RUSSIAN ONLINE INFLUENCE ON SOCIAL MEDIA SENTIMENT

1. Findings

Tables 1, 2, and 3 show the results of four ordered logit models and their performance. The first table includes the goodness of fit scores for the different models, the second presents the base term coefficients, and the third shows the multiplicative interactive terms in the tested regression models. The analysis of models' goodness of fit scores reveals that the models achieve similar overall error rates, shown by the mean absolute error (MAE) and the root mean squared error (RMSE), while Model 4 performs slightly better than the others according to the Akaike's Information Criteria (AIC) scores. Thus, Model 4 is used for further analysis.

Table 1. Sentiment Regression Models: Goodness of Fit

	Sentiment			
	Model 1	Model 2	Model 3	Model 4
	(1)	(2)	(3)	(4)
Observations	57,377	57,377	57,377	57,377
MAE	0.222	0.222	0.222	0.222
RMSE	0.341	0.341	0.341	0.341
AIC	51,658	51,634	51,618	51,617
BIC	51,774	51,769	51,771	51,787
Log Likelihood	-25,816.011	-25,802.100	-25,792.176	-25,789.443

The results in Table 2 show that there is a positive (0.065) statistically significant relationship ($p < 0.01$) between the number of IRA tweets and the average sentiment of the NATO conversation. Russia's overt media activities also have positive relationship (0.051) to sentiment of the tweets across country-day, though with a lower level of statistical significance ($p < 0.05$). The edge density of the network of users is the third coefficient that is also positively related to sentiment of the tweets. Finally, the control variables are

Page 2893 of 3957

statistically significant, although on a different level. All of them have a p-value<0.01, except political regime with a p-value<0.1. All their coefficients except the country's access to the internet are negative.

Table 2. Sentiment Regression Models: Base Terms

	Sentiment			
	Model 1	Model 2	Model 3	Model 4
	(1)	(2)	(3)	(4)
NATO Exercise	-0.001	-0.152	-0.099	-0.365
	(0.038)	(0.137)	(0.137)	(0.252)
Russian Exercise	0.080	0.071	0.807***	0.807***
	(0.052)	(0.052)	(0.200)	(0.200)
IRA's Tweets	0.039***	0.052***	0.052***	0.065***
	(0.010)	(0.010)	(0.011)	(0.013)
Russian Media Tweets	0.062**	0.060**	0.060**	0.051**
	(0.025)	(0.025)	(0.025)	(0.026)
Distance to Russia	0.005	0.0003	0.004	0.004
	(0.003)	(0.004)	(0.004)	(0.004)
Edge Density	0.320***	0.326***	0.325***	0.325***
	(0.020)	(0.021)	(0.021)	(0.021)
Total Tweets	-0.107***	-0.107***	-0.107***	-0.107***
	(0.009)	(0.009)	(0.009)	(0.009)
Political Regime	-0.015***	-0.015***	-0.015***	-0.008*
	(0.002)	(0.002)	(0.002)	(0.004)
GDP per capita	-0.165***	-0.164***	-0.164***	-0.163***
	(0.022)	(0.022)	(0.022)	(0.022)
Population	-0.180***	-0.180***	-0.180***	-0.180***
	(0.014)	(0.014)	(0.014)	(0.014)
Access to Internet	0.173***	0.171***	0.171***	0.171***
	(0.026)	(0.027)	(0.027)	(0.027)
1| 2	-5.579***	-5.648***	-5.595***	-5.580***
	(0.174)	(0.175)	(0.175)	(0.176)
2| 3	0.110	0.043	0.100	0.115
	(0.170)	(0.171)	(0.172)	(0.173)
Note:				*p<0.1; **p<0.05; ***p<0.01

Page 2894 of 3957

Table 3 provides information about the multiplicative interaction terms included in Models 2, 3, and 4. The first two terms test Hypothesis 2, or whether there is a negative effect on sentiment arising from the combination of NATO exercises and the activity of Russia's overt and covert media actors. The first interaction term between *NATO Exercise* and *IRA Tweets* is negative (-0.106) and statistically significant ($p < 0.01$). The second term, which reflects the influence of Russia's overt media outlets on sentiment during NATO exercises, is not statistically significant. Therefore, it is impossible to draw firm conclusions concerning the direction and the strength of the relationship. The third term, which represents how the users' distance from the Russian border influences the sentiment of their tweets when a NATO exercise occurs, is positive and statistically significant, indicating that sentiment is stronger at longer distances. The fourth and fifth terms test the effects of *IRA Tweets* and *Distance to Russia* on sentiment during Russian military exercises rather than NATO exercises. Of these, only the interaction between *Distance to Russia* and *Russian Exercise* is statistically significant ($p < 0.01$), with a negative (-0.054) coefficient, implying that Russian exercises generate more negative effects on sentiment as the distance from Russia grows. Finally, the sixth term tests how IRA activities and the country's political regime type generate combined effects on sentiment. It is negative (-0.003) and statistically significant, although to a lesser degree ($p < 0.1$), implying that IRA activities generate more negative impacts on sentiments in democracies than in autocracies.

Page 2895 of 3957

Table 3. Sentiment Regression Models: Multiplicative Interaction Terms

	Sentiment			
	Model 1	Model 2	Model 3	Model 4
	(1)	(2)	(3)	(4)
NATO Exercise*IRA Tweets		-0.105***	-0.105***	-0.104***
		(0.029)	(0.029)	(0.029)
NATO Exercise*Russian Media Tweets				0.108
				(0.086)
NATO Exercise*Distance to Russia		0.031***	0.027***	0.027***
		(0.008)	(0.008)	(0.008)
Russian Exercise*IRA Tweets			0.005	0.005
			(0.033)	(0.033)
Russian Exercise*Distance to Russia			-0.055***	-0.055***
			(0.012)	(0.012)
IRA Tweets *Political Regime				-0.003**
				(0.002)
Note:				*p<0.1; **p<0.05; ***p<0.01

2. Analysis of the Findings

Hypothesis 1: *The overall sentiment of the NATO online conversation will become more negative if there is an increase in IRA and Russian media activity.*

The results from the regression models do not support Hypothesis 1. Figure 1, showing estimates derived from Model 4, demonstrates that increased IRA activity heightens the probability that the average sentiment will be positive (blue line) and lowers the probability for negative sentiment (red line) in the graph at the left. The second graph on the right shows that the that the tweets by overt Russian media have a similar effect on sentiment, though that effect is slightly weaker.

Page 2896 of 3957

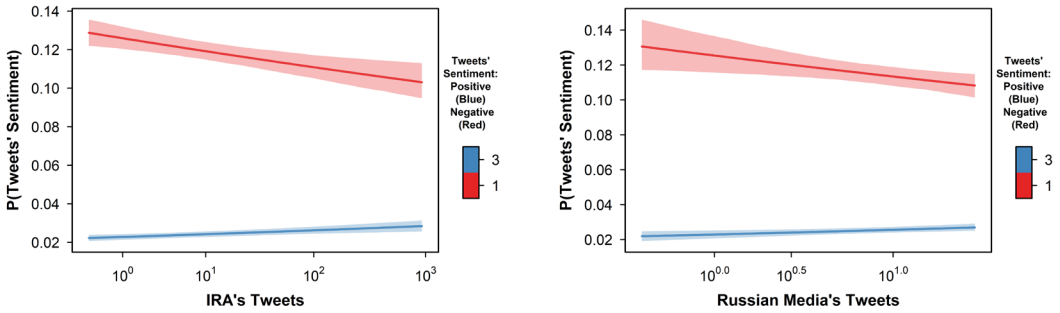


Figure 1. IRA and Russian Media Tweets vs. Sentiment in the NATO Conversation

The colored shading around the lines in the graphs shown in Figure 1 represent the 95% confidence interval of the respective variables and to what degree the slope of the lines in the graphs can vary within this interval. The comparison of the two graphs in Figure 1 reveals that the slopes of the lines are different. Both lines in the graph at left, depicting the IRA's tweets, have a steeper slope than those in the graph at right, depicting the effects of tweets by overt Russian media, which means that the IRA's activity has a more substantial effect on the sentiment than does the activity of overt Russian media.

Figure 2 further supports this conclusion by presenting the substantive effects of IRA and Russian media tweets on positive or negative sentiment probability. For convenience and better comparison, the graphic on the right in Figure 2 presents the absolute values of these effects. From Figure 2, it is easy to compare of the effect magnitudes, which are, in fact, negative (given the red lines on the graphs in Figure 1 have negative slopes).

Page 2897 of 3957

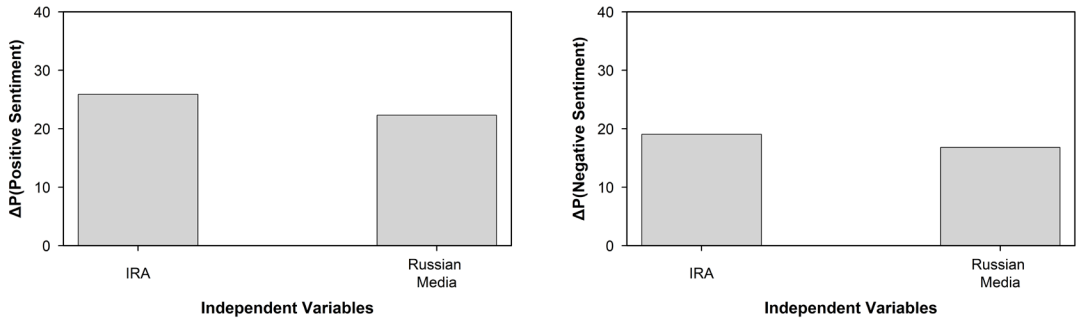


Figure 2. Substantive Effects of IRA and Russian Media Tweets on the Probability of Positive and Negative Sentiment

The graphics in Figure 2 demonstrate two important findings. First, the IRA's tweets have a stronger impact on the probability of sentiment change than tweets by the overt Russian media. Second, both the overt and the covert Russian actors more effectively generate positive sentiment and are counter-intuitively associated with decreases in negative sentiment.

Hypothesis 2: *The sentiment of the online NATO conversation during NATO exercises will become more negative with the increase of the activity of Russian media organizations, whether covert or overt.*

The regression models provide evidence that is partially supportive of Hypothesis 2. The first and second interaction terms in Table 3 provide the necessary information to examine how the Twitter activity of Russia's covert and overt media organizations affects the online conversation about NATO during NATO exercises. The first term *NATO Exercises*IRA Tweets* is statistically significant ($p < 0.01$) and negative (-0.106), implying that IRA activities generate more negative effects during NATO exercises. Figure 3 demonstrates this effect graphically. When NATO exercises take place, the increase in IRA's online activity results in a decreased probability for positive sentiment among network users. Conversely, when there is no NATO exercise, the probability for positive sentiment about NATO among network users increases when the number of the IRA tweets increases.

Page 2898 of 3957

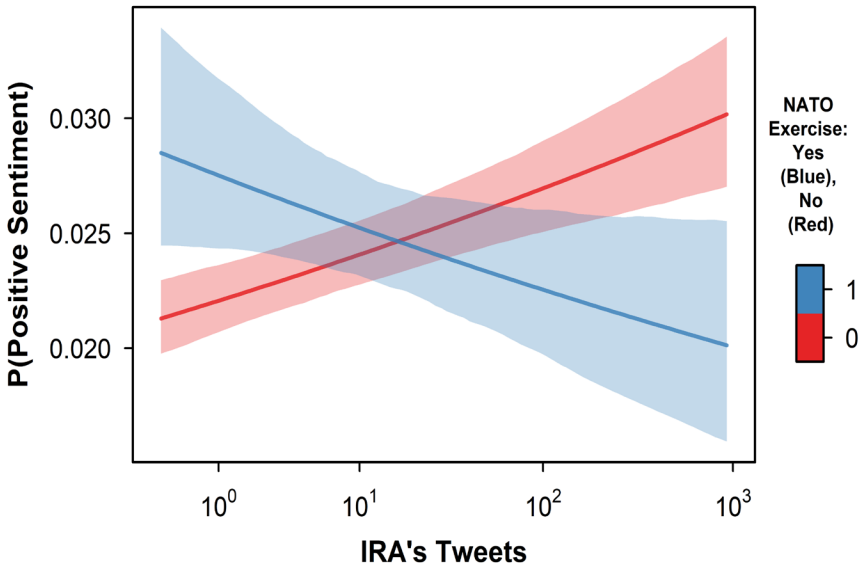


Figure 3. NATO Exercises and IRA Tweets vs. Probability of Positive Sentiment

In contrast, the term *NATO Exercise*Russian Media Tweets* is not statistically significant. This finding suggests that in the researched period, during NATO exercises, the Twitter accounts of overt Russian media probably were not as active in the online NATO conversation. This is contrary to the prediction of Hypothesis #2, which expected both overt and covert Russian media to have similarly negative effects during NATO exercises.

Hypothesis 3 *The change of sentiment during NATO exercises will be more negative if the country is closer to the borders of the Russian Federation.*

The regression results support this hypothesis. The multiplicative interaction term *NATO Exercise*Distance to Russia* is statistically significant ($p < 0.01$) and positive (0.027). Figure 4 shows that when NATO exercises take place, the probability that the average sentiment in the online conversation about NATO will be positive is lower in countries that are closer to the borders of Russia. In contrast, when there is no NATO exercise, the likelihood for positive sentiment decreases in countries that are further from Russia.

Page 2899 of 3957

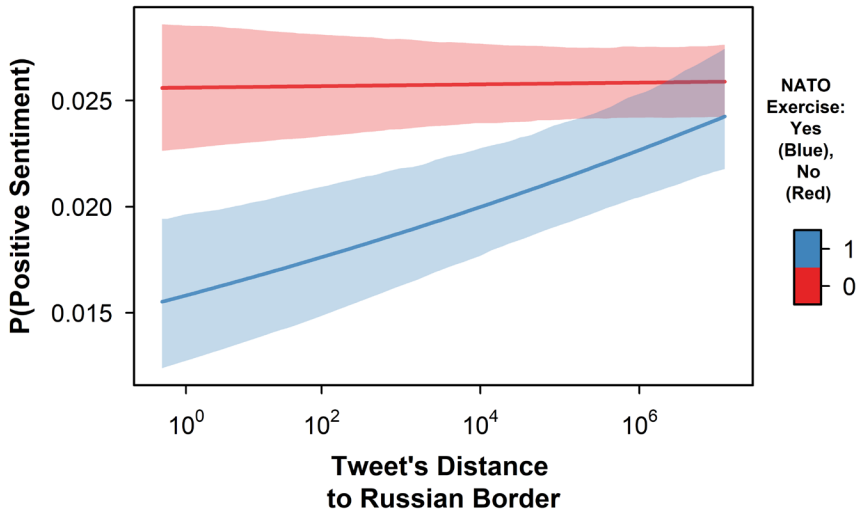


Figure 4. NATO Exercises and Distance to Russia vs. Probability of Positive Sentiment

B. NETWORK MEASURES AND RUSSIAN ONLINE INFLUENCE

Based on the models' performance scores in Table 4, it is possible to conclude that models 6, 8, and 10 have the best goodness of fit. They each have lower AIC and Bayesian Information Criteria (BIC) scores than the other three paired models presented in the table, indicating that the addition of the interaction terms decreases the models' errors.

The IRA and Russian media coefficients are statistically significant ($p < 0.01$) for all three topology measures. Those for clustering coefficient and network size are positive, for both overt and covert media activity, suggesting that these Russian entities' actions make the daily networks larger and more interconnected. The degree centralization coefficient for IRA activities is also statistically significant ($p < 0.01$). However, it is negative, which indicates that the daily network becomes less centralized with the increasing activity of Russia's covert media organizations.

The interaction term *NATO Exercise*IRA Tweets* is statistically significant ($p < 0.01$) for all three models. It is negative in the models for network size (-0.143) and clustering (-0.064), and it is positive in the case of degree centralization (0.027). The term

Page 2900 of 3957

*NATO Exercise*Russian Media Tweets* is statistically significant and positive only in the degree centralization ($p < 0.05$) and clustering ($p < 0.01$) models.

Table 4. Network Regression Models

	Network Size		Degree Centralization		Clustering Coefficient	
	Linear	Linear	Linear	Linear	Linear	Linear
	(5)	(6)	(7)	(8)	(9)	(10)
IRA's Tweets	0.167***	0.179***	-0.049***	-0.051***	0.471***	0.471***
	(0.002)	(0.002)	(0.002)	(0.002)	(0.007)	(0.007)
Russian Media Tweets	0.430***	0.349***	-0.005	0.011***	0.449***	0.274***
	(0.005)	(0.005)	(0.004)	(0.004)	(0.018)	(0.019)
Distance to Russia	0.002***	0.002***	-0.001	-0.0004	0.004*	0.004
	(0.001)	(0.001)	(0.001)	(0.001)	(0.002)	(0.002)
Total Tweets	-0.009***	-0.008***	0.002	0.001	-0.018**	-0.015**
	(0.002)	(0.002)	(0.002)	(0.001)	(0.007)	(0.007)
Political Regime	-0.001	-0.0004	0.0002	0.0001	-0.001	-0.001
	(0.0005)	(0.0005)	(0.0004)	(0.0004)	(0.002)	(0.002)
GDP per capita	-0.073***	-0.064***	0.018***	0.016***	-0.121***	-0.106***
	(0.005)	(0.005)	(0.004)	(0.004)	(0.016)	(0.016)
Population	0.012***	0.010***	-0.002	-0.002	0.022**	0.019*
	(0.003)	(0.003)	(0.002)	(0.002)	(0.011)	(0.011)
Access to Internet	0.113***	0.099***	-0.026***	-0.023***	0.191***	0.167***
	(0.006)	(0.006)	(0.004)	(0.004)	(0.020)	(0.020)
NATO Exercise		0.984***		-0.287***		0.375**
		(0.049)		(0.037)		(0.172)
NATO Exercise*IRA Tweets		-0.143***		0.027***		-0.064***
		(0.006)		(0.005)		(0.022)
NATO Exercise*Russian Media Tweets		-0.018		0.033**		0.346***
		(0.019)		(0.014)		(0.065)
Constant	3.986***	4.052***	-3.124***	-3.136***	-9.010***	-8.784***
	(0.034)	(0.032)	(0.024)	(0.024)	(0.113)	(0.113)
Observations	57,377	57,377	57,377	57,377	57,377	57,377
MAE	139.775	127.017	0.017	0.017	0.006	0.006
RMSE	216.542	209.942	0.030	0.030	0.011	0.011
AIC	117,498	111,696	80,989	80,405	257,323	255,768
BIC	117,588	111,812	81,079	80,521	257,412	255,885
Log Likelihood	-58,739	-55,835	-40,485	-40,189	-128,651	-127,871

Note: *p<0.1; **p<0.05; ***p<0.01

Page 2901 of 3957

1. Analysis of the Findings

Hypothesis 4: *IRA and Russian media activity during NATO exercises will increase the size of the daily network of users in the NATO conversation, and it will become more centralized and interconnected.*

The results from these models are partially supportive of Hypothesis 4. Figure 5 demonstrates that an increase in the number of IRA tweets is associated with a larger size of the daily user network, which supports Hypothesis 4. The blue line in the graphic is less steep than the red, which means that the IRA's actions have a weaker effect on the network size when there is a NATO exercise than when there is none. The higher starting point of the blue line is expected because the dataset for this research is based on the online NATO conversation. Thus, when such military drills occur, more Twitter accounts are likely to become active and join the online NATO communication. The multiplicative interaction term between NATO exercises and Russian media tweets is not statistically significant; thus, it is impossible to determine if there is a consistent conditional relationship between these variables. However, the coefficient for *IRA Tweets* is statistically significant ($p < 0.01$) and positive (0.349). Thus, over the entire research period, both on exercise days and non-exercise days, increased levels of *Russian Media Tweets* were associated with a larger network size in the NATO conversation, which also supports Hypothesis 4.

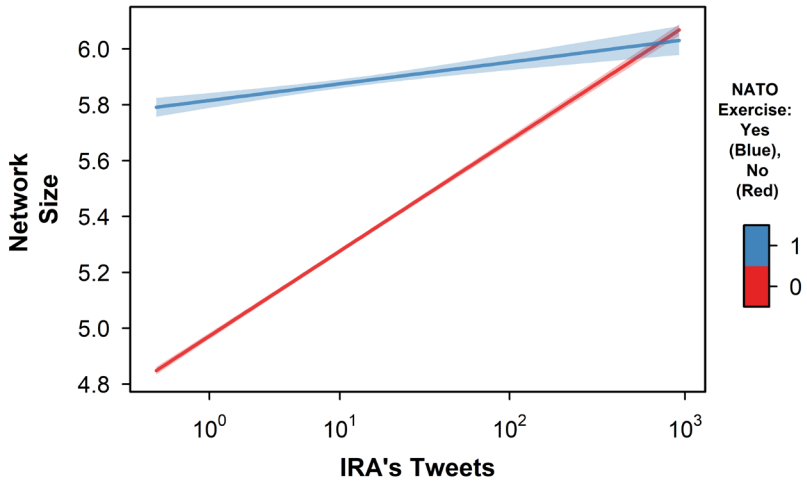


Figure 5. NATO Exercises and IRA Tweets vs. Network Size

In contrast, Model 9's results show that the online behavior of the IRA and Russia's overt media have different effects on the centralization of the daily networks. The results are partially supportive and partially contrary to Hypothesis 4. The blue lines on both graphics in Figure 6 lie below the red ones, which demonstrates that during NATO exercises, the centralization of the networks is lower than during periods without such military drills. However, the online behavior of the different types of Russian actors has an opposite effect on network centralization. When the IRA increases its online activity, centralization decreases. By contrast, when overt Russian media outlets are more active, centralization increases. Therefore, only findings about the effect of Russia's overt media organizations on network centralization support Hypothesis 4.

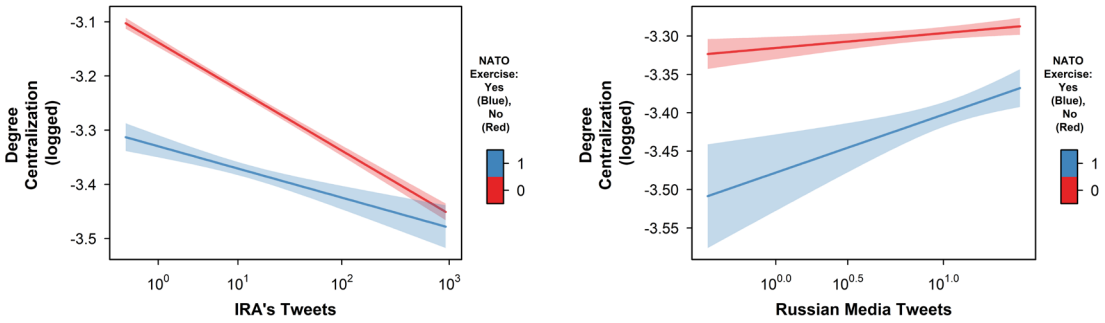


Figure 6. NATO Exercises, IRA Tweets, and Russian Media Tweets vs. Degree Centralization

The clustering coefficient is a measure of the network interconnectedness. It provides information on the degree to which the accounts in the explored daily networks have second-order ties. Figure 7 illustrates Model 10's results, which support Hypothesis 4. The clustering coefficient increases when Russia's covert and overt media organizations are more active. NATO exercises also lead to a further increase of interconnectedness in the daily networks.

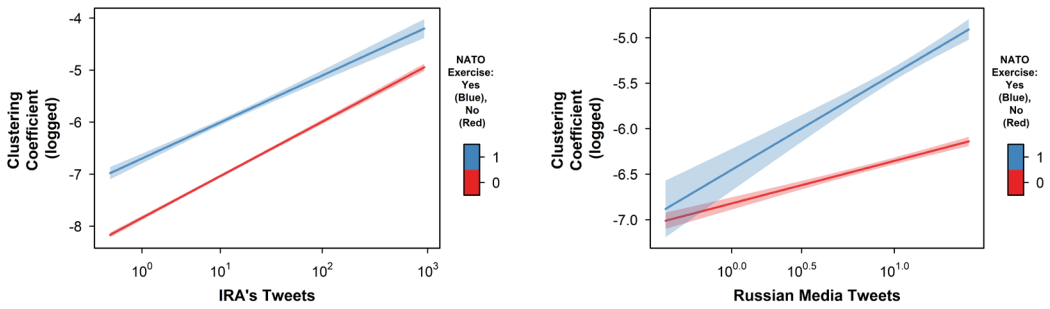


Figure 7. NATO Exercises, IRA Tweets, and Russian Media Tweets vs. Clustering Coefficient

C. DISCUSSION

In the examined period, July 2013 to August 2014, the regression analysis demonstrates that there is a statistically significant relationship between the sentiment of the online conversation about NATO and the online activities of Russia's overt and covert media organizations. At that time, the IRA was in its initial stage of formation. As Howard et al. point out, the agency used Twitter as a "training ground for the political polarization efforts."[111] The goal of IRA operatives then was to create "beachheads" in social networks by attracting followers, infiltrating online media platforms groups, and gaining credibility for its fake accounts. The prevalence of such preparatory actions could be one of the reasons why we observe the IRA's activity increasing the probability for positive sentiment in the research period, contrary to the expectations of Hypothesis 1.

Closer examination of the effects reveals that the influence potential of covert organizations is higher than that of overt media (Figure 2, Chapter V). This finding is logical because covert agencies can use fake identities or accounts to avoid attribution, infiltrate various online conversations, and implement tactics such as the "4D Approach" described by Nimmo.[112] At the same time, overt media outlets and the journalists who work for them cannot avoid this attribution, and the targeted audience can perhaps,

[111] Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012–2018," 10.

[112] Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It."

Page 2904 of 3957

therefore, more easily rebuff some of the information. This effect could explain why the regression model indicates that overt actors are weaker influencers than covert ones.

The findings about the effects of IRA and Russian media tweets during NATO exercises demonstrate that only the IRA's online activities have a statistically significant impact on sentiment. In this case, the model shows that the increase in the number of IRA tweets results in a lower probability for positive sentiment among network users. At the same time, the multiplicative interaction term combining NATO exercises with the online activity of Russia's overt media is not statistically significant. A possible interpretation of this regression result is that Russian media outlets did not target the NATO audience when the exercises took place. Another finding of the model supports this interpretation. The interaction term combining Russian exercises and IRA tweets is also not statistically significant. This result implies that the IRA's leadership probably did not make consistent use of its capabilities to manipulate the Twitter audience and influence their attitudes in favor of Russian military activities.

Although the model's results show that covert actors are more efficient in Twitter influence campaigns than overt media, the latter also have some advantages. First, they legally operate on social media platforms under their genuine identities. In this manner, the platforms cannot easily restrict their activities as long as the accounts adhere to the platforms' established rules and policies. In contrast, covert media agencies rely on fake accounts that act in violation of these regulations, and they could be banned or suspended at any time. As with all covert assets, their activity is efficient only as long as they operate hidden from their target. Second, official media companies, especially in the case of Russia, are quasi-private, and they can receive generous state funding to establish vast networks and create quality content. In return, they can be expected to coordinate and align their information policy with the ruling political elite.[113]

Both types of organizations can produce diverse online content adapted to specific social groups and geographical regions. The regression model indicates that there is a statistically significant relationship between the prevailing sentiment of tweets and their

[113] Hanley and Kuzichkin, *Russian Media Landscape*, 13–30.

Page 2905 of 3957

authors' distance from the Russian border, conditioned by whether there is a NATO exercise or not (Figure 4, Chapter V). It demonstrates that in the vicinity of the Russian border, the probability for positive tweets is much lower when a NATO exercise takes place than when there is none. The farther from Russia the tweet originates, the greater the probabilities for positive sentiment—regardless of whether a NATO exercise is in progress. This result suggests that the Twitter users closer to the Russian border are more sensitive about NATO exercises. One of the possible reasons for this effect is that the dataset includes, by definition, a significant number of Russian accounts. In addition, as the discussion in Chapter III revealed, in the countries from the so-called 'near abroad' there are many communities that share Moscow's attitude towards NATO. These social groups are more susceptible to Russian "soft power" because of their common language, ethnicity, religion, or shared history.[114] The regression results also support this explanation. Figure 8 presents a situation where a Russian military exercise occurs, showing that the probability for positive sentiment is significantly higher near the border of Russia than when there is no exercise. In the absence of an exercise, the probability is almost constant as a function of distance to Russia.

[114] Rotaru, "Forced Attraction?," 3–9.

Page 2906 of 3957

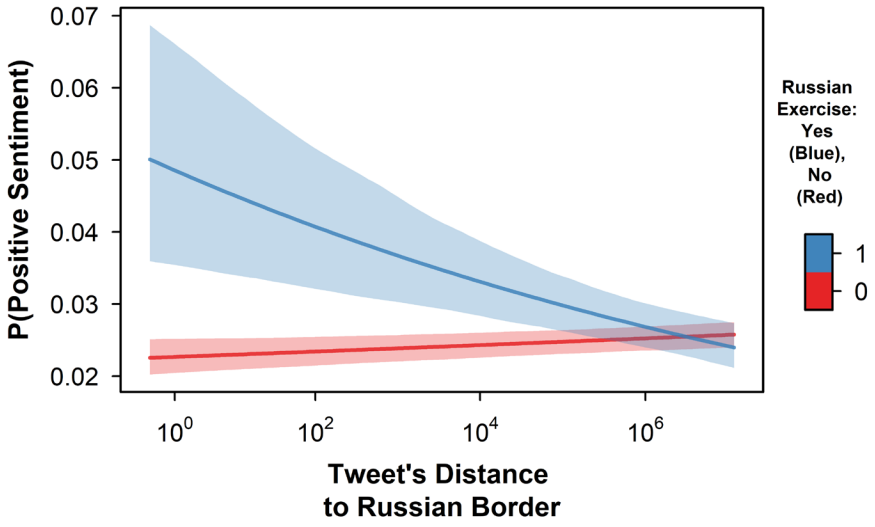


Figure 8. Russian Military Exercises and Distance to Russia vs. Probability of Positive Sentiment

The regression analysis of the daily networks of Twitter users also reveals statistically significant relations between the activity of Russia's overt and covert information agencies and network topology measures. This conclusion suggests that, during NATO exercises, these networks change their topology due to the actions of overt Russian media outlets and the covert operations of entities such as the IRA. In line with Hypothesis 4, the network becomes larger, and the clustering coefficient is higher when NATO exercises occur than in periods without military drills. Their values further increase if IRA or Russian media intensify their activity on Twitter. The finding on network enlargement can be explained by the expected appearance of new accounts engaging in the online conversation about NATO when that organization's exercises take place. The observed change in the clustering coefficient suggests that IRA and online media accounts also increase their second-order interactions. They start tweeting, mentioning, or quoting each other more frequently. This interconnectedness becomes even higher during NATO exercises. However, there is an important difference between the effect of the online activities of the IRA and the overt media outlets, as Figure 6 shows. During NATO exercises, IRA activities increase the network interconnectedness at the same rate as they do during periods without exercises. Howard et al. explain that "IRA accounts typically

operated in 'teams' of co-mentioners …[that]… tended to mention teammates far more often than non-teammates; thus, forming a number of coherent communities of interaction."[115] Similarly, Russian media organizations push the conversation to become more interconnected, but with a rate that increases substantially during NATO exercises. In other words, participants in the online conversation about NATO start retweeting, mentioning, or quoting each other more during NATO exercises.

Although the regression results for degree centralization partially support Hypothesis 4, they also reveal more specific patterns. Contrary to Hypothesis 4, the increase in IRA tweets results in a decrease in centralization. On the other hand, Russian media activity increases the centralization of the daily networks. These findings suggest that the increase in the Russian media's online activity probably makes some nodes in the network more central. This conclusion corresponds to the qualitative findings in Chapter III that several central and larger online news agencies such as RT, Sputnik, and Ruptly appear to dominate the Russian media landscape. In contrast, covert entities such as the IRA seem to represent as a more "egalitarian" network composed of what Howard et al. referred to as small "communities of interaction" with a more similar number of ties.

[115] Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012–2018," 26.

Page 2908 of 3957

VI. CONCLUSIONS

This thesis has sought to examine the conversation about NATO on Twitter and to explore the relationships between the average sentiment in that conversation and the online activities of Russia's overt and covert online media agencies. In addition to the sentiments expressed in the tweets, the thesis analyzed how the basic topology measures of the social networks hosting this conversation relate to the online activity of overt Russian media and so-called troll factories. The thesis's research period was one year, from July 1, 2013, through August 31, 2014. The focus was on the conversation about NATO that appeared on Twitter and the activity on Twitter caried out by the major Russian media outlets and the Internet Research Agency during the NATO exercises that occurred in this period. The regression analysis of the online conversation about NATO in the specified period provided evidence of a statistically significant relationship between the sentiment of the tweets and the online actions of the Russia's covert and overt agencies. Several findings follow from the tested models' results.

First, the overall sentiment of the online conversation about NATO generally becomes more positive if there is an increase in online activity by the IRA and overt Russian media. Further, the IRA's tweets have a more substantial impact on the probability for sentiment change than do tweets by Russia's traditional media outlets. Both the overt and the covert Russian actors more effectively influence positive than negative sentiments.

Second, the prevailing sentiment of the online conversation about NATO during NATO exercises becomes more negative as the online activity of covert Russian media organizations increases. When a NATO exercise takes place, an increase in the IRA's online activity results in a decreased probability for positive sentiment. By contrast, when there is no NATO exercise, the probability for positive sentiment increases when the number of IRA messages increases.

Third, the sentiment expressed in tweets during NATO exercises is generally more negative if the location of the tweet's originator is closer to the borders of the Russian Federation.

Page 2909 of 3957

Fourth, IRA and Russian media online activity during NATO exercises increases the size of the daily network of users participating in the conversation on NATO, and that network becomes less centralized and more interconnected. During NATO exercises, Russian media activities online tend to increase the centralization of the daily network. In comparison, the IRA seems to act as a more "egalitarian" network composed of small teams with a similar number of ties.

These conclusions suggest that close tracking and examination of the online activities of Russia's covert and overt media agencies can provide the necessary base for detecting ongoing information operations. However, their proper identification faces specific difficulties. First, today's social media platforms are rapidly increasing their number, making monitoring Russian online activities difficult and resource-consuming. Second, each social media platform has its own specific and often restrictive rules for sharing information about its users' behavior and how other individuals can extract and collect such data. As in the example of the Twitter API,[116] there is a limit on the number of tweets collected as well as on access to historical data.

Nonetheless, further refining of the analytical methods can overcome some of these limitations and deliver a more comprehensive outcome. These improvements should focus on several directions. First, the measurement of sentiment in tweets could include machine learning algorithms that can increase the precision of the final result. Second, the online activities of covert agencies similar to the IRA can be tracked across different online platforms by natural language processing algorithms. They have great potential to discover patterns in online communication that will enable the timely identification of trolls' accounts.

Finally, it is hoped that the results of this thesis contribute to our better understanding of Russian information operations. These results indicate that the activities of Russia's covert and overt media agencies can effectively influence online conversation and shape public perception. Although the thesis focuses on the narrow topic of NATO

116 Twitter, "Twitter API Documentation," February 27, 2022, https://developer.twitter.com/en/docs/twitter-api.

Page 2910 of 3957

exercises, its results could have implications for other significant events such as elections, referendums, or conflicts such as the February 2022 war between Russia and Ukraine. The results demonstrate that the online activities of companies such as the IRA need close monitoring. The thesis's findings show that the IRA's actions more substantially affect online conversation than do channels operated by Russia's overt media.

Moreover, the events during the current war between Ukraine and Russia suggest that the role of covertly operating troll networks can be even more significant in a time of crisis or conflict. The European Union imposed restrictions on RT and Sputnik media platforms and publicly labeled them as sources of disinformation in 2022.[117] As a result, major online platforms including Twitter, Facebook, and Instagram declared that they will comply with the sanctions and will prevent these Russian media networks from posting content.[118] Such restrictions will reduce the ability of these covert influencers to interact with targeted audiences and diminish their role in the information operations. In this situation, only networks covertly established by trolls can continue to operate and affect the information environment. Thus, preventive measures against information operations must include constant monitoring and timely counteraction of such networks as well.

[117] Foo Yun Chee, "EU Bans RT, Sputnik over Ukraine Disinformation," Reuters, March 2, 2022, sec. Europe, https://www.reuters.com/world/europe/eu-bans-rt-sputnik-banned-over-ukraine-disinformation-2022-03-02/.

[118] Elizabeth Culliford, "Twitter to Comply with EU Sanctions on Russian State Media," Reuters, March 2, 2022, sec. Technology, https://www.reuters.com/technology/twitter-comply-with-eu-sanctions-russian-state-media-2022-03-02/.

THIS PAGE INTENTIONALLY LEFT BLANK

Page 2912 of 3957

LIST OF REFERENCES

Arif, Ahmer, Leo Graiden Stewart, and Kate Starbird. "Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse." *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (November 2018): 1–27. https://doi.org/10.1145/3274289.

Awan, Imran. "Cyber-Extremism: Isis and the Power of Social Media." *Society* 54, no. 2 (April 2017): 138–49. https://doi.org/10.1007/s12115-017-0114-0.

Beauchamp-Mustafaga, Nathan, and Michael S. Chase. *Borrowing a Boat Out to Sea: The Chinese Military's Use of Social Media for Influence Operations*. Policy Papers. Washington, DC: Johns Hopkins University School of Advanced International Studies, 2019.

Bennett, W. Lance, and Steven Livingston. "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions." *European Journal of Communication* 33, no. 2 (April 2018): 122–39. https://doi.org/10.1177/0267323118760317.

Bernatis, Vincent. "The Taliban and Twitter: Tactical Reporting and Strategic Messaging." *Perspectives on Terrorism* 8, no. 6 (2014): 25–35. http://www.jstor.org/stable/26297291.

Beskow, David M., and Kathleen M. Carley. *Bot-Hunter: A Tiered Approach to Detecting & Characterizing Automated Activity on Twitter*. Pittsburgh, PA: Carnegie Mellon University, 2018. https://www.researchgate.net/publication/326606376_Bot-hunter_A_Tiered_Approach_to_Detecting_Characterizing_Automated_Activity_on_Twitter.

———. "Its All in a Name: Detecting and Labeling Bots by Their Name." *Computational and Mathematical Organization Theory* 25, no. 1 (March 2019): 24–35. https://doi.org/10.1007/s10588-018-09290-1.

———. "Social Cybersecurity: An Emerging National Security Requirement." *Military Review*, March-April (2019). https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MA-2019/Beskow-Carley-Social-Cyber.pdf.

Blei, David M., Andrew Ng, and Michael Jordan. "Latent Dirichlet Allocation." *Journal of Machine Learning Research* 3 (January 2003): 993–1022.

Brzezinski, Jan J., and Nicholas Varangis. "The NATO-Russia Exercise Gap." *Atlantic Council* (blog), February 23, 2015. https://www.atlanticcouncil.org/blogs/natosource/the-nato-russia-exercise-gap/.

Page 2913 of 3957

Carley, Kathleen M., Guido Cervone, Nitin Agarwal, and Huan Liu. "Social Cyber-Security." In *Social, Cultural, and Behavioral Modeling*, edited by Robert Thomson, Christopher Dancy, Ayaz Hyder, and Halil Bisgin, Vol. 10899. Lecture Notes in Computer Science. Cham, Switzerland: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-93372-6_42.

Carley, Kathleen M., Jana Diesner, Jeffrey Reminga, and Maksim Tsvetovat. "Toward an Interoperable Dynamic Network Analysis Toolkit." *Decision Support Systems* 43, no. 4 (August 2007): 1324–47. https://doi.org/10.1016/j.dss.2006.04.003.

Center for Systemic Peace. "Polity5 Project, Political Regime Characteristics and Transitions, 1800–2018," April 23, 2020. https://www.systemicpeace.org/inscrdata.html.

Chan, Elvis M. "Fighting Bears and Trolls: An Analysis of Social Media Companies and U.S. Government Efforts to Combat Russian Influence Campaigns during the 2020 U.S. Elections." Master's thesis, Naval Postgraduate School, 2021. http://hdl.handle.net/10945/68309.

Charon, Paul, and Jean-Baptist Jeangène Vilmer. *Chinese Influence Operations: A Machiavellian Moment*. Paris, France: Ministry for the Armed Forces, Institute for Strategic Research, 2021. https://www.irsem.fr/report.html.

Chee, Foo Yun. "EU Bans RT, Sputnik over Ukraine Disinformation." Reuters, March 2, 2022, sec. Europe. https://www.reuters.com/world/europe/eu-bans-rt-sputnik-banned-over-ukraine-disinformation-2022-03-02/.

Csardi, Gabor, and Tamas Nepusz. "The Igraph Software Package for Complex Network Research." *InterJournal Complex Systems* (2006): 1695. https://igraph.org.

Culliford, Elizabeth. "Twitter to Comply with EU Sanctions on Russian State Media." Reuters, March 2, 2022, sec. Technology. https://www.reuters.com/technology/twitter-comply-with-eu-sanctions-russian-state-media-2022-03-02/.

Cunningham, Daniel. Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis. Lanham, MD: Rowman & Littlefield, 2016.

Ferrara, Emilio. *Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election*. Los Angeles, CA: University of Southern California, Information Sciences Institute, 2017. https://ssrn.com/abstract=2995809.

Garrett, R. Kelly. "Echo Chambers Online?: Politically Motivated Selective Exposure among Internet News Users." *Journal of Computer-Mediated Communication* 14, no. 2 (January 2009): 265–85. https://doi.org/10.1111/j.1083-6101.2009.01440.x.

Page 2914 of 3957

Gerasimov, Valery "The Science's Value is in the Prediction." *Military Industrial Courier* no. 8(476), 02/27-03/05/2013, https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf, accessed February 1, 2022

Golovchenko, Yevgeniy, Mareike Hartmann, and Rebecca Adler-Nissen. "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation." *International Affairs* 94, no. 5 (September 1, 2018): 975–94. https://doi.org/10.1093/ia/iiy148.

Hanley, Monica, and Andrey Kuzichkin. *Russian Media Landscape:Structures, Mechanisms, and Technologies of Information Operations*. Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2021. https://stratcomcoe.org/publications/russian-media-landscape-structures-mechanisms-and-technologies-of-information-operations/215.

Helmus, Todd C. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. Research Report (Rand Corporation), RR-2237-OSD. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2237.html.

Howard, Philip N., and Samantha Bradshaw. "The Global Organization of Social Media Disinformation Campaigns." *The Journal of International Affairs, SIPA* 71 (September 2018). https://jia.sipa.columbia.edu/global-organization-social-media-disinformation-campaigns.

Howard, Philip N., Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. "The IRA, Social Media and Political Polarization in the United States, 2012–2018." *Oxford, UK: University of Oxford, Computational Propaganda Research Project, 2019*, October 2019, 48. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs.

Hu, Minqing, and Bing Liu. *Mining and Summarizing Customer Reviews*. Research Track Paper. Chicago, IL: University of Illinois at Chicago, 2004.

Kania, Elsa. "The PLA's Latest Strategic Thinking on the Three Warfares." *China Brief* 16, no. 13 (August 2016). https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/.

Lee, Kyumin, Brian David Eoff, and James Caverlee. "Seven Months with the Devils: A Long-Term Study of Content Polluters on Twitter." In *Fifth International AAAI Conference on Weblogs and Social Media*, 185–92. Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media. College Station, TX: Texas A&M University, 2011.

Linvill, Darren L., and Patrick L. Warren. "Troll Factories: Manufacturing Specialized Disinformation on Twitter." *Political Communication* 37, no. 4 (February 2020): 447–67. https://doi.org/10.1080/10584609.2020.1718257.

Page 2915 of 3957

———. *Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building*. Clemson, SC: Clemson University, 2018. http://pwarren.people.clemson.edu/Linvill_Warren_TrollFactory.pdf.

Mejias, Ulises A., and Nikolai E. Vokuev. "Disinformation and the Media: The Case of Russia and Ukraine." *Media, Culture & Society* 39, no. 7 (October 2017): 1027–42. https://doi.org/10.1177/0163443716686672.

Mihaylov, Todor, Georgi Georgiev, and Preslav Nakov. "Finding Opinion Manipulation Trolls in News Community Forums." In *Proceedings of the Nineteenth Conference on Computational Natural Language Learning*, 310–14. Beijing, China: Association for Computational Linguistics, 2015. https://doi.org/10.18653/v1/K15-1032.

Morales, James. "Assessing Anti-American Sentiment through Social Media Analysis." Master's thesis, Naval Postgraduate School, 2016. http://hdl.handle.net/10945/51587.

Morstatter, Fred, Jürgen Pfeffer, Huan Liu, and Kathleen M. Carley. "Is the Sample Good Enough? Comparing Data from Twitter's Streaming API with Twitter's Firehose." *ICWSM 2013*, June 2013. http://arxiv.org/abs/1306.5204.

Nekmat, Elmie. "Prosocial vs. Trolling Community on Facebook: A Comparative Study of Individual Group Communicative Behaviors." *International Journal of Communication* 12 (2018): 1–22. http://ijoc.org.

Nimmo, Ben. "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It." *Central European Policy Institute* 15 (2015). https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

Panarin, I. N. *Informatsionnaia Voina i Geopolitika*. [Information Warfare and Geopolitics] Velikii Put′. Moskva: Pokolenie, 2006.

Pomerantsev, Peter, and Michael Weiss. *The Menace of Unreality:How the Kremlin Weaponizes Information, Culture and Money*. The Interpreter. New York, NY: The Institute of Modern Russia, 2014. https://www.almendron.com/tribuna/wp-content/uploads/2015/08/The_Menace_of_Unreality_Final.pdf.

Qi, SiHua, Lulwah AlKulaib, and David A. Broniatowski. "Detecting and Characterizing Bot-Like Behavior on Twitter." In *Social, Cultural, and Behavioral Modeling: 11th International Conference*, SBP-BRiMS 2018. Washington, DC, USA, July 10–13, 2018.

Qiao, Liang, and Xiangsui Wang. *Unrestricted Warfare*. 2nd ed. Wuhan, China: Chongwen, 2011.

Page 2916 of 3957

Reynolds, Nathaniel. *Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group*. The Return of the Global Russia. Washington, DC: Carnegie Endowment for International Peace, 2019. https://carnegieendowment.org/files/GlobalRussia_NateReynolds_Vagner.pdf.

Rotaru, Vasile. "Forced Attraction?: How Russia Is Instrumentalizing Its Soft Power Sources in the 'Near Abroad.'" *Problems of Post-Communism* 65, no. 1 (January 2, 2018): 37–48. https://doi.org/10.1080/10758216.2016.1276400.

Selph, Gregory R., Michael H. Crain, and Andrew Anderson. "Measuring Sentiment Response to Collective Violence through Social Media." Master's thesis, Naval Postgraduate School, 2018. http://hdl.handle.net/10945/66275.

Shu, Kai, Amy Sliva, Suhang Wang, Jiliang Tang, and Huan Liu. *Fake News Detection on Social Media: A Data Mining Perspective*. Vol. 19, 2017. https://arxiv.org/pdf/1708.01967.pdf.

The Joint Chiefs of Staff. *Joint Publication 3-13: Information Operations*. JP 3-13. Washington, DC: Joint Chief of Staff, 2012. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

U.S. Congress. House of Representatives. *The Internet Research Agency's Handles as of June 2018*. Washington, DC: U.S. House of Representatives Permanent Select Committee on Intelligence, 2018. https://intelligence.house.gov/uploadedfiles/ira_handles_june_2018.pdf.

———. *Russia Investigative Task Force: Testimony before Permanent Select Committee on Intelligence*, 115th Cong. (2017) (statement of Sean J. Edgett Acting General Counsel, Twitter, Inc). Accessed February 4, 2022. https://docs.house.gov/meetings/IG/IG00/20171101/106558/HHRG-115-IG00-Wstate-EdgettS-20171101.pdf.

Twitter. "Twitter API Documentation," February 27, 2022. https://developer.twitter.com/en/docs/twitter-api.

Uyheng, Joshua, Thomas Magelinski, Ramon Villa-Cox, Christine Sowa, and Kathleen M. Carley. "Interoperable Pipelines for Social Cyber-Security: Assessing Twitter Information Operations during NATO Trident Juncture 2018." *Computational and Mathematical Organization Theory* 26, no. 4 (December 2020): 465–83. https://doi.org/10.1007/s10588-019-09298-1.

Weisburd, Andrew, Clint Watts, and Jim Berger. "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy." War on the Rocks, November 6, 2016. https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

Page 2917 of 3957

World Bank. “World Development Indicator.” Accessed February 27, 2022. https://datatopics.worldbank.org/world-development-indicators/.

Zhou, Xinyi, Reza Zafarani, Kai Shu, and Huan Liu. “Fake News: Fundamental Theories, Detection Strategies and Challenges.” In *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining*, 836–37. Melbourne, ,Australia: ACM, 2019. https://doi.org/10.1145/3289600.3291382.

Page 2918 of 3957

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

Page 2919 of 3957

TC 18-06

Special Forces
Guide to Information Operations

March 2013

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies and their contractors only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This determination was made on 30 March 2012. Other requests for this document must be referred to Commander, United States Army John F. Kennedy Special Warfare Center and School, ATTN: AOJK-CDI-SF, 3004 Ardennes Street, Stop A, Fort Bragg, NC 28310-9610.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

FOREIGN DISCLOSURE RESTRICTION (FD 6): This publication has been reviewed by the product developers in coordination with the United States Army John F. Kennedy Special Warfare Center and School foreign disclosure authority. This product is releasable to students from foreign countries on a case-by-case basis only.

Headquarters, Department of the Army

This publication is available at Army Knowledge Online
(https://armypubs.us.army.mil/doctrine/index.html).
To receive publishing updates, please subscribe at
http://www.apd.army.mil/AdminPubs/new_subscribe.asp.

TC 18-06

Training Circular
No. 18-06

Headquarters
Department of the Army
Washington, DC, 22 March 2013

Special Forces
Guide to Information Operations

Contents

		Page
	PREFACE	**vi**
Chapter 1	**FUNDAMENTALS**	**1-1**
	Information Operations	1-2
	The Information Environment	1-3
	Information Superiority	1-4
	Information Operations Capabilities	1-5
	Considerations	1-5
	Conclusion	1-5
Chapter 2	**INFORMATION OPERATIONS CAPABILITIES AND TACTICS**	**2-1**
	Operations Security	2-2
	Military Deception	2-5
	Military Information Support Operations	2-11
	Electronic Warfare	2-15
	Computer Network Operations	2-16
	Combat Camera	2-17
	Local Populace and Key-Leader Engagements	2-19
	Countering Adversary Information Activities	2-26
	Rewards Programs	2-29
	Civil-Military Operations	2-30
	Public Affairs	2-31
	Defense Support to Public Diplomacy	2-31

Distribution Restriction: Distribution authorized to U.S. Government agencies and their contractors only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This determination was made on 30 March 2012. Other requests for this document must be referred to Commander, United States Army John F. Kennedy Special Warfare Center and School, ATTN: AOJK-CDI-SF, 3004 Ardennes Street, Stop A, Fort Bragg, NC 28310-9610.

Destruction Notice: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Foreign Disclosure Restriction (FD 6): This publication has been reviewed by the product developers in coordination with the United States Army John F. Kennedy Special Warfare Center and School foreign disclosure authority. This product is releasable to students from foreign countries on a case-by-case basis only.

Page 2922 of 3957

Chapter 3 **PLANNING INFORMATION OPERATIONS 3-1**
The Staff Estimate for Information Operations 3-2
Planning Considerations During Mission Analysis 3-2
Mission Analysis Work Sheet 3-7
Course of Action Development 3-7
Considerations 3-19
Consequence Management 3-19

Chapter 4 **EXECUTION OF INFORMATION OPERATIONS 4-1**
Monitoring 4-1
Evaluating 4-1
Adjusting 4-3
Reporting 4-8

Chapter 5 **INTELLIGENCE SUPPORT TO INFORMATION OPERATIONS 5-1**
Information Operations and the Intelligence Cycle 5-2
Intelligence “Push” and “Pull” 5-2
Requests for Information 5-3
Intelligence Preparation of the Operational Environment 5-3
Visualizing the Information Environment 5-3
The Combined Information Overlay 5-5
Adversary Operations in the Information Environment 5-6
Templating Using Center-of-Gravity Analysis 5-7
Adversary Activities in the Information Environment 5-9
Considerations 5-9

Appendix A **PLANNING AIDS A-1**

Appendix B **TACTICAL DECEPTION AID B-1**

Appendix C **TACTICAL OPERATIONS SECURITY AID C-1**

Appendix D **MEDIA ASSESSMENT AID D-1**

Appendix E **CONDUCTING FACE-TO-FACE MEETINGS E-1**

Appendix F **HOW TO USE TRANSLATORS F-1**

GLOSSARY Glossary-1

REFERENCES References-1

INDEX Index-1

Page 2923 of 3957

Figures

Figure 1-1. Information operations capabilities 1-2
Figure 1-2. Information environment 1-3
Figure 2-1. Information operations employment 2-1
Figure 2-2. Summary of the five-step operations security process 2-3
Figure 2-3. Useful format for determining risk to critical information 2-4
Figure 2-4. Useful format for planning operations security tasks 2-5
Figure 2-5. Military deception usage 2-5
Figure 2-6. Example of a military deception work sheet 2-9
Figure 2-7. Five-step computer network operations planning process 2-17
Figure 2-8. Example message (paired to themes) 2-22
Figure 2-9. Example message development matrix 2-22
Figure 2-10. Example of a face-to-face engagement work sheet 2-25
Figure 2-11. Mutual support within information operations capabilities 2-32
Figure 2-12. Potential conflicts within information operations capabilities 2-36
Figure 2-13. Support roles of information operations, civil-military operations, public affairs, defense support to public diplomacy, and combat camera 2-39
Figure 3-1. Information operations staff estimate 3-3
Figure 3-2. Example graphic information operations estimate 3-4
Figure 3-3. Sample information operations asset list 3-5
Figure 3-4. Example of information content and flow organization 3-6
Figure 3-5. Mission analysis work sheet 3-7
Figure 3-6. Information advantage work sheet 3-9
Figure 3-7. Examples of information superiority 3-9
Figure 3-8. Effects for information operations 3-11
Figure 3-9. Tasks for information operations capabilities 3-13
Figure 3-10. Example of an information operations planning work sheet 3-14
Figure 3-11. Example information operations concept of support sketch 3-15
Figure 3-12. Format for a five-paragraph information operations annex (Army orders format) 3-16
Figure 3-13. Example of a format for a matrix information operations annex (Army orders format) 3-17
Figure 3-14. Example 1 of an information operations execution matrix 3-18
Figure 3-15. Example 2 of an information operations execution matrix 3-19
Figure 4-1. Sources of data collection 4-3
Figure 4-2. Example of an assessment graphic 4-3
Figure 4-3. Battle drill format for insurgent-related violence 4-6
Figure 4-4. Abbreviated staff battle drill 4-7
Figure 5-1. Visualization of the information environment 5-4
Figure 5-2. Example combined information overlay 5-6

Figure 5-3. Example center-of-gravity analysis and the use of the CARVER process to rank and plot critical vulnerabilities in the information environment 5-7
Figure A-1. Information operations working group duties and responsibilities A-2
Figure A-2. Sample intelligence update format A-4
Figure A-3. Sample assessment update format A-4
Figure A-4. Sample operations update format A-5
Figure A-5. Sample operations calendar A-6
Figure A-6. Information operations planning aid A-6
Figure A-7. Relationship between intelligence preparation of the operational environment and information operations A-7
Figure A-8. Sample center-of-gravity analysis A-7
Figure A-9. Sample combined information overlay A-9
Figure A-10. Mission-to-task products A-9
Figure A-11. Sample information operations mission and tasks (tactical level) A-10
Figure A-12. Sample course-of-action sketch A-10
Figure A-13. Mission analysis and information operations A-11
Figure A-14. Example of a mission-analysis work sheet A-12
Figure A-15. Example of an information operations asset/capability matrix A-13
Figure A-16. Example of a fact and assumption analysis A-14
Figure A-17. Example of a commander's critical information requirement and essential elements of information for information operations A-15
Figure A-18. Information environment A-15
Figure A-19. Information environment variances by level of war A-16
Figure A-20. Sample information environment effects matrix A-17
Figure A-21. Combined information operations overlay template A-18
Figure A-22. Example of a combined information operation A-19
Figure A-23. Relationship between center-of-gravity analysis and the planning process A-20
Figure A-24. Decisionmaking template A-20
Figure A-25. Information infrastructure template A-21
Figure A-26. Information tactics template A-21
Figure A-27. Information situation template A-22
Figure A-28. Example of an information operations estimate format A-23
Figure A-29. Graphic information operations estimate A-24
Figure A-30. Example of an execution matrix A-25
Figure B-1. Deception planning process overview B-1
Figure B-2. Deception estimate format B-2
Figure C-1. Operations security and the planning process C-1
Figure C-2. Example of a counterintelligence template C-2
Figure D-1. Media analysis process D-2
Figure D-2. Media theme assessment diagram D-3

Figure D-3. Sample media report D-4
Figure D-4. Consequence-management tracker format D-5
Figure D-5. Example of a consequence-management tracker D-5

Page 2926 of 3957

Preface

Information operations (IO) are essential to the successful execution of military operations. The goal of IO is to gain and maintain information superiority that translates to a competitive edge in the information environment.

Users of Training Circular (TC) 18-06, *Special Forces Guide to Information Operations,* must be familiar with the decisionmaking process established in Army Doctrine Publication (ADP) 5-0, *The Operations Process,* and the operational concepts established in ADP 3-0, *Unified Land Operations.*

PURPOSE

This TC serves as a guide to describe the fundamentals of how to incorporate IO at the tactical and operational level. Appendixes A through F offer tactics, techniques, and procedures (TTP) Special Forces (SF) Soldiers can use to analyze and plan information operations. This TC implements Army and joint IO doctrine established in FM 3-13, *Inform and Influence Activities,* and Joint Publication (JP) 3-13, *Information Operations.*

This TC reinforces the definition of IO used by Army forces: IO employs the core capabilities of electronic warfare (EW), computer network operations (CNO), Military Information Support operations (MISO), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to affect or defend information and information systems and to influence decisionmaking. This TC is specifically targeted for SF; however, it is also useful to Army special operations forces (ARSOF) and the Army in understanding how SF employs IO.

SCOPE

TC 18-6 significantly affects the conduct of full-spectrum operations as an SF-common skill set that applies to offensive as well as defensive operations. This TC links to a broad variety of doctrine to provide a rudimentary understanding of IO.

APPLICABILITY

This publication applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the United States Army Reserve, unless otherwise stated.

ADMINISTRATIVE INFORMATION

The proponent of this manual is the United States Army John F. Kennedy Special Warfare Center and School (USAJFKSWCS). Reviewers and users of this manual should submit comments and recommended changes on Department of the Army Form (DA Form) 2028 (Recommended Changes to Publications and Blank Forms) to Commander, United States Army John F. Kennedy Special Warfare Center and School, ATTN: AOJK-CDI-SF, 3004 Ardennes Street, Stop A, Fort Bragg, NC 28310-9610.

Page 2927 of 3957

Chapter 1

Fundamentals

IO should be viewed as an element of combat power, focused when and where it best supports the operation. As with other elements of combat power, there is no universal formula for the application of IO. Mission, enemy, terrain and weather, troops and support available-time available, and civil considerations are the major determinants.

The purpose of IO is to achieve and maintain information superiority or advantage over the adversary at a particular time and place. To achieve an information advantage, an SF unit must understand the characteristics of the information environment in its operational area. The unit must also understand how adversary and third-party organizations use information to achieve their objectives.

Operation VALHALLA

Operation VALHALLA was a typical SF-type mission. The Jaish al-Mahdi death squad was tracked down because of the especially brutal murders of a number of civilians and Iraqi troops. On 26 March 2006, a battalion from the 10th Special Forces Group (Airborne) (SFG[A]), as part of the Combined Joint Special Operations Task Force—Arabian Peninsula (CJSOTF-AP), along with the Iraqi special forces unit it was training, engaged the Jaish al-Mahdi at their compound. The mission was successful with no friendly casualties. There were approximately 17 Jaish al-Mahdi members killed, a weapons cache found and destroyed, a badly abused hostage found and rescued, and approximately 16 Jaish al-Mahdi members detained. A combat-camera element, along with some SF Soldiers wearing helmet cameras, recorded the entire operation.

By the time the SF and Iraqi forces returned to their compound, roughly an hour after leaving the site of the firefight, someone had moved the Jaish al-Mahdi bodies. The guns of the Jaish al-Mahdi fighters were taken, and their bodies were put back inside the compound so it appeared as if the Jaish al-Mahdi members were killed while engaging in prayer. Someone then photographed the bodies in these new poses, and loaded the images onto the web, along with a press release explaining that American Soldiers had entered a mosque and killed men peacefully at prayer. This was done in under an hour. Both the American and Arab media picked up the story almost immediately. The United States (U.S.) did not release a statement until 70 hours after the operation. During the resulting investigation, which took close to a month, the SF Soldiers, who had soundly and justly defeated their adversary, were made combat ineffective by a cell-phone camera.

Paraphrased from an article written by Cori E. Dauber
Military Review
January–February 2009

Page 2928 of 3957

Key terms used throughout this chapter are defined below:

- *IO.* The integrated employment, during military operations, of information related capabilities in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries and potential adversaries while protecting our own.
- *Information environment.* The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.
- *Information superiority.* The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

INFORMATION OPERATIONS

1-1. The possession and use of information can provide a marked advantage to one military force over another. SF units expend significant time and resources to collect, process, and internally transfer information for the purpose of mission command. Without adequate and accurate information, an SF unit is unlikely to successfully accomplish its mission or meet its objectives.

1-2. Stated in the simplest way, IO is the use of information to gain an advantage over an opponent. Such an advantage, known as information superiority, is achieved by a series of actions by military and other forces to impact both enemy forces and the operational area. To gain the advantage over the adversary, an SF unit should use any available capability at its disposal, whether doctrinal or not, to achieve information superiority at specific times and places in the operation. Figure 1-1 describes the five core capabilities, five supporting capabilities, and three related capabilities of IO. IO forces can affect data, information, and knowledge in three basic ways by—

- Taking specific psychological, electronic, or physical actions that add, modify, or remove information from the environment of various individuals or groups of decisionmakers.
- Taking actions to affect the infrastructure that collects, communicates, processes, and stores information in support of targeted decisionmakers.
- Influencing the way people receive, process, interpret, and use data, information, and knowledge.

Core Capabilities	*Supporting Capabilities*	*Related Capabilities*
Electronic Warfare (EW)	Information Assurance (IA)	Public Affairs (PA)
Computer Network Operations (CNO)	Physical Security	Civil-Military Operations (CMO)
Military Information Support Operations (MISO)	Physical Attack	Defense Support to Public Diplomacy (DSPD)
Military Deception (MILDEC)	Counterintelligence (CI)	
Operations Security (OPSEC)	Combat Camera (COMCAM)	

Figure 1-1. Information operations capabilities

1-3. Thinking about IO within the terms of this doctrinal construct may do injustice to IO's true capabilities. Field experience shows that IO is less about doctrinal capabilities than it is about understanding that every military action has the potential to positively and negatively affect populations within the operational environment. In the end, everything an SF unit or detachment does or does not do can affect the information environment, and any asset that affects information content and flow is a possible contributor to (or detractor from) achieving the mission or the commander's objective. For this reason, IO should include any methods and means that can affect information content and flow, and target perceptions and behaviors in the operating area.

THE INFORMATION ENVIRONMENT

1-4. To use IO properly, SF commanders and staffs must understand the characteristics of the information environment in their operational area. Unfortunately, visualization of the information environment is challenging because the most important aspects of the information environment—information content and flow—cannot be seen the same way we see terrain. This is because information is an abstract concept and the information environment is largely nonphysical.

1-5. The information environment has existed since humans first began communicating. That is because information resides in the minds of humans, is communicated between humans, and is the end result of how humans perceive themselves and their surroundings. To explain this phenomenon, most practitioners of IO use a three-dimensional model of the information environment (Figure 1-2).

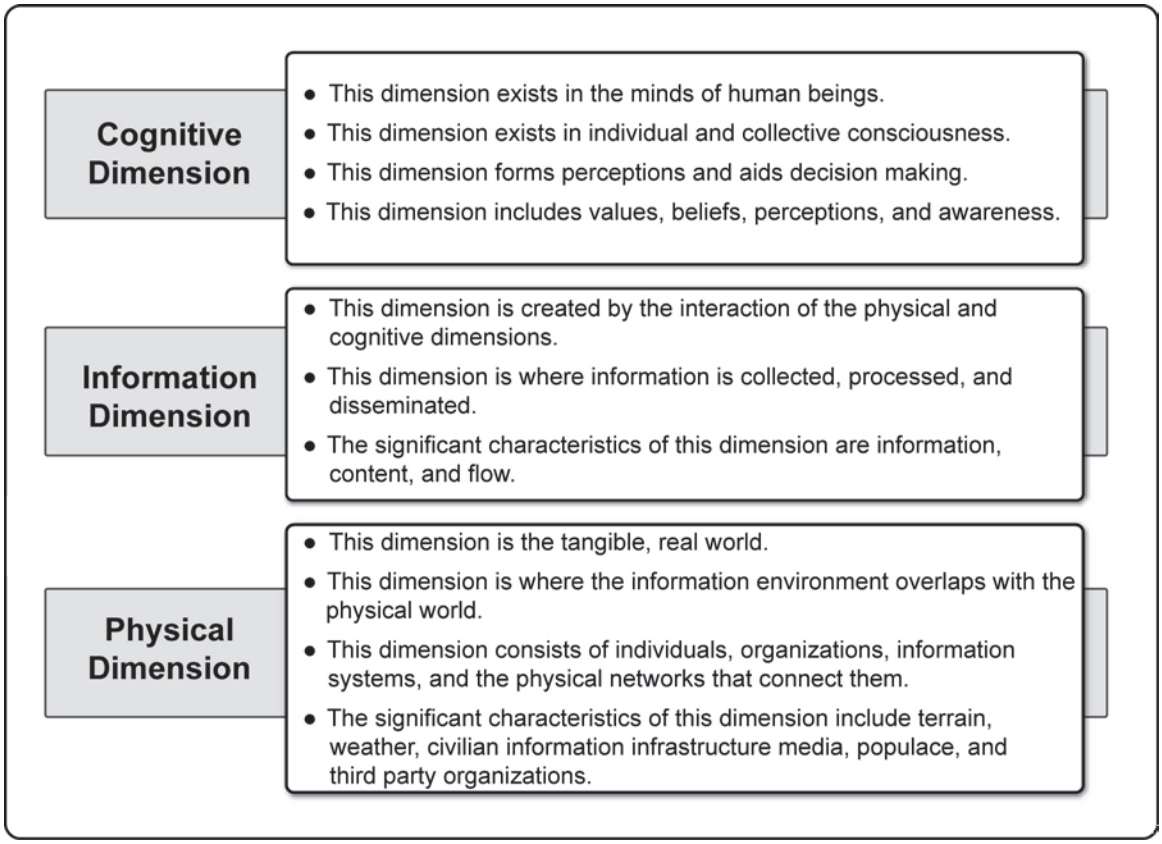


Figure 1-2. Information environment

1-6. When taken together, the information environment's three dimensions explain how the creation and flow of information causes real-world effects by converting real-world (physical) situations into human perceptions that form the basis of individual and organizational behavior. Unfortunately, although the effects of information are observable, the cause—information content and flow—is largely invisible. However, analysis of the information environment's dimensions can explain the disposition of the information environment in any specific operational area and its impact on SF operations. Broad considerations include the following:

- *The information environment is not uniform.* Physical features of the operational area (for example, terrain, information infrastructure, population demographics, and so on) determine the topography of an information environment and the cognitive aspects of the people and organizations present in the area (for example, their collective values, beliefs, and perceptions). The interactions of these factors form distinct subinformation environments, or areas in which the information environment's characteristics are notably different from those of adjacent areas.

Analysis of a specific operational area can identify subinformation environments and their effect on SF operations. SF units must anticipate having to employ IO differently within each subinformation environment.

- *Information content and flow are variable.* The relevance or importance of information changes according to the needs of the various population groups and organizations. For example, people located in an area devastated by a natural disaster desire information concerning humanitarian assistance, whereas the populace in an insurgent-infested area is primarily interested in information related to security. The task for SF units is to determine what information in the operational area is important to the mission and then to identify and track its primary themes and flow, just as SF units observe and monitor the presence of enemy forces.
- *The information environment's character changes by the level of war and mission.* The information environment becomes less tangible and more conceptual as operations move from the tactical to the strategic. At the tactical level, information flow is primarily by short-range communications systems and observable means, such as graffiti and banners. What people see of their physical surroundings is critical to their situational awareness, perceptions, and behavior. On the other end of the spectrum—the strategic level—the information environment is impacted less by physical features and more by abstract ideas, ideologies, and philosophies. Information flow is not terrain-dependent, extending well over the horizon by long-range and mass-communications systems. Finally, the assigned mission (for example, combat, peacekeeping, humanitarian assistance, and so on) is a critical determinant of an SF unit's relationship to its information environment because it establishes the relative importance of the information environment's specific characteristics to the conduct of operations. For example, in conventional combat, the physical information infrastructure in the operational area is often a dominant characteristic because of its potential use by the enemy. In counterinsurgency missions, populace support (a cognitive aspect of the information environment) is a critical characteristic because of its importance to enemy and friendly operations.

1-7. To impact the information environment, an SF unit must identify subinformation environments and information nodes in its operating area. Subinformation environments are areas in which the information environment's characteristics and effects are notably different from those of adjacent areas. Information nodes are places, persons, or infrastructure that shape information content and flow by creating or transmitting information into the surrounding area. It is important to note that information nodes can change from day to day so what worked one day may not necessarily work the next.

1-8. Operations in the information environment are asymmetrical and not benign, often favoring one side over another. Opposing forces use the information environment just as they use the physical environments of air, land, and sea to place their enemy at a disadvantage and to achieve their objectives. Furthermore, U.S. adversaries do not use the information environment in the same way or have the same means as U.S. forces. Understanding this, an SF unit must identify how its adversary views and uses the information environment. This is a challenge, because even though two opposing forces occupy the same operational environment, they will not have the same capabilities in the information environment. It is important to avoid *mirror imaging* U.S. concept of IO upon the adversary and mismatching U.S. capabilities and vulnerabilities to those of the adversary. Chapter 5 provides additional information.

INFORMATION SUPERIORITY

1-9. Information superiority is the purpose of IO. It is also the reason why a commander allocates resources to IO. Information superiority should not be treated as a doctrinal catch-phrase. Just as each mission's end state is different, so is information superiority. For example, during combat operations, information superiority can be gaining surprise over the enemy or preventing the enemy from employing its reserve forces. During counterinsurgency operations, information superiority can be gaining populace support for friendly operations or preventing enemy freedom of flow. In each case, information superiority is defined specifically for the mission in terms of what advantage is sought for the friendly force.

1-10. To achieve information superiority, an SF unit uses information to actively attack the adversary and to shape the information environment to the force's own advantage. This duality of operations—attacking

the adversary and shaping the information environment—is analogous to “fires and maneuvers,” where fires equate to attacking the adversary’s ability to use information, and maneuvers are actions to seize and retain information nodes to gain a positional advantage in the information environment. To be effective, an information operation balances lethal and nonlethal activities to attack the adversary with those that shape the information environment. Through a combination of both, an SF unit seeks information superiority over its opponent.

1-11. An SF unit will rarely achieve absolute and universal information superiority. The actions of opposing forces, as well as the information content and flow in the operational area, are not static. Therefore, information superiority is a localized and transitory condition over the adversary. SF units seek information superiority at certain times and places, usually at or before the decisive point of the operation. Chapter 3 provides additional information.

INFORMATION OPERATIONS CAPABILITIES

1-12. SF operations are not planned for the purpose of using any particular capability. Mission requirements, namely campaign objectives, operating environments, and adversary and friendly forces, dictate what capabilities a commander uses and how they are employed. IO are no different.

1-13. Although often described as a discrete set of capabilities (doctrinally organized as core, supporting, and related capabilities), IO are much more than that. Capabilities used for information operations should be selected based on mission requirements, specifically focused on the desired effect. Some doctrinal IO capabilities—MISO, EW, and CNO—require trained specialists and equipment. However, each element of an SF unit must be able to employ OPSEC, MILDEC, and COMCAM, as well as other IO enablers, such as key-leader engagements and rewards programs. Additionally, various IO capabilities are used in concert with PA, Civil Affairs (CA), host nation (HN), foreign internal defense (FID), partner nation information capabilities, and select interagency capabilities (for example, provincial reconstruction teams). Chapter 2 provides additional information leverage.

CONSIDERATIONS

1-14. Subject-matter experts for core IO capabilities are typically positioned at the special operations task force (SOTF) level and higher when deployed; however, it is essential that commanders at detachment levels understand the core capabilities of IO and how to effectively utilize them to achieve information superiority and accomplish the assigned missions. SOTF staffs can include an IO planner, EW planner, Military Information Support (MIS) planner, a MIS detachment commander, a CA planner, and a COMCAM and PA representative. At the joint special operations task force (JSOTF) level, the staff mirrors the battalion with the addition of a special technical operations planner and the group public affairs officer (PAO), along with retaining the conduits to leverage the higher headquarters (HQ) assets and interagency capabilities. The subject-matter experts at the SOTF and JSOTF can provide training and recommendations to the Special Forces operational detachments A (SFODAs) and Special Forces operational detachments B (SFODBs) on how best to utilize information capabilities, and provide assistance in coordination and deconfliction for IO capabilities in support of their concept of operations.

CONCLUSION

1-15. IO is the use of information as a military capability. Many of the principles and concepts that guide the conduct of other military operations also guide the employment of IO. One way for SF commanders and staffs to integrate IO into operations is to consider IO in terms of the factors of mission, enemy, terrain and weather, troops and support available-time available, and civil considerations:

- *Mission.* The role of IO in the unit mission is to achieve information superiority. As such, it is important to identify exactly what advantage over the enemy IO is expected to achieve.
- *Enemy.* Gaining an advantage over the adversary in the information environment starts with pairing friendly capabilities and vulnerabilities in the information environment against those of the adversary. An information operation that defeats the adversary’s capabilities and turns the information environment to the friendly force’s favor will achieve information superiority.

- *Terrain and weather*. Terrain and weather interact with the information environment to affect information content and flow as well as the employment of IO capabilities. SF units must adjust the employment of IO to the terrain and weather.
- *Troops and support available.* Rarely does an SF unit have all the assets needed to conduct an information operation. Commanders and staffs can fill the gap by thinking beyond doctrine for other ways and means to affect information content and flow.
- *Time available.* Regardless of echelon, IO requires long lead times compared to other operations. Typically, IO must be planned one phase or event in advance of fire and maneuver.
- *Civil considerations.* When civil considerations are important to the unit mission, IO capabilities can be applied to influence the populace, if doing so will achieve an advantage over the adversary.

Chapter 2

Information Operations Capabilities and Tactics

This chapter focuses on the employment of IO capabilities and tactics to gain information superiority. It also shows the links among the capabilities in diagram form. The core and supporting IO capabilities are similar to the warfighting functions. They are independent capabilities that, when taken together and synchronized, constitute IO. IO planners must not let doctrine constrain their selection of capabilities. Any available assets, means, capabilities, or tactics that can shape the information environment or target the adversary's ability to use information should be considered for employment as part of IO.

The use of assets and means for the purposes of IO require judgment in application. Some capabilities—notably MISO, EW, and CNO—are disciplines that require specialized training and skill sets. Employment of these capabilities requires specialized technical expertise to properly plan and execute. Other capabilities already reside within a command or unit and require only planning and coordination to employ them as part of IO. Figure 2-1 outlines some of the more commonly employed IO capabilities.

	Capability	*Employment*
Doctrinal Capabilities	OPSEC	Deny critical friendly information to the adversary.
	MILDEC	Mislead adversary leaders into making decisions that are favorable to friendly forces.
	MISO	Change or reinforce attitudes and behavior favorable to friendly objectives.
	EW	Degrade, disrupt, or deny adversary use of the electromagnetic spectrum (EMS).
	CNO	Degrade, disrupt, or deny adversary use of cyberspace.
	COMCAM	Visually document friendly and adversary forces' operations and activities.
	CMO	Gain local populace acceptance and support.
	PA	Inform populace groups and counter misinformation and propaganda.
Tactics	COMCAM	Visually document friendly and adversary forces' operations and activities.
	Local populace and key-leader engagements	Gain support for friendly-force operations and HN government activities.
	Countering adversary information	Neutralize hostile propaganda or mitigate its effects.
	Rewards program	Influence adversary leaders' perceptions.

Figure 2-1. Information operations employment

Page 2934 of 3957

OPERATIONS SECURITY

2-1. OPSEC is a universal IO capability. It is not just an "in-garrison" competency and needs to be operational at strategic, operational, and tactical levels. OPSEC should be included in all plans, operations, and activities. The goal of OPSEC, in conjunction with unit security programs, is to achieve essential secrecy. Essential secrecy is concerned with the content and flow of critical information. Military forces seek critical information about their opponents to fulfill their own information needs. To do this they attempt to collect accurate, timely, and relevant information, process the information, and disseminate it for use in planning and directing operations. Conversely, if a military force is to prevent its adversary from gaining useful information, then it must prevent the flow of critical information from friendly to adversary forces. At its core¸ OPSEC is an approach to conducting operations. To have a good OPSEC program, it is imperative that the unit identify this critical information, understand the OPSEC indicators and vulnerabilities, and practice essential secrecy. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines essential secrecy as *the condition achieved by the denial of critical information to adversaries.* Essential secrecy depends on the combination of two approaches to protection—security programs to protect classified information, and OPSEC to deny adversaries critical information (which is often unclassified).

2-2. Each command and operation has a tremendous amount of information, both classified and unclassified, that must be protected. However, denying all information about a friendly operation or activity is seldom cost-effective or realistic. Central to this idea is the concept of essential secrecy. By achieving essential secrecy, military forces protect their intentions, capabilities, and activities to retain initiative and the element of surprise for operations. As a condition, essential secrecy is not static—it must first be developed and then maintained as the situation and mission evolve. Essential secrecy cannot be achieved in all places and at all times; therefore, the protection of information must be focused and prioritized to counter specific threats.

2-3. Essential secrecy and the protection of critical information is not the exclusive responsibility of OPSEC. It is the result of mutually supportive OPSEC and security programs. The purpose of OPSEC is to prevent, or at least limit, the flow of sensitive, unclassified information to adversary forces. The actual content of the information, whether classified or unclassified, is the responsibility of information security program controls and procedures. OPSEC denies critical, friendly information to the adversary by eliminating or reducing to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Because OPSEC is not the sole contributor to essential secrecy, an IO objective can integrate other capabilities—such as MILDEC, physical security, information security, and CI—that are not related to OPSEC.

2-4. OPSEC is a process of identifying and protecting critical information and actions that could benefit the adversary. A good OPSEC operation starves the adversary's intelligence system by denying it the information it seeks. Without information on friendly organization, disposition, and intent, the adversary leader's decisionmaking is degraded.

2-5. The basis for OPSEC's contribution to an operation is the commander's key tasks for IO. This means that, for OPSEC to be part of an information operation, at least one essential IO task should address the protection or defense of friendly information.

2-6. Although the purpose of OPSEC is a constant, its focus may change by echelon. At the tactical level, OPSEC prevents the adversary's detection and identification of friendly activities and operations to prevent the targeting of critical assets and countering of current activities and operations. Operational-level OPSEC prevents the disclosure of intentions, capabilities, and future operations (that is, courses of action [COAs]) to avoid the compromise of planning and operations. Tactical-level OPSEC addresses specific measures to defeat the adversary's collection capabilities; whereas, at the operational level, OPSEC addresses broad guidance or general measures for the entire force and new measures to counter the adversary's intelligence capabilities.

2-7. As a way to systematically identify, analyze, and protect critical information relevant to the mission, OPSEC is integrated into the military decisionmaking process. Figure 2-2, pages 2-3 and 2-4, depicts a summary of the five-step OPSEC process.

Note. The five-step process is used at the JSOTF where the assets to form an OPSEC working group exist. At the tactical level, the type of information contained in the OPSEC work sheet (Figure 2-3, page 2-4) and the OPSEC tasks (Figure 2-4, page 2-5) needs to be considered when developing a concept of operations.

1. **Identify Critical Information.** Determine what information needs protection by identifying the information required by the adversary to prevent friendly-force mission success (list of critical information or essential elements of friendly information [EEFI]). Adversaries can derive critical information from the aggregation of indicators resulting from the observation or detection of friendly-force activity. Friendly actions generate indicators (detectable actions and open-source information) that can be collected and developed into critical information (facts about friendly intentions, capabilities, and activities). An adversary can plan and execute its own operations by using critical information. To identify critical information—
   - Identify what information is critical to the friendly mission. Sources of critical information include higher HQ plans and operations orders, commander's guidance, and current unit-critical information lists. Focus on friendly-force intentions (time and place of units and operations), capabilities, and vulnerabilities (strength, technologies, and tactics).
   - Keep in mind that critical information is different for every operation. Do not use a "cookie-cutter" approach. Continually develop or refine critical-information lists.
   - Use an OPSEC working group to take advantage of subject-matter experts (for example, aviation, communications, and computer systems).
   - Identify the length of time each element of critical information must be protected (not all information needs protection for the duration of the operation).
   - Write critical information in the form of a statement (do not write critical information in the form of a question). Generic examples include current and future locations of unit elements; intelligence, surveillance, and reconnaissance capabilities and limitations; and unit movement methods and routes.
   - List the elements of critical information (for example, time and route of helicopter flight) in the order of priority and keep to a manageable number (perhaps five).
2. **Analyze Threat.** Identify the threat to the critical information by determining the adversary's information needs and collection capabilities:
   - Information needs are items of information the adversary requires. Do not bother trying to protect information that the adversary already has.
   - Collection capabilities include human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence, and open-source intelligence (OSINT). An estimated 90 percent of the adversary's information needs are met from OSINT.

   Example threat analysis: Adversary knows: personnel and equipment move by helicopter; adversary needs: departure times and routes of flight; adversary collection method: visual observation by spotters.
3. **Analyze Vulnerabilities.** Identify each element of critical information and its vulnerability to adversary intelligence collection. These are known as OPSEC vulnerabilities and are the result of detectable indicators of the critical information. OPSEC indicators become OPSEC vulnerabilities if they can be observed, analyzed, and acted upon by the adversary. To determine OPSEC vulnerabilities:
   - Identify OPSEC indicators. Determine what detectable actions and OSINT can be interpreted or pieced together by the adversary to derive the unit's critical information.
   - Compare OPSEC indicators to adversary collection capabilities. Determine which indicators can be observed, analyzed, and acted upon by the adversary.

   Example OPSEC vulnerabilities: Direction of flight, helicopters taking off, loading of troops and equipment, and assembly of troops and equipment.
4. **Assess Risks.** The goal is to reduce risk to an acceptable level based on the commander's guidance. Conduct a risk assessment for each vulnerability to determine which really need protection. Focus on the

Figure 2-2. Summary of the five-step operations security process

vulnerabilities that produce the most risk to mission success and, therefore, are an unacceptable risk, and then select one or more OPSEC measure for each vulnerability:

- There are three types of OPSEC measures:
  - Action controls that change unit procedures, activities, and actions (randomized routine activities, avoid repetitive tactics and procedures).
  - Countermeasures that disrupt enemy information gathering and targeting (jamming [EW], physical attack, and camouflage, cover, and concealment).
  - Counteranalysis that deceives the enemy by providing false indicators (decoys, deception in support of OPSEC).
- Decide which OPSEC measures to implement. Check that OPSEC measures do not create new vulnerabilities. Balance OPSEC measures with operational effectiveness (risk versus unit resources). Developing OPSEC measures is a balance between cost and resources in terms of time, personnel, assets, and interference with operations.

Example OPSEC vulnerabilities and mitigating measures: direction of flight (fly in false direction, change direction en route), helicopters taking off (vary flight times, conduct false missions), loading of troops and equipment (load just prior to takeoff), assembly of troops and equipment (assemble troops and equipment under cover).

5. **Apply OPSEC Measures.** Tasks turn OPSEC measures into specified actions. Because OPSEC measures do not follow any doctrinal format, it is necessary to convert them to tasks that the executing units and elements can understand. Develop tasks that support the command's key IO tasks, as well as protect and control the specific indicators associated with key operational tasks:

- Rewrite approved OPSEC measures as tasks. A useful format is task, purpose, and method. In general, for OPSEC, a *task* is an action that controls or protects observable activities, *purpose* can be critical information requiring protection, and *method* is the OPSEC means or methods used to execute the task.

Example OPSEC task that supports combat operations: task—jam enemy ground surveillance radars, purpose—conceal flow of combat elements from electronic collection, method—screen jamming.

Example OPSEC task to support stability operations: task—deny civilian populace access to base-camp overwatch sites, purpose—prevent line-of-sight observation of security activities, method—unit patrols, local police.

- Assign responsibility and coordinate OPSEC tasks with units and staff, to include the intelligence directorate of a joint staff (J-2)/assistant chief of staff, intelligence staff section (G-2)/intelligence staff officer (S-2), and CI for monitoring, and then include OPSEC tasks in the operation plan or operation order.

Figure 2-2. Summary of the five-step operations security process (continued)

EEFI	*Vulnerability*	*Indicators*	*Adversary Collection*	*Risk Level*	*OPSEC Measure*	*Residual Risk*	*Assess*
Location of unit elements	Assault-force insertion	Rotary-wing movement	Sympathetic populace	Extremely High	False insertions	Medium	No adversary contact on ground flow
		Ground movement	Direct observation	High	Reconnaissance element placed on route	Low	Adversary surprised on objective

Figure 2-3. Useful format for determining risk to critical information

EEFI	*Adversary Collection*	*Vulnerable Indicators*	*Standing Operating Procedures or Current OPSEC Measures*	*Additional OPSEC Measures*	*OPSEC Tasks*
Task organization	Spotters on forward operating bases and main supply routes	Vehicle markings	Cover vehicles markings	Remove unit markings	1st Battalion 2d Battalion
		Command vehicles	None	No unsecured communications	Group HQ

Figure 2-4. Useful format for planning operations security tasks

2-8. During operations, the current operation staff should monitor and adjust the elements of critical information based on the adversary's reaction to the implemented OPSEC tasks and for inadvertent disclosure by friendly forces. Tools useful to planning and implementing an OPSEC plan are the OPSEC working group, OPSEC standing operating procedures (SOPs), and OPSEC work sheets.

2-9. The OPSEC working group is a group of subject-matter experts that determines critical information, identifies OPSEC vulnerabilities, coordinates and synchronizes OPSEC measures and tasks, and assesses the effectiveness of OPSEC tasks. Typical membership includes an intelligence analyst to assist with threat analysis, CI personnel to analyze vulnerabilities, a force protection officer, communications and aviation representatives, and subordinate unit liaison officers. The OPSEC working group should conduct periodic assessments of command critical information, threat collection capabilities, OPSEC vulnerabilities, and OPSEC measures.

2-10. An OPSEC SOP is critical to ingraining OPSEC into unit operations. The SOP should be short and direct and should include standing critical information or EEFI, standing OPSEC measures, composition and responsibilities of the OPSEC working group, and OPSEC assessment procedures.

MILITARY DECEPTION

2-11. JP 1-02 defines MILDEC as *actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.*

2-12. MILDEC is more of a process or way of thinking than a capability with tangible assets and resources. It may be executed using a unit's own troops and equipment. An effective deception does not have to be elaborate or complex; however, any time deception is part of an operation, it is the main effort for the information operation and should be included in the defined operational advantage (information superiority) provided for the mission.

2-13. MILDEC is a method, not a result. MILDEC is not conducted merely to deceive an adversary. Deception is used only to support the mission. Figure 2-5 shows ways to employ MILDEC.

Application	*Purpose*	*Focus*
MILDEC	Achieve an exploitable advantage	The adversary's leaders and decisionmakers
Deception in support of OPSEC	Deny information about friendly forces	The adversary's intelligence, surveillance, and reconnaissance capabilities
Deception as part of camouflage, concealment, and decoys	Protect units, systems, and personnel	The adversary's weapons and target-acquisition system

Figure 2-5. Military deception usage

2-14. MILDEC actively targets adversary leaders and decisionmakers in support of specific battles and engagements. It creates an exploitable advantage by misleading or confusing the adversary's decisionmaker. Distorting, concealing, or falsifying indicators of friendly intentions, capabilities, or dispositions that the adversary will see and collect can mislead or confuse the adversary. MILDEC is conducted at all levels—strategic, operational, and tactical—and must be carefully coordinated to deconflict operations between the HQ and subordinate units.

2-15. Deception in support of OPSEC is conducted to reinforce unit OPSEC and is planned using the OPSEC plan as the basis for the deception. A deception in support of OPSEC uses false information about friendly forces' intentions, capabilities, or vulnerabilities to shape the adversary's perceptions. It targets the adversary's intelligence, surveillance, and reconnaissance abilities to distract the adversary's intelligence collection away from, or provide cover for, unit operations. A deception in support of OPSEC is a relatively easy form of deception to use and is very appropriate for use at battalion-level and below. To be successful, a balance must be achieved between OPSEC and MILDEC requirements.

2-16. Camouflage, concealment, and decoys are normally individual or unit responsibilities and governed by SOP. These actions may be taken for their own ends. They can also play a role in a larger MILDEC or deception in support of OPSEC operations where camouflage, concealment, and decoys comprise just a few of many elements that mislead the adversary's intelligence, surveillance, and reconnaissance abilities. Merely hiding forces may not be adequate, as the adversary may need to "see" these forces elsewhere. In such cases, cover and concealment can hide the presence of friendly forces, but decoy placement should be coordinated as part of the deception in support of OPSEC.

2-17. The uncertainties of combat make decisionmakers susceptible to deception. The basic mechanism for any deception is either to increase or decrease the level of uncertainty (commonly referred to as ambiguity) in the mind of the deception target. Both MILDEC and deception in support of OPSEC present false information to the adversary's decisionmaker to manipulate their uncertainty. Deception may be used in the following ways:

- *Ambiguity-decreasing deception.* This type of deception presents false information that shapes the adversary decisionmaker's thinking so he makes and executes a specific decision that can be exploited by friendly forces. This deception reduces uncertainty and normally confirms the adversary decisionmaker's preconceived beliefs so the decisionmaker becomes very certain about his COA. By making the wrong decision, which is the deception objective, the adversary could misemploy forces and provide friendly forces an operational advantage. For example, ambiguity-decreasing deceptions can present supporting elements of information concerning a specific adversary's COA. These deceptions are complex to plan and execute, but the potential rewards are often worth the increased effort and resources.
- *Ambiguity-increasing deception.* This deception presents false information aimed to confuse the adversary decisionmaker, thereby increasing the decisionmaker's uncertainty. This confusion can produce different results. Ambiguity-increasing deceptions can challenge the enemy's preconceived beliefs, draw enemy attention from one set of activities to another, create the illusion of strength where weakness exists, create the illusion of weakness where strength exists, and accustom the adversary to particular patterns of activity that are exploitable at a later time. For example, it can cause the target to delay a decision until it is too late to prevent friendly-mission success. It can place the target in a dilemma for which there is no acceptable solution. It may even prevent the target from taking any action at all. Deceptions in support of OPSEC are typically executed as this type of deception.

2-18. Before planning a deception, it is first necessary to determine if there is a deception opportunity. A deception may be a feasible option if it is appropriate to the mission and if there is a possibility of success against the adversary. The following questions should be considered when planning deception:

- *Is the adversary susceptible to deception?* Planners should use the J-2/G-2/S-2 adversary COA as a basis to develop information about the adversary's system and decisionmaking process. Planners should determine how the deception target acquires and acts on information, what knowledge the target has of the situation and how the target views the friendly force. If

necessary, planners should make assumptions. To do this, they should try to place themselves in the position of the adversary without mirror imaging.

- *Does the friendly mission lend itself to deception?* Some missions are better suited to deception than others. Planners should not feel compelled to work deception into every operation. Generally, when a unit has the initiative and can exercise some control over the mission area of operations (AO), then deception is possible.
- *Do constraints prevent the use of deception?* Other than the constraints imposed by authorities and political considerations, the most important consideration is time. Execution of the mission must allow enough time for the adversary to see the deceptive activities, reconstruct the activities into the deception story, form the desired perceptions, and issue the orders that will cause the adversary force to act in a manner consistent with the deception objective.
- *Are friendly assets available?* To successfully deceive the adversary, MILDEC requires assets. However, very few assets are specifically designed and designated for deception purposes. This means that existing assets have to dedicate support to the deception. This is sometimes difficult, especially when assets are limited. Therefore, the unit may have to be creative to find assets and to use them efficiently.

Note. JSOTF will support strategic MILDEC plans and plan operational MILDEC. At the SOTF and below, units will use tactical MILDEC. Appendix B provides additional information and a tactical deception aid format.

2-19. As with other operations, deception planning follows the military decisionmaking process. Planning a deception does not have to be difficult, but there are certain steps that must be taken to ensure the deception is properly constructed. The steps are as follows:

- *Determine the deception goal.* The deception goal is the desired contribution of the deception to friendly-mission success. In other words, what advantage does the deception provide for friendly forces (for example, provide target opportunities for friendly forces)?
- *Determine the deception objective.* The deception objective is the purpose of the deception operation expressed in terms of what the adversary is to do or not to do at the critical time and location. In simpler terms, it is the action or inaction that friendly forces want the adversary to take (for example, cause insurgent forces to move into the open).
- *Identify the deception target.* The target is the adversary decisionmaker with the authority to make the decision that will achieve the deception objective (for example, the insurgent group commander).
- *Identify desired perceptions.* These are what the deception target must believe to make the decision that will achieve the deception objective. Based on the deception objective and target, the planner must determine the nature of the desired perceptions—will they increase or decrease the target's uncertainty (ambiguity increasing or decreasing)? Desired perceptions eventually translate to resource requirements; therefore, the number of perceptions should be kept to an absolute minimum to conserve the assets needed for the deception (for example, U.S. forces are going to attack from the south).
- *Develop the deception story.* The deception story is a plausible, but false, view of the situation which leads the deception target to act in a manner that accomplishes the deception objective. To be plausible, the story must be integrated into the overall COA. The story is built and stated exactly as the planner wants the target to reconstruct it. To develop the deception story, the planner thinks about how the target sees the situation and then writes the story like the deception target's own intelligence estimate. The story is always written from the target's perspective—what does the target expect to see and think and what will he do (for example, indications are that U.S. forces are massing to the south in preparation for an attack)?
- *Identify the deception means.* These are the methods, resources, and techniques that the unit will use to create required observables (things the adversary decisionmaker needs to see to deduce the desired perceptions) and act out the deception story. The planner must determine for each desired perception what means—physical, technical, and administrative—can be used. Physical means

are observable physical activities of forces, systems, and individuals that present visual indicators. Technical means include radio broadcasts, radar emissions, and electromagnetic deception. Administrative means are used to convey oral, pictorial, documentary, or other material evidence to the deception target.

- *Develop deception events.* These are the activities conducted by the deception means at a specific time and location to convey the deception story to the target. To convey the deception story, the deceptive activities must be observed by the adversary. To determine this, planners pair up the available deception means with the capabilities of the adversary's intelligence collection system. If the adversary intelligence system can "see" the deceptive event, then it can collect the information it needs to piece together the deception story. Deception events must be translated into tasks to subordinate units if the deception operation is to be executed (for example, loudspeaker simulating vehicle traffic, SFODA present in area).
- *Develop OPSEC measures.* Without OPSEC to deny critical information to the adversary, the deceptive activities may not convince the adversary to believe the deception story. In order for the deception to be successful, the unit must adhere to a strict need-to-know policy.
- *Develop assessment requirements.* Collecting feedback is a difficult challenge. However, to judge the effectiveness of the deception, it is necessary to have indications of how the target is responding to the deception. Ideally, there will be indicators of whether the target is receiving the deception story as planned, and if the target is acting in accordance with the deception objective (for example, insurgents move from building to highway).
- *Develop a termination plan.* A deception operation does not just end on its own. Part of the operation is a termination plan that establishes when organized deception activities cease, and how deception means, techniques, and events will be protected. This is important, because there is no logic in executing a deception after the objectives have been met. Additionally, the adversary should not know what deception means, techniques, and events were used. Otherwise, the next deception operation may not have the desired effect due to the adversary gaining insights into friendly TTP.

2-20. In time-constrained deception operations, the "see–think–do" methodology can be used as an abbreviated planning process. The planner uses this process by identifying what he wants the target to *do* (for example, the deception objective), then determines what the target must *think* (for example, required perceptions), and then establishes what the target must *see* (for example, deception events).

2-21. Deception operations cannot proceed without approval or coordination. Two authorities can direct a deception operation: a higher HQ and the unit commander. In both cases, the command's deception plan must be coordinated with the higher HQ. To ensure coordination, deception plans are normally approved two levels above the employing unit HQ. It is imperative that a deception be thoroughly coordinated to prevent information fratricide; that is, employing deception in a way that causes effects in the information environment that impede the conduct of friendly operations or adversely affect friendly forces.

2-22. The military deception work sheet (Figure 2-6, pages 2-9 through 2-11) is a tool that can be used to capture the key elements of the deception plan. Elements of planning information are listed on the work sheet in the order they are developed using the deception methodology.

<table>
<tr><td>Unit Mission: (Concise restatement of the mission. Identifies the operational goal(s) of the command to which the deception must contribute.)

Establish a bridgehead across the Knewt Canal to rapidly advance forces deep into Towie territory and occupy key terrain on Sangria Ridge.</td><td>Deception Constraints: (Identify constraints on the command from higher to lower as they affect the deception plan.)

All liaison activities with members of friendly foreign governments and Allies that concern this operation will not be conducted with prior approval by the Atari Chief of Staff of the military.

War stocks, particularly ammunition, will be stored, handled, transported, and issued with exercise ammunition. The perception that Atari is conducting Exercise SACRED HEART must be maintained.

Wartime SOPs, wartime communications, and wartime modes of operation will not be implemented until two hours prior to commencement of the actual attack operation.</td></tr>
<tr><td colspan="2">Commander’s Guidance for Disposition/Deception Goal: (Describe the desired effects or the end state a commander wishes to achieve [commander’s intent for the deception operation].)

Intent: We will mask the plans for our attack and build-up of our military strike forces by massing supporting logistic elements, the forward deployment of our assault engineers and air defense umbrella, and our increased communications under the guise of Exercise SACRED HEART (the annual Atari command post and maneuver exercise). Exercise SACRED HEART provides the overall cover to conceal our actual intentions.

End State: Numerically and qualitatively superior combat, combat support, and combat service support elements of the Atari 1st Army will be fully deployed on the south bank of Knewt Canal to execute canal crossing operations, drive deeply into Towie territory, and occupy key terrain on Sangria Ridge.

Atari Commander’s Goal Statement: Use MILDEC to achieve operational surprise during Atari canal crossing operations; and enable Atari freedom of maneuver during our drive to the Sangria Ridge.</td></tr>
<tr><td colspan="2">Deception Objective: (Describe the desired action or inaction on the part of the adversary at the critical time and location.)

Cause the Towie front commander to delay mobilization and commitment of the Towie strategic reserve in response to operations. (Note: If a delay in mobilization and commitment of the strategic reserve is achieved, this delay then contributes to/supports the Atari commander’s goal statement of achieving surprise.)</td></tr>
<tr><td colspan="2">Deception Target: (Identify adversary decisionmakers responsible for the actions(s) or inaction(s) specified in the deception objectives.)

The Towie front commander has sole authority to mobilize and commit the Towie strategic reserve—he is the single and only decisionmaker that can make this decision.</td></tr>
<tr><td colspan="2">Desired Perceptions: (Describe what the deception target must believe for it to make the decision that will achieve the deception objective.)

The Towie front commander must believe:

- The Atari military is not preparing for immediate combat operations against the Towie forces or nation.

- The Atari military is conducting Exercise SACRED HEART to improve wartime fighting efficiency, mission command, and logistics; hence, the buildup of its military forces.

- Towie intelligence should detect visible signs of impending combat operations, but Atari forces would be preparing for an exercise and training in the open.</td></tr>
<tr><td>Deception Story: (Outline a scenario of friendly actions or capabilities that will be portrayed to cause the deception target to adopt the desired perception.)

Atari military forces are conducting Exercise SACRED HEART. The purpose of Exercise SACRED HEART is to improve the fighting efficiency, mission command, and logistics of the Atari Army via the exercise’s numerous training and maneuver phases.</td><td>Deception Means: (Describe how the plan will be implemented and how it supports the unit’s overall mission.)

Atari forces can employ the following MILDEC means to get the target to take the action desired: physical, technical, and administrative. These means can be employed independently or in collaboration depending on the situation.

(continued)</td></tr>
</table>

Figure 2-6. Example of a military deception work sheet

	Physical means are those activities and resources used to convey or deny selected information to the decisionmaker. Physical means include operational activities and resources such as: - The movement of the Atari Army and Air Force. - Exercise SACRED HEART subexercises and training events. - Atari logistic actions and the location of stockpiles and repair facilities during Exercise SACRED HEART. - Reconnaissance and surveillance activities performed during Exercise SACRED HEART. ***Technical means*** are the military material resources and their associated operating techniques used to convey or deny selected information to an adversary. As with any use of Atari military material resources, any use of technical means to achieve MILDEC will strictly comply with Atari domestic and international law. A variety of technical means include the following: - Deliberate radiation energy is accomplished when Atari command posts, reconnaissance and surveillance, and air defense networks go operational during Exercise SACRED HEART. - Atari multimedia (radio, television, sound broadcasting, or computers). ***Administrative means*** include resources, methods, and techniques designed to convey or deny oral, pictorial, documentary evidence. The best example of this is a well-publicized announcement (all media outlets) of the upcoming Exercise SACRED HEART.
Assessment: *(Describe the methodology to assess the deception plan if the plan is successful; if the deception fails, or is compromised to Allies or adversaries.)* The command military deception officer will use feedback and intelligence information collected by the command's intelligence officer/directorate to assess if the deception plan is successful, has failed, or had been compromised. Feedback: Is the information providing indications of the response (positive or negative) of the deception target and conduits to elements of the deception. Target (Analytical) Feedback: This is information or analytical determinations regarding the actions of the target in response to the deception executed by the deceiver. Conduit (Operational) Feedback: This is information that provides indications of if and how the conduits are receiving, processing, and transmitting elements of the deception to the target. Indications of identification of enemy deception and counterdeception are provided by the command's intelligence officer/directorate. It is their responsibility to identify foreign deception operations against friendly forces.	**OPSEC Measures to Protect Deception:** *(What OPSEC and other countermeasures are to be used to protect the deception plan from compromise.)* OPSEC measures to implement include the following: - The true nature of the operation will be strictly enforced by using the principles of "need to know." - Encrypted communications, secure land lines, and couriers will be used to convey information about our true intentions. All other traffic will use the Exercise SACRED HEART communications network to pass information. - The Exercise SACRED HEART SOP is in effect command wide; implement the wartime SOP during Exercise SACRED HEART pause but no later than two hours prior to commencement of the actual operation. - No special emphasis will be placed on camouflage and concealment of actual assault forces. In the vicinity of crossing sites standard camouflage and concealment practices to be in place and enforced. - Standard counterintelligence operations are executed throughout the exercise area but with increased focus on the crossing site areas. - OPSEC assessments and monitoring will be in effect up until the time of the attack.

Figure 2-6. Example of a military deception work sheet (continued)

	Termination Plan: *(What is the plan for terminating he deception plan if the desired effects are achieved, not achieved, or compromised?)* Reasons for Termination: - Success. *The deception operation has run its course and the MILDEC operation concludes because the deception target (Towie front commander) took the action envisioned in the MILDEC plan.* - Change of mission scenario. *The overall operation situation has changed and events and circumstances that prompted the deception operation no longer pertain or are applicable and the MILDEC operation is terminated by executing commander.* - Recalculated Risk/Success/Probability of Success Scenario. *Key elements in the deception have changed in a negative way that increases the risks and costs (for example, casualty estimates rise) to the commander and the commander elects to end the deception.* - Failure Scenario. *The deception target does not understand key elements of the deception or does not care about the deception elements being executed and therefore he fails to take the action envisioned in the MILDEC plan. The MILDEC plan is terminated because the Towie front commander has not taken the bait.* - Compromise. *The deceiver believes the adversary has learned some or all elements of t he actual deception operation. Compromise of the deception poses special challenges to the deceiver and the termination process. Not only can important deception capabilities and techniques be placed at risk, but once the adversary has discovered the MILDEC operation he may be able to "read the evidence" and reconstruct the tails of the MILDEC. Worst case scenario—the enemy (Towie front commander) may be able to exploit the compromised deception by initiating his own counterdeception operation to counter/negate the true operation.*

Figure 2-6. Example of a military deception work sheet (continued)

MILITARY INFORMATION SUPPORT OPERATIONS

2-23. The purpose of MISO is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. In simpler terms, MISO seek to change or reinforce foreign attitudes to further U.S. national objectives.

2-24. The more deliberate the planning process is prior to execution, the more likely the MISO effort will be coordinated and integrated with the supported unit's plans. Planning for MISO begins the process of identifying specific individuals, groups, or organizations to influence as part of the commander's overall objectives. When the MISO process is properly executed, it provides the commander with a formidable tool to gain a decisive advantage on the battlefield and potentially save lives.

2-25. Key terms discussed throughout this chapter are defined below:

- *MISO programs* support U.S. national policy and objectives and are approved by the Under Secretary of Defense for Policy (USD[P]) through the interagency process. Approved MISO programs provide the framework for the execution of MISO in support of the range of military operations. MISO programs include objectives, themes to stress, themes to avoid, potential target audiences, attribution posture, means of dissemination, a concept of operations, and funding sources. To execute MISO, U.S. policy requires a USD(P)-approved MISO program be in effect

for the operation in question as well as specified execution authorities in the form of an execution order, operation order, or theater security cooperation plan.

- A MISO *theme* is an overarching subject, topic, or idea. It often comes from policymakers who establish the parameters for conducting MISO by delineating the themes to stress and avoid.
- *Target audiences* are groups of people that can effect achievement of the commander's mission and toward which actions are directed. Planning for MISO requires a thorough analysis of each group's attitude, behavior, susceptibility, and sources of information to determine which themes, messages, and means will effectively influence the group to exhibit the desired behavior.
- *MISO objectives* are general statements of measurable response that reflect the desired behavioral change of foreign target audiences and best support the accomplishment of the supported commander's mission. Generally, the MISO objective is written at the geographic combatant commander level and is part of the geographic combatant commander's overall campaign plan.
- *Supporting MISO objectives* are the specific behavioral responses desired from the target audience to accomplish a given MISO objective. Supporting MISO objectives are unique for each MISO objective, and each MISO objective always has two or more supporting MISO objectives.
- *MISO series* consist of all the MISO products and actions designed to accomplish one behavioral change by a single target audience.
- *Distribution* is the movement of completed MISO products from the production source to the point of dissemination.
- *Dissemination* is the delivery of MISO products directly to the target audience. Planners must keep in mind that each target audience varies greatly in their access to a particular medium, whether it is radio, television (TV), newspapers, posters, and so on. Additionally, the ability of target audiences to understand the message varies because of language, cultural, or other barriers.

Note. An essential element of effectively planning for MISO is integration into the targeting process. This allows MIS forces the opportunity to get the rest of the staff to understand the importance of its nonlethal targets and the psychological effects of planned operations on target audiences.

2-26. Tactical-level MISO are typically conducted by MIS forces (directly attached at the SFODA level) through close-range means, such as face-to-face meetings, loudspeaker broadcasts, or by pinpoint distribution of products, such as leaflets to a particular village.

2-27. Strategic-level MISO focuses on conveying select information to international regional foreign audiences. Operational-level MISO focuses on a theater of operations, whereas tactical-level MISO focuses on conveying select information inside a tactical unit's AO. Because MISO are planned and executed at all levels, it is important that they be mutually supporting or complementary of other United States Government (USG) information activities, as well as other information capabilities (for example, PA and OPSEC). Generally, tactical-level MIS units will use this higher-level guidance as the basis for their own information activities.

Note. The proximity to the target audience does not determine the level of support (tactical, operational, or strategic). Mission analysis and, ultimately, the MISO objective determine the level of support. Likewise, the impact of a MISO effort at the tactical level can have operational or strategic implications.

2-28. Generally, a joint MISO task force assigned to the higher joint command provides direct guidance to all MIS forces in-theater to coordinate MISO at the strategic, operational, and tactical levels. Depending on the mission, either a company- or detachment-sized MIS element will typically support the JSOTF or a SOTF. Task organization is tailored in accordance with the mission, available resources, and priority of effort.

2-29. The primary mission of a MIS company supporting a JSOTF is to conduct operations that influence behavioral responses and advise the commander of those responses and their impact on the operation. The

MIS company typically supports a variety of tactical-level special operations forces missions, monitors the psychological state of target audiences in the operating environment, and analyzes adversary information activities. It can develop, produce, and disseminate tactical-level products within the guidance assigned by the approval authority. The company consists of a company HQ section with a span-of-control of three to five detachments. Development and production of MISO products are typically conducted at the company level.

2-30. A MIS detachment attached to the SOTF is comprised of a HQ section and three to six teams comprised of three to five Soldiers. The MIS detachment provides direction and oversight of the teams. The MIS detachment does product-dissemination planning by determining dissemination priorities and tracking the dissemination of products within the AO. (FM 3-53, *Military Information Support Operations*, and FM 3-05.301, *Psychological Operations Process, Tactics, Techniques, and Procedures*, provide a complete description of the responsibilities and duties of the respective MIS elements.) The team is a three- to five-man element led by an E-7; the team is generally task-organized down to the SFODA. The E-7 also serves as the MIS planner and advisor to the SFODA/SFODB commander and is responsible for the integration and employment of the team. The MIS team is the link between the SF commander and local target audiences in a given AO. This linkage is possible through face-to-face communication and rapport-building with local nationals. Whether conducting loudspeaker operations in support of combat operations or collecting information, on target audiences and the operational environment, the MIS team is a tactical asset that can significantly influence overall operations. Because of its integrated nature, the team is most effective when maintained as a cohesive element. After-action reviews suggest the division of a team decreases its capability.

2-31. A tactical MIS team can perform the following functions during combat operations:

- Reduce the adversary's will to fight. MIS Soldiers can use loudspeakers and leaflets to instill and exploit the fear of death or defeat in the adversary; undermine the adversary's confidence in their leadership; decrease their morale and combat efficiency; and encourage surrender, defection, or desertion.
- Support deception activities through employment of loudspeaker assets and other means.
- Minimize civilian interference with military operations.
- Monitor and assist in efforts to counter propaganda in the AO.
- Plan, develop, and monitor a key-leader engagement strategy for supported commanders to ensure this critical influence tool is appropriately aimed at achieving the commander's objectives.

2-32. During stability and support operations, in addition to discouraging civilian interference and assisting in efforts to counter propaganda, MISO can support the following:

- *Humanitarian assistance.* MIS units support humanitarian assistance operations by providing information on program benefits, shelter locations, food and water points, and medical-care locations. MIS units also publicize humanitarian assistance operations to build support for the United States and HN governments.
- *Peacekeeping.* MISO help gain acceptance for U.S. or allied forces in the AO, thereby gaining support and compliance with U.S. and allied policies and directives, and increasing support for HN governments or military and police forces.
- *Noncombatant evacuation operations.* MIS units support these operations by reducing interference from friendly, neutral, and hostile target audiences and by informing evacuees.
- *Demining operations.* MISO educate the target audience on the dangers of mines, how to recognize mines, and what to do when a mine is encountered. MIS units encourage target audiences to report locations of mines and unexploded ordnance.
- *Foreign internal defense.* MISO help build and maintain support for the HN government and its forces while decreasing support for insurgents.

2-33. In the execution of the MISO series, the team leader coordinates the dissemination of all products through the higher MIS detachment and the maneuver unit. Products normally comprised of standard visual products, such as posters, handbills, and novelty items; audio products, such as loudspeaker

broadcasts, radio messages, and compact discs; and audiovisual products, such as video compact discs or digital videodiscs. In dissemination, the team follows the guidelines set forth in the series dissemination work sheet, which gives specific instructions for required dissemination to the appropriate target audiences. As part of its support to MISO development, the team provides details on possible dissemination sites and optimal dissemination times.

2-34. Whatever dissemination means are used, the MISO messages communicated to the target audiences are guided by themes. A theme is a subject, topic, or idea used as a planning tool to develop a MISO series. For MISO, a theme is developed through target audience analysis based on approved MISO objectives and formulated to affect the attitudes or behaviors of the target audience. As such, themes are broad, somewhat static, and not communicated to the target audience. At the tactical level, MISO themes should be the basis for all communication with the adversary, local populace, and any other target audiences. The two types of themes are the themes to be stressed and the themes to be avoided. The list of themes to stress and avoid can be found in the higher HQ MIS annex. The following are examples of themes:

- *Themes to stress.* Only local people can resolve problems, coalition forces do not favor any group or faction, and displaced persons should return to their homes. Themes to be stressed vary according to the target audience:
  - *Enemy forces.* Themes include inevitability of defeat, hardship and privation, and absence from loved ones.
  - *Local population.* Themes to stress include security and stability, reconstruction and economic prosperity, tribal and cultural, nationality and history (for example, Iraq is a multi-ethnic, tribal-sect-dominated state), insurgents are criminals and miscreants.
  - *Foreign governments.* Themes to stress include commitment and resolve, international security, and cooperation.
  - *Third-party organizations.* Themes to stress include security, stability, and solidarity with military forces.
- *Themes to avoid.* Themes to avoid include religious issues, cultural comparisons, women's roles in local society, themes that appear to favor one faction or group over another, and themes that degrade local ethnic, cultural, or religious values.

2-35. A message is a communication of the theme, whether visually, audibly, or in written form. Messages are communicated to the target audiences to influence their attitudes and behavior. As such, messages are specific, constantly evolving with the situation, and tailored to specific target audiences. Messages may take either of the following forms:

- *Spoken.* Messages can be spoken communication delivered in TV and radio broadcasts, talking points delivered during face-to-face communication or loudspeaker broadcasts.
- *Written.* Written messages can be delivered by leaflets, handbills, or posters.

In any case, a message is a single thought to be conveyed from U.S. forces to the enemy or other target audience (such as the local populace).

2-36. Because of the number of messages and themes available to the commander for his information activities, it is imperative that the IO staff coordinate and synchronize all messages (for example, MIS planner, PAO, CA planner) emanating from the commander. This deconfliction should ensure that messages from different elements are not contradicting one another and that the correct message is communicated to the correct target audience at the right time and place.

2-37. MISO are not the only IO capability that produces themes and communicates messages to the adversary or populace. PA produces and uses PA themes and messages to communicate with the media and inform the populace. MILDEC may communicate deceptive messages to the adversary. Therefore, MISO, PA, and MILDEC must coordinate and synchronize themes and messages so that the correct message is communicated to the correct target audience at the right time and place to avoid information fratricide.

2-38. By using MISO, the commander brings to bear a force-multiplier that uses its capabilities to degrade the enemy's will to fight, reduce civilian interference, minimize collateral damage, and maximize the local population's support for operations. MIS forces do this by using assets at their disposal to reach local and over-the-horizon targets with different visual, audio, and audiovisual products. Proper employment of

MISO means fewer casualties (friendly, enemy, and civilian), fewer U.S. troops required to accomplish the mission, shorter operations, and less damage to infrastructure. Success in these areas results in faster reconsolidation of combat elements, less required rebuilding of infrastructure, and ultimately, quicker return of a nation to self-sufficiency.

2-39. When employing MISO, there are three primary limitations to consider. First, only personnel school trained in MISO and designated by their Service as MIS officers or Soldiers should develop MISO series (although any friendly-force element can disseminate products and conduct face-to-face engagements). Second, there are legal and political factors that may restrict the use of MISO. MISO must follow U.S. and international laws, especially when used without a declaration of war. The third constraint is time. MISO planning must begin early in the operation and continue throughout if it is going to effectively influence the target audience in time to support the operation. FM 3-53 and FM 3-05.301 provide further details on MISO planning and TTP.

ELECTRONIC WARFARE

2-40. EW plays a major role in attacking and exploiting the adversary's ability to use information, while defending the U.S. ability to process information. By definition, EW is any military action involving the use of electromagnetic and directed energy to control the EMS or to attack the enemy. It consists of three divisions: electronic attack (EA), electronic protection, and electronic warfare support. EA is the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA is considered a form of fires. Electronic warfare support involves actions taken to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, and planning. Electronic protection involves passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW. Of EW's three major components, EA has the most direct role in support of IO, especially at the tactical level. At the tactical level, EA is primarily used to attack adversaries by jamming the electromagnetic frequencies used by the adversary (degrading or disrupting information flow) or using the EMS to deceive the adversary (affecting the information content available to decisionmakers).

2-41. The objective of EA planning and execution is to ensure use of the EMS for friendly forces while preventing the adversary's effective use of the spectrum. Electromagnetic jamming denies the adversary the use of its receivers by overwhelming them with high-powered signals on the same frequency as the receiver. Procedurally, this is accomplished through spectrum management and deconfliction. Spectrum management controls frequencies that all friendly emitters use to prevent interference and fratricide. Deconfliction is the process used to avoid conflicts in frequency usage. It is also used during mission execution to resolve interference problems.

2-42. To meet the technical requirements of EA, an EW officer is often needed to effectively plan, coordinate, monitor, and assess friendly and adversary force activity in the EMS. However, depending upon the unit, an EW officer may not be authorized. If the unit does not have an EW officer, EA responsibilities will usually fall to the IO planners. In such a case, IO planners should research the EW assets available to the command from higher HQ and establish contact with representatives from the units that possess the assets.

2-43. Synchronization of EW tasks is imperative. Up to a certain point in the operation, friendly forces may want adversary decisionmakers to communicate, so they do not want to tip off the adversary by jamming too early in the operation. Additionally, lack of frequency deconfliction can result in information fratricide among friendly forces.

2-44. Basic planning considerations for EA include the following:

- *Enemy vulnerabilities.* The J-2/G-2/S-2 should have an electronic order of battle and other intelligence products that identify how the enemy uses the EMS—which systems are critical to adversary operations, what those systems are used for, and what frequencies those systems use. This information helps determine specific electromagnetic vulnerabilities that may be exploited.

- *Friendly capabilities.* Tactical units have limited organic EA assets. Most EA assets are assigned at higher echelons. It is important to know specific capabilities organically available to the unit, as well as those assets that are available through higher HQ.
- *EA deconfliction.* Frequency-spectrum management ensures effective use of the EMS, preventing interference with military and civilian frequencies.
- *Rules of engagement.* EA usually has rules of engagement that must be followed to avoid violating international treaties that control the use of the EMS. In peacetime, EA is generally used only to protect friendly forces. In wartime or conflict, there are restrictions concerning the impact of EA on civilian emergency services.

Note. At the SFODA/SFODB level, leaders must coordinate with the SOTF IO planner for an effect in the EMS. The IO planner will coordinate with the EW officer to identify the means to achieve the effect. It is imperative that EA be coordinated and deconflicted with higher and adjacent elements. The frequency range on the EMS or the cell tower that needs to be jammed for an operation may be the primary means of communications or intelligence collection for friendly forces.

COMPUTER NETWORK OPERATIONS

2-45. CNO provide IO planners with the ability to affect information content and flow within cyberspace. The three elements of CNO are computer network attack, computer network defense (CND), and computer network exploitation. A computer network attack is the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CND is the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks. Information technology professionals assigned to the command, control, communications, and computer systems directorate of a joint staff (J-6); assistant chief of staff, command, control, communications, and computer systems staff section (G-6); command, control, communications, and computer systems staff officer (S-6); and specialized organizations typically execute CMD. Often these same personnel conduct IA activities. Computer network exploitation is an enabling operation and intelligence collection capability conducted by using computer networks to gather data from target or adversary automated information systems or networks. IO planners strive to integrate these CNO elements in cyberspace while synchronizing and coordinating them with other IO capabilities to ultimately achieve information superiority. CNO is typically a collective effort involving separate Services and interagency organizations seeking to achieve effects across the globally interdependent network of information technology infrastructures that include the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Note. Other than CND, which is executed by the J-6/G-6/S-6, CNO is not conducted at the JSOTF. If a need for CNO arises, the IO planner at the JSOTF will request support through appropriate channels. It requires a long lead time for the approval process**.**

2-46. Although CNO has a unique request process involving the joint operations planning process and classified supplemental processes, successful CNO planning relies on a five-step process (Figure 2-7, page 2-17) that should be integrated into the unit's planning process.

1. **Identify CNO contributions to the information operation and determine targets.** IO planners should refrain from identifying specific tasks to CNO and should focus on the desired effect for CNO in support of the information operation. This can be achieved by reviewing the previously determined IO objectives and identifying which objectives can be supported by CNO in terms of the effect included in the objective. Once the objectives to be supported are identified, IO planners coordinate with J-2/G-2/S-2 to identify potential targets for CNO. Related planning factors for a typical computer network attack include the—
   - Quality of available intelligence.
   - Reliability of access to the targeted network.
   - Level of risk determined through a collateral-effects estimate.
   - Timely availability of a required capability.

   IO planners should include CNO-related activities when developing measures of effectiveness (MOEs) associated with the IO objectives and identify collection methods for MOEs associated with CNO.
2. **Determine time available.** During this step, IO planners determine if there is time available to employ CNO in support of the information operation. Considerations include approval timelines, required timing and execution of other IO capabilities in regard to shaping the information environment, and whether delayed or disapproved CNO integration will substantially affect specific IO capability efforts or IO's overall contribution to the mission.
3. **Obtain approval.** Although CNO is an operational-level planning function, units at the tactical level should not hesitate to request CNO support if they identify an appropriate use. The request for CNO is a request for national-level assets. The CNO approval process has unique complexities. CNO-related authorities are retained at high echelons, and IO planners should plan accordingly. When completing CNO requests, IO planners should clearly show the necessity for CNO and its impact on mission accomplishment. IO planners at the tactical level should contact operational-level IO planners to submit CNO requests. Operational-level planners should handle the somewhat-formal approval process. One significant factor pertaining to approval is the fact that computer network exploitation has two distinct subelements. The first is that of an intelligence function (collection) and the second is that of an operations activity (enabling). This distinction is important because CNO, by doctrinal definition, does not include the intelligence subelement of computer network exploitation. However, under Title 10, United States Code, CNO can conduct similar activities as long as they are not for the purposes of intelligence collection. The intelligence community, operating under Title 50, United States Code, can conduct both subelements of computer network exploitation. Therefore, to ensure all activities are legal, coordination between these communities is usually required prior to approval.
4. **Execute CNO tasks.** Execution of CNO should be monitored by the unit to ensure synchronization with other IO capabilities as well as unit maneuver elements. IO planners should identify collected CNO-associated MOEs and make recommendations to the commander concerning variations to the plan.
5. **Conduct after-action review.** Upon completion of the operation, IO planners should determine if CNO tasks supported the IO objectives, as planned. IO planners should identify additional CNO tasks that may have increased friendly-force advantage. IO planners also review the request for CNO and determine what information would have expedited the request. They determine if all MOEs were able to be collected. If not, they determine what changes should be made for future operations? Finally, IO planners determine how the unit will handle unexpected CNO-related adversary responses in the future.

Figure 2-7. Five-step computer network operations planning process

COMBAT CAMERA

2-47. JP 1-02 defines COMCAM as *the acquisition and utilization of still and motion imagery in support of operational and planning requirements across the range of military operations and during joint exercises.*

No, We Did Not

In the spring of 2009, Iraqi Security Forces conducted an operation in central Iraq with U.S. SF advisors to capture an insurgent leader. During the course of the operation, sensitive-site exploitation information led the FID partner-force to a second location. The Iraqi Security Force with U.S. SF advisors searched the second location and then departed. Following the operation, the government of Iraq received complaints that property had been damaged and personnel were harmed during the search.

Due to the IO planning for the operation, COMCAM accompanied the assault force and provided crucial footage proving that no damage was caused to the facility and personnel were treated with respect. The footage was reviewed and released by higher HQ to refute the accusations.

2-48. COMCAM documents military operations with both video and still photography. When the mission dictates, it is used to—

- *Gather intelligence.* COMCAM provides imagery of potential targets or target areas and supports battle-damage assessments.
- *Support planning efforts.* COMCAM validates assumptions by providing accurate images of a situation.
- *Provide imagery to PA and other IO capabilities.* COMCAM provides graphics, photography, video products, and print media to enhance the effectiveness of PA press releases and MISO products.

  Document interrogations and autopsies. COMCAM provides evidence of proper techniques and procedures.
- *Support landing zone studies.* COMCAM imagery can help determine the diameter of the area and the terrain's grade.
- *Provide historical documentation.* COMCAM provides evidence of events for future use (for example, Red Cross investigations) and preserves the accuracy of historically significant events.

2-49. COMCAM captures a photographic record of military operations but, more importantly, it allows commanders to provide visual proof of operations for MISO and PA and to counter adversary IO for enemy, adversary, and neutral information activities. Once the COMCAM team's captured imagery or video is released by the supported commander, the imagery is digitally transmitted to the noncommissioned officer in charge of the JSOTF. Prior to sending the product to the joint combat camera center (JCCC), the imagery is reviewed to obtain the commander's release approval. Once approved, the image is sent to the JCCC, where it may be used by any Department of Defense entity that has access to the imagery database. For example, MIS elements may use these pictures to develop products, whereas PA will use these pictures during press conferences and media-engagement activities. At the tactical level, units can use these images to make immediate impact on the populace within the operating area by producing visual products highlighting local events, good or bad, to achieve the goals set by the unit commander. The complete cycle from image acquisition to receipt by the JCCC must occur within 24 hours for the collection imagery to remain a viable decisionmaking tool for national-level leaders.

2-50. The method of documentation depends on the purpose of the mission, the environment in which the documentation occurs, and the support available to the Soldiers documenting the event. There are three different COMCAM documentation methods:

- *Still photography.* Still photography involves producing, processing, and reproducing still-picture films, prints, and transparencies. These images can be captured using film or digital cameras or can be taken from motion picture or video photography. COMCAM teams use digital still-video cameras to capture and transmit images electronically. Some cameras also have night-vision devices that permit them to be used during darkness or other limited-light conditions.

- *Motion media.* Motion media is documentation of activities or operations as they occur. Motion media technology can be used in daytime, nighttime, and limited-visibility operations. The film, which captures positive and negative images, must be edited before IO or other staff elements can effectively use it.
- *Multimedia presentations.* Multimedia products can be used for a variety of purposes, from meeting training requirements to serving as a means to transmit public information. They allow commanders to review the operations and training of their forces, and introduce new and improved operational techniques and developments to subordinates.

2-51. COMCAM imagery must be reviewed by appropriate staff members of the supported command prior to release. The supported commander is the release authority for all collected COMCAM images before they are transmitted out of theater. Composition of the review board should be tailored based on the specific unit design. A typical review board includes the following individuals:

- J-2/G-2/S-2 representative (for identification of possible intelligence and exposure of classified information).
- OPSEC officer (for identification of possible disclosure of unit critical information [EEFI]).
- Judge Advocate General (for identification of possible or perceived violations of the laws of land warfare).
- Operations directorate of a joint staff (J-3)/assistant chief of staff, operations staff section (G-3)/operations staff officer (S-3) representative (for identification of exposed TTP or any content that is not desirable for release).
- PAO (for public-release consideration).

2-52. To maximize COMCAM support, leaders should—

- Employ COMCAM as an operational asset assigned to the J-3/G-3/S-3. A COMCAM representative is identified within the J-3/G-3/S-3 to plan for the employment of COMCAM.
- Plan to employ COMCAM during the initial phases of an operation to ensure comprehensive mission documentation.
- Provide COMCAM with full mission access (as is reasonably and tactically feasible) during each phase of the operation.
- Ensure COMCAM coverage availability before, during, and after operations.
- Ensure tasks to COMCAM personnel include clearly defined requirements and priorities. Include a purpose for each task to take advantage of COMCAM personnel initiative.
- Ensure COMCAM imagery is reviewed by PAO prior to release outside of the organization.
- Ensure COMCAM personnel provide imagery to the JCCC for immediate distribution to support strategic and operational objectives.

Note. COMCAM can provide images for MISO, MILDEC, PA, and CMO. It can be used for battle damage MOEs. It can also serve as a record.

LOCAL POPULACE AND KEY-LEADER ENGAGEMENTS

> *The people…represent many things in [a] conflict—an audience, an actor, and a source of leverage—but above all, they are the objective. The population can also be a source of strength and intelligence and provide resistance to the insurgency. Alternatively, they can often change sides and provide tacit or real support to the insurgents. Communities make deliberate choices to resist, support, or allow insurgent influence.*
>
> General Stanley A. McChrystal

2-53. Engagement of the local populace and key leaders is an important part of any counterinsurgency campaign or operation. Effective communication with key leaders and key communicators can be critical to mission success at all levels. Not only do commanders and senior leaders conduct key-leader

engagements, but every Soldier has the potential to conduct some form of engagement with the local populace and leaders, and most importantly, to communicate a message through their actions.

2-54. Military leaders who prepare, listen well, and communicate effectively are more likely to gain the cooperation and trust of the local populace. Commanders must also understand that influencing a given populace will most certainly require committing assets to help meet the people's needs—talk will only go so far. People associate actions with messages. SFODA actions on the objective must support the command's themes and messages. Messages with few or no supporting actions generally are given little credibility.

2-55. The attached MIS element is the most capable, by purpose, training, and organization, to develop, plan, monitor, and assess a commander's key-leader engagement strategy. As key-leader engagement is targeted to influence an action or nonaction, it falls to the MIS element to develop the appropriate messages to be disseminated to the appropriate target audience at the right time as part of the commander's larger influence efforts. By using attached MISO personnel to manage the KLE program, a commander ensures a broader, more effective influence effort in his AO.

TYPES OF ENGAGEMENTS

2-56. In interacting with the local population, there are well-planned and coordinated meetings and chance encounters, as described below:

- *Planned face-to-face meetings.* These meetings are daily or weekly key tactical-leadership activities that occur with local leaders and populace. Planned face-to-face engagements are well thought out and resourced. They are an important facet of the mission during counterinsurgency. Face-to-face meetings are often the result of the targeting process and support specific effects tied to accomplishing the desired end state.
- *Key-leader engagements.* These meetings are at all levels between military leaders, HN government, and tribal or village leaders to achieve or support a specific desired effect. To match the appropriate military leader with the leader being engaged requires careful planning.
- *Chance encounters and contacts.* Chance encounters typically occur with the local populace during patrols and other mission activities by MIS teams, Civil Affairs teams, and SFODAs. All personnel with access to the local populace and leadership should be briefed on how to conduct face-to-face engagements, be aware of current matters of interest to the local populace, and be knowledgeable of the command's themes and messages.

THEMES AND MESSAGES

2-57. Themes and messages are two distinct entities. Each has its own purpose—they are not interchangeable. Themes are usually associated with specific lines of operations and are planning tools that guide the development of messages and other information tools (for example, talking points, MISO print and broadcast products, and PA guidance). Themes represent the broad idea the commander wants to get into the mind of the target audience. Themes are not communicated to the target audience; that is the role of messages. Themes are broad and enduring.

2-58. Messages support themes and are communicated by speech, writing, or signals. They contain the information that will be delivered to the target audience. Messages are tailored to specific audiences and are meant to elicit or prevent a certain behavior. Messages constantly change with the situation and mission. Sources of messages include the following:

- *Command information messages.* These messages convey the policies and intent of local commanders to their subordinates. The PAO develops command information messages.
- *Public information messages.* These messages convey information to local target audiences through news, public-service information, and announcements from HN officials. The PAO develops public information messages.
- *MISO messages.* These messages convey specific information to selected foreign audiences to influence their attitudes, perceptions, beliefs, and behavior. MIS elements develop these messages.

Page 2953 of 3957

TYPES OF MESSAGES

2-59. Messages may be either negative or positive. Negative messages are used to attack the target audience or to convey the likelihood of negative consequences if the target audience does not engage in the desired behavior (for example, if you do not surrender, you will be killed). Positive messaging offers specific or implied benefits if the target audience engages in a certain behavior (for example, cooperation with coalition forces will result in the construction of a health clinic).

Note. By doctrine, there are no IO themes and messages. MISO and PA have themes and messages. If needed, in coordination with MISO and PA representatives, the IO staff may have to develop command themes and messages.

MESSAGE DEVELOPMENT

2-60. When developing messages, it is important that message content addresses target-audience vulnerabilities (or perhaps an interest or motivation). Target-audience vulnerabilities are determined by considering the following four factors:

- *Motives.* Look for factors that drive target-audience behavior. Primary motives include basic life needs such as shelter, security, and food. Secondary motives evolve from social interaction within the family, clan, or tribe, or from membership in political and religious organizations.
- *Demographics.* Look for target-audience characteristics, such as gender, ethnicity, religion, and age. Planners must determine which characteristics can be exploited to affect target-audience behavior.
- *Psychographics.* Look for the target audience's cognitive characteristics relevant to the world around them, both near and far. These can be values, beliefs, attitudes, and ideology that trigger emotional responses.
- *Symbols.* Symbols are a sophisticated mix of graphics, video, audio, or audiovisual objects that reference architecture, religious symbols, historical events, and symbols with cultural or contextual significance to the target audience.

2-61. Once vulnerabilities are identified, messages are crafted that communicate the approved themes to the target audience and address its vulnerabilities. Crafting messages is an art that requires time and thought. Figure 2-8, page 2-22, provides a sample message. A few guidelines to follow include—

- Limit each message to one thought.
- Keep each message succinct. Complex messages pose challenges for senders, translators, and receivers. Limit each message to one sentence and minimize internal sentence punctuation.
- Keep messages to a manageable number. Rule of thumb is no more than five messages per theme or target audience.
- Tailor messages for the means and method of delivery and the target audience.
- Convey a story (the theme) by arranging the messages from first to last. The sum of the messages should then tell the story (or theme).
- Place the bottom line up front and summarize at the end. The first message should contain the most important thought. The last message should restate the first message.
- Consider developing "escape" messages that leaders and Soldiers can use to deflect conversations away from the themes to avoid.

Themes	*Messages*
It is inevitable that the insurgents will be defeated.	• While your leaders sleep safe in their warm beds, you are left to suffer in the cold and wind. • Your mothers will mourn the deaths of their sons, and your children will be orphans when you meet the bloody death that awaits you. • Lay down your weapons and return home to the families who need you.
The Army is honorable and capable.	• The Army is the guardian of the people. • The Soldiers fight like bold lions for the freedom of the nation. • The enemy comes with foreigners in the night to murder and rob their fellow tribesmen. • Help the Army defeat its enemies and provide information about terrorists, weapons, people, and activities.
The insurgents are responsible for civilian deaths.	• The United States and its allies do everything possible to avoid civilian deaths. • The insurgents hide among the populace. • It is well known that the terrorists place women and children in harm's way when it suits their purposes.

Figure 2-8. Example message (paired to themes)

2-62. The tool that can be used to develop and organize themes and messages is a message development matrix (Figure 2-9).

Target Audience	*Target Audience Vulnerability*	*Desired Target Audience Action(s)*	*Themes*	*Messages*
People in Village X.	Security from villagers in Town Y.	Halt violent demonstrations.	Violence does not solve any problems.	• Violence does not improve your situation. • Further violence will lead to the withdrawal of coalition aid and support.

Figure 2-9. Example message development matrix

PREPARING FOR A FACE-TO-FACE MEETING

2-63. Conducting planned and unplanned engagements with the local populace and their leaders requires preparation to be effective. Time spent researching the target, anticipating requests and issues, and rehearsing the meeting often pays high dividends. Units conducting operations among the local populace should assume engagements will occur and prepare for them prior to the mission. Lack of preparation may lead to embarrassing situations that have the potential to diminish the effectiveness of friendly forces and create an advantage for the adversary.

2-64. Leaders should consider the following, when preparing for a key-leader engagement or planned meeting:

- *Identify upcoming meeting.* Meetings may occur because of—
  - *A recurring schedule.* Unit leaders often have schedules for reoccurring meetings, such as weekly city council meetings or occasional sit-downs with elected officials, clan or familial

leaders, or tribal sheikhs. These meetings present a preplanned opportunity to conduct a key-leader engagement.

- *Direction from higher HQ.* A higher HQ may direct a unit to engage a specific leader or group to support its objectives. Units should incorporate higher HQ directions into the existing schedule of meetings.
- *Mission planning.* During mission planning, key-leader engagements may be identified as part of the operation. These engagements may have to be conducted outside the normal schedule of meetings.
- *Requests from local leaders.* Local leaders sometimes seek a meeting to address specific concerns or emergencies. When arranging these meetings, always consider the importance of pairing the right military leader with the right civilian leader. Leaders should be very cautious about giving access to relatively insignificant or noninfluential civilian leaders who may try to gain access to senior military leaders.

Note. After identifying a meeting, leaders should determine an appropriate location for the meeting. If hosting the event, leaders ensure the area is presentable and cleared of any operational information. They ensure the location is quiet and away from disturbances such as phones or radios.

- *Identify target-audience characteristics.* Gather as much information about the local leader as possible (for example, proper name and title, approximate age, family members, ethnicity, language spoken, and relationships to other leaders, friendly forces, third-party organizations, and the adversary). One way to obtain this information and prepare for a meeting is to consult personnel who have met with the person before. It is important to continually refine and update background information based on experience with the individual. Characteristics of the local leader that are good to know include—
  - *Language spoken.* Identifying the leader's language may be difficult if multiple languages and dialects are spoken in the operational area, all of which could require different interpreters.
  - *Education/literacy level.* Level of education may determine which form of the language the local leader speaks. Many languages have a colloquial version and a more formal textbook version (often referred to as high or formal). Knowing the individual's level of literacy may impact on decisions to leave written products during the meeting.
  - *Customs and etiquette.* Identifying unique customs and proper etiquette prevents awkward moments during the meeting.
  - *Attitudes.* Understanding the local leader's attitudes toward military forces and toward other organizations and groups in the AO helps to avoid a tense discussion. Plan a strategy to overcome the leader's negative perceptions.
  - *Key advisors.* Knowing the local leader's key advisors facilitates follow-on discussions and may bridge gaps that cannot be resolved with the target directly. Advisors are also helpful in gauging the leader's perceptions of U.S. forces and of the results of the meeting.
- *Identify target-audience concerns.* Every individual engaged has some key concerns that may be raised during the meeting. Being prepared to address these concerns will greatly facilitate communication. Some of the local leader's concerns may include—
  - *Local conditions.* Religious, public health, crime, and economic issues in the key leader's AO may impact the dialogue during the engagement.
  - *Needs.* The local leader will probably discuss the needs of his followers. Needs can be the basic requirements of food, water, and shelter, or they can be more complex—political power-sharing, contact between the populace and U.S. forces, or getting help with reconstruction or security matters. Anticipating the leader's concerns allows the U.S. leader to plan resources that can enhance cooperation.

  - *Religious, political, and economic viewpoints.* Conditions in the operating area may shape religious, political, and economic viewpoints, but viewpoints vary depending on the individual. Knowing the local leader's viewpoints makes it easier to address or avoid sensitive topics that may detract from the meeting. This does not mean that these topics should be avoided, but in general it is best to avoid sensitive topics until one is more familiar with the target audience.
- *Review previous meetings.* Notes, comments, and debriefings from previous meetings with the key leader may indentify previous agreements made with the local leader and reoccurring topics that are likely to be raised at the meeting. For example, if during previous meetings with a city mayor, the mayor asked for more money at each meeting, chances are that he will ask for money again.
- *Identify end state.* Typically, the engagement's end state is the action (or, at times, the inaction) friendly forces want the target to take. For example, the unit may want a leader to actively support Army recruiting or a religious leader to stop encouraging violence.
- *Develop messages.* Develop tailored messages that support the engagement's end state and address the key leader's vulnerabilities. When possible, use already approved messages. Review MISO themes to stress and avoid.
- *War-game responses and reactions.* Develop appropriate counteractions to the key leader's most likely responses and possible demands.
- *Develop meeting exit strategy.* Have an exit strategy so the meeting can end tactfully.

2-65. Leaders can use a face-to-face engagement work sheet (Figure 2-10, page 2-25) to plan critical aspects of key-leader engagements. When kept current, the work sheets are a useful planning tool for future engagements with the same target. Commanders and leaders should also rely heavily on assigned or appropriate themes and messages for reinforcement during the engagement. MIS forces habitually do target audience analyses on various individuals, groups, and factions within their assigned AO and are skilled at planning operations to influence.

CONDUCTING A FACE-TO-FACE ENGAGEMENT

2-66. The following guidelines can help ensure a productive engagement. The spokesman should—

- Position himself immediately next to the engaged key leader and designate a second person to be a recorder.
- Establish rapport with the target audience. The spokesman uses a greeting phrase in the native language, when possible. The spokesman arranges for seating and offers something to drink for the meeting.
- Introduce everyone in the party and record the names and positions of everyone in attendance.
- Avoid rushing through the meeting. The spokesman plans for enough time to accommodate the culture and avoids making the target audience feel they are low on the priority list. The spokesman is prepared for small talk before discussing business. He takes cues from the target audience.
- Ask permission to take photos of the target audience.
- Apologize in advance for any cultural mistakes made. The spokesman assures the target audience that he does not mean to offend and asks that the target audience identify any mistakes made. The spokesman is careful about telling jokes; they can backfire when translated.
- Avoid restricted topics and confrontational attitudes.
- Never assume that the target audience does not speak or understand English.
- Always maintain eye contact with the person he is speaking with, not the translator. The translator is his voice. The spokesman communicates through the translator, not to him. He watches the target audience's gestures, eyes, and body language, not those of the translator.
- Speak in short clips. He should not recite a long paragraph and expect the translator to accurately convey the message. The target audience should feel like he is being conversed with, not being lectured to. He should remember that one to two sentences at a time is a good rule.
- Avoid using acronyms, slang, and idioms. He should keep the language simple.

- Treat all members of the target audience with courtesy and respect.
- Avoid making or implying promises that cannot be kept.
- Avoid elevating his position or embellishing his authority. Although he certainly may have to check with higher authorities before making promises or decisions, using it as an excuse too often may decrease the target audience's respect for him as a leader.
- Use open-ended questions to facilitate discussion. Yes or no answers tend to be incomplete and inaccurate.
- Be aware of the body language from all parties. He ensures that the body language does not negate the message.
- Recap what has been said, as the meeting closes, and clarify expected actions by both parties.

<table>
<tr><td>Target:

Intended target is John Smith.</td><td>Date-Time Group:

210900DEC11</td><td>Location:

FOB Bragg, Building 2, Room 123</td></tr>
<tr><td colspan="3">Characteristics:

Records from previous meetings indicate John Smith is a stern tribal leader. Research shows him to be supportive of U.S. interests, but he has been known to support operations against U.S. forces when it benefits him personally. A number of Smith's acquaintances verify this information. Meeting will be limited to one hour.</td></tr>
<tr><td colspan="2">Environment and Concerns:

Meeting at FOB Bragg is a friendly environment. Our goal is to provide assurance to Smith that the United States will support him upon his return to the tribal region.</td><td>Previous Meetings:

Previous meetings have been cordial and show Smith appears to support U.S. interests. Smith has indicated a desire to partner with U.S. forces in the tribal region.</td></tr>
<tr><td colspan="2">Desired End State:

Reconfirm to Smith that the United States will continue to support his tribe by providing a detachment to support training against insurgency.</td><td>Themes/Messages:

The message Smith must receive is that the United States will continue to provide support for training and combat operations. Posters and pamphlets clarifying this support will be provided to Smith upon his departure.</td></tr>
<tr><td colspan="2">Anticipated Reaction/Issues:

Smith's reaction should be positive provided he is affirmed of continued U.S. support for his tribe. As an issue, it is anticipated that Smith will request monetary compensation for the families of wounded and killed tribal members.</td><td>Response:

Previous meetings indicate that Smith is a hard negotiator, and will initially request more than the United States is prepared to offer. Negotiators must remain steadfast in limiting promised support to that which is deemed appropriate.</td></tr>
<tr><td colspan="2">Meeting Strategy:

Meeting rehearsal is scheduled for 200900DEC11. The team leader and team sergeant will negotiate on behalf of the United States. Participants should be firm, but respectful. Negotiation will occur with Smith only. Samples of products will be provided. Promises of support must remain in keeping with commander's guidance.</td><td>Exit Strategy:

Time limit for the meeting is set at 1 hour. The code word DISCONTENT will be used to end the meeting.</td></tr>
<tr><td colspan="3">Attendees:

Scheduled attendees include John Smith, his aide (Michael Jones), the team leader, team sergeant, and intelligence sergeant. The intelligence sergeant will maintain a list of additional attendees, including approximate age, home town, contact information, profession, and demeanor.</td></tr>
<tr><td colspan="3">Notes:

Team will conduct after-action review immediately following the meeting to compare notes and ensure an accurate understanding. Final report will be submitted to Colonel Jackson not later than 220900DEC11.</td></tr>
<tr><td colspan="2">Follow-up Actions:

Meeting notes and after-action report will be provided to all detachments in the area. Any required coordination with higher will occur within 10 days of the conclusion of the meeting.</td><td>Next Meeting:

Next meeting is scheduled for 200900JAN12.</td></tr>
</table>

Figure 2-10. Example of a face-to-face engagement work sheet

CHANCE ENCOUNTERS AND CONTACTS

2-67. During a chance encounter or contact with the target audience, the leader of the unit should conduct the face-to-face engagement based upon a preplanned battle drill, to include:

- *Security.* Protect both friendly troops and the target audience.
- *Time.* Limit the length of the engagement. Establish a codeword for when it is time to end the meeting.
- *Identify the local leader.* Ask who is in charge and talk to him. Otherwise, select a maximum one or two people to talk with. Do not distribute anything to the populace without the local leader's permission.
- *Take notes.* Get names of all people contacted, approximate ages, hometowns, businesses or activities, subjects covered, demeanor toward friendly forces, and any particular concerns of the target audience.
- *Establish rapport.* Offer the target audience refreshment (such as a bottle of water) and move to a comfortable location. Sit if possible.
- *Focus.* Stay on message by communicating the command's messages.
- *Report.* Report contacts with local leaders up the chain of command to ensure that an accurate picture of the situation is developed.

WORKING WITH TRANSLATORS

2-68. Translators should be treated as a part of the unit. The better the translator is integrated into the unit, the better the translator's performance. Leaders must ensure translators are used for translation duties only. Using them for other activities may violate their contract. An example of misemployment is using a translator to run errands in town. However, sending the translator to town to coordinate a meeting for a U.S. official is allowed. A good rule of thumb is if the translator is acting as the leader's official voice, the action is legal.

2-69. Leaders must know each translator's strengths and weaknesses. The lives of Soldiers may be in the translator's hands. Translators should speak in first-person, remain nearby during engagements with the populace or key leaders, carry a notepad and take notes, project clearly, and mirror the leader's vocal stresses and overall tone.

2-70. The translator should be allowed rest periods to collect his thoughts. Meal meetings are especially challenging for a translator. Leaders should allow the translator to eat during or after the meeting.

2-71. Leaders must rehearse with the translator. If a translator performs poorly, it affects the target audience's perceptions of friendly forces. Rehearsals verify the translator's abilities, help identify words the translator may not know, and ensure the translator understands the overall message to be conveyed. This is especially important with complex, new, or sensitive issues.

2-72. The translator should be briefed on expected behavior. Leaders must recognize that translators are often seen as a representative of the command. All aspects of translator behavior must be kept professional and ethical, regardless of nationality or ethnicity. If operational details are briefed to the translator during the mission rehearsal, leaders should consider having the translator remain on the base camp until execution. Also, the translator should not have a cellular telephone or other communication device.

2-73. When using a translator, a leader must always maintain eye contact with his counterpart and not the translator. The leader communicates *through* the translator—not *to* the translator. The target audience should be observed for changes in gestures, postures, and body language. Leaders should speak in short clips—it is difficult to recite a long paragraph and expect the translator to accurately convey the intent.

COUNTERING ADVERSARY INFORMATION ACTIVITIES

2-74. Countering adversary information consists of programs of products and actions designed to nullify information for effect, misinformation, disinformation, and propaganda or to mitigate the effects of the

information. Successful operations to counter adversary information require the use of all IO and other capabilities.

2-75. All elements of IO can and will support the operations to counter adversary information plans, but the focal point for such operations should remain with PA forces. *Adversary information* is used to describe information and activities used by an adversary or enemy, in peacetime and wartime, to undermine the legitimacy of operations and the credibility of the force. Previously the term *propaganda* was used to describe all forms of adversary information. The evolution of media forms and capabilities has made the term propaganda too limiting in describing how information is used by adversary states and nonstate actors to gain an advantage in the global information environment. To better clarify the use and application of adversary information this manual divides adversary information into the following four categories:

- *Information for effect.* Information for effect involves the use, publication, or broadcast of factual information to negatively affect perceptions and/or damage credibility and capability of the targeted group. Examples of uses of information for effect involve the premature announcement of collateral damage caused by friendly forces, reporting or images of the results of insurgent attacks on friendly forces, or release of captured sensitive, or classified information.
- *Propaganda.* Any form of adversary communication, especially of a biased or misleading nature, designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly (JP 1-02).
- *Misinformation.* Incorrect information from any source that is released for unknown reasons or to solicit a response or interest from a nonpolitical or nonmilitary target (FM 3-13).
- *Disinformation.* Information disseminated primarily by intelligence organizations or other covert agencies designed to distort information or deceive or influence U.S. decisionmaker, U.S. forces, coalition allies, key actors, or individuals via indirect or unconventional means (FM 3-13).

Countering Adversary Information in Iraq

In the early part of 2009, U.S. forces were beginning to transfer bases to Iraqi Security Force control. During the planning of the transfer, a vulnerability was identified that enabled insurgent groups to exploit information and claim they had driven U.S. forces out of the bases. In the north, the Islamic State of Iraq propaganda efforts were active and could exploit upcoming transfers.

The SFODA identified Islamic State of Iraq activity in the vicinity of a future base transfer. The SFODA, in concert with the SOTF, developed a plan with conventional forces to counter Islamic State of Iraq propaganda and highlight the upcoming transfer to Iraqi Security Forces using multiple information capabilities, to include key-leader engagement, PA, PSYOP, and Iraqi Security Force engagement of media. This aggressive information operation with significant Psychological Operations support informed the population of the purpose for the base transfer, countered Islamic State of Iraq propaganda, and discredited Islamic State of Iraq in the area.

2-76. For the purposes of IO, adversary information justifies actions and bolsters legitimacy of an adversary. By communicating with the populace and, at times, friendly forces, the adversary offers a window into its philosophy, goals, objectives, and operations. Therefore, adversary information may provide a useful insight into how to defeat the adversary. Some of the more commonly used techniques include the following:

- *Name-calling.* This describes the use of a name or word to connect a person to something negative (for example, Muslim extremists describing or terming Westerners as Crusaders).
- *Glittering generalities.* This describes the twisting of the meaning of a word that has great symbolic value (for example, terming terrorist attacks as a jihad).
- *Euphemisms.* This describes the use of a milder word to make a situation seem less threatening (for example, “revenue enhancement” to describe a tax hike).

- *Transfer.* This describes the use of symbols to associate an agenda with a respected institution (for example, placing official letterhead on a piece of disinformation).
- *Testimonial.* Testimonials add credibility to a position (for example, using celebrities to testify on political issues).
- *Bandwagon.* This describes a technique which plays on the desire of people to fit in (for example, 7 of 10 workers prefer candidate X).
- *Fear.* This describes the manipulating of people's fears to elicit a behavior (for example, without jihad, the crusaders will invade your homes).

2-77. To effectively counter adversary information, it is necessary to understand the environment in which the adversary information exists. One way to establish the context of adversary information is to determine the interrelationship between information indigenous to the operational area and the culture and history of the people. This information is often available in the MISO studies and appendixes to the command's operation plan. Furthermore, it is also necessary to identify adversary information from other forms of information in the operating environment. Adversary information is often subtle and nuanced, and may be mixed in with misinformation and disinformation. To separate propaganda, it is necessary to identify adversary capabilities to develop and spread propaganda, as well as the receptiveness of the target audience to the adversary's lines of persuasion. This is typically a MISO task, conducted using the source-content-audience-media-effects analysis technique for individual pieces or instances of opponent propaganda and series analysis to determine the operational impact. Source-content-audience-media-effects analysis requires thorough analysis and resources normally found with the MIS elements at the JSOTF level. IO planners can facilitate this analysis by assisting intelligence and MIS personnel in the collection of suspected propaganda. A simple description of source-content-audience-media-effects is as follows:

- *Source.* Identify the originator or sponsor of the propaganda.
- *Content.* Identify the line(s) of persuasion used (the message and the source's desired effect).
- *Audience.* Identify the audiences targeted by the source and actually reached by the propaganda. This step is critical to countering adversary IO planning.
- *Media.* Identify the medium used and why that particular medium was selected by the source.
- *Effects.* Determine the impact of the opponent's propaganda on the target audience. Try to determine whether the propaganda has caused attitudinal or behavioral change.

2-78. A possible staff solution to the problem of countering adversary information activities is to form a working group of personnel from the IO, MISO, PA, and intelligence staffs who can fuse propaganda analysis and media analysis with the current intelligence estimate. In general, the working group seeks to determine how the adversary affects the content and flow of information in the operating environment, how propaganda impacts the various target audiences, and what audience needs are being targeted by the propaganda.

2-79. Countering adversary information activities does not commence upon discovery of adversary propaganda. Effective operations to counter adversary information activities proactively seek to mitigate propaganda's effects before their onset.

2-80. Countering adversary information activities is a long-term operation. To mitigate or nullify the effects of adversary propaganda, countermeasures must anticipate the adversary's response. Success of this effort rests with the ability to correctly direct the capabilities at affecting specific information to the target audience. An effective operation to counter adversary information efforts selects the appropriate capabilities and determines how these capabilities can be employed to match or overmatch the effects of opponent propaganda. Common techniques to counter adversary information include the following:

- *Forestalling.* Forestalling counters possible lines of persuasion prior to the release of propaganda.
- *Conditioning.* Conditioning preemptively shapes target audience vulnerabilities prior to exposure to propaganda.
- *Restrictive measures.* Restrictive measures deny the intended target audience access to the propaganda.
- *Direct refutation.* Direct refutation rebuts the propaganda point-for-point.

- *Indirect refutation.* Indirect refutation questions the validity of some aspect of the opponent's argument.
- *Diversion.* Diversion diverts attention by presenting more important or relevant themes to the target audience.
- *Imitative deception.* Imitative deception alters the propaganda to degrade its impact.
- *Silence.* Silence offers no response to the propaganda.
- *Minimization.* Minimization acknowledges selected elements of the propaganda while downplaying the importance of the content.

2-81. It is unlikely that any one set of countermeasures will apply a complete solution. The effects of opponent propaganda and friendly countermeasures will likely develop in a nonlinear fashion; hence, a constant process of analysis and application is necessary. It is unlikely that any one set of countermeasures will apply a complete solution. The effects of opponent propaganda and friendly countermeasures will likely develop in a nonlinear fashion; hence, a constant process of analysis and application is necessary. To do this, IO planners must monitor any effects produced by the countermeasures, changes to the operating and information environments, and adversary responses to the countermeasures. Then, if applicable, IO planners reengage the target audiences with new countermeasures. Although there is no doctrinal methodology for countering propaganda, the following steps can be used:

- *Analyze target audiences.* Understand the environment, the operational area, the inhabitants, the culture, and the adversary.
- *Analyze propaganda.* Establish a collection plan to identify and collect adversary propaganda. Use the source-content-audience-media-effects process to analyze.
- *Analyze media affecting the environment.* Identify media in AO and then determine its bias and use by adversary for propaganda purposes.
- *Apply countering adversary information measures.* Compare the propaganda analysis to the various capabilities and countering adversary information techniques and then apply appropriate countermeasures.
- *Monitor.* Evaluate the effects of the countering adversary information measures.

REWARDS PROGRAMS

2-82. The Department of Defense Rewards Program pays rewards to persons for providing USG personnel with information or nonlethal assistance that is beneficial to—

- An operation or activity of the Armed Forces or of allied forces participating in a combined operation with allied forces conducted outside of the United States against international terrorism.
- Force protection of the Armed Forces or allied forces participating in a combined operation with U.S. Armed Forces.

2-83. There are two types of Department of Defense rewards:

- Preapproved rewards allow a geographic combatant commander to nominate individuals or items to be placed on the Secretary of Defense preapproved rewards list for rewards in amounts that are in excess of the authority delegated to combatant commanders.
- Regular rewards paid to individuals providing the information after the target has been prosecuted and a monetary value established.

2-84. The Department of Defense Rewards Program can be used for information leading to the killing or capture of high-value individuals, the recovery of weapons caches, or information of impending attack on U.S. forces. Rewards can be paid in monetary funds or barter items. It cannot be used for weapons buyback programs, running an intelligence program, paying intelligence-source salaries, deceased persons (for example, an assassination program), or paying for illegal drugs (for example, a poppy, heroin, or cocaine buying program).

2-85. Rewards programs can be a potent asset to IO used to shape the information environment and provide a conduit to pass messages to the populace and the adversary. Examples of how rewards can be used for the purposes of IO include the following:

- *Key-leader engagement.* Rewards can be used as a means to establish working relationships and build influence with key leaders who have influence in their communities. Rewards can be used to bolster a key leader's position in their community.
- *Influence local population.* Rewards can be used to convince the local populace they can help control the local security situation. They can receive cash rewards for turning in weapon caches and insurgents that cause insecurity in their communities.
- *Message insurgent leaders and fighters.* Rewards can be used to send messages that affect adversary perceptions and decisionmaking. Placing a preapproved reward on a mid-level insurgent leader and then saturating his operating area with wanted posters and handbills may curtail his ability to move and conduct operations.
- *Rewards as part of deception*. Deceptive information about rewards can be used to conceal friendly TTP. Messages can be disseminated that insurgents are being captured because they are being turned in for rewards and not by friendly collection assets. The success of the reward program can be highlighted through MISO products, key-leader engagements, and the "rumor-mill."
- *Rewards as a divisive tool.* As rewards are paid to individuals concurrent with the kill or capture of high-value individuals, friction can be created within an enemy network as members consider who may be leaking information, intentionally or unintentionally, that places the network at risk.

CIVIL-MILITARY OPERATIONS

2-86. CMO establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civil organizations, and the local populace. CMO contribute to shaping the operational area by focusing on civil aspects of the mission, their impact on military operations, and the impact of military operations on the civilian populace. A supportive civilian population can provide resources and information that facilitate friendly operations. As is the case with PA, CMO rely heavily on credibility with local leaders and the populace. CA forces are the designated forces and units organized, trained, and equipped to support the commander in planning and conducting CMO.

2-87. CA forces are structured to support JSOTF operations at the strategic, operational, and tactical levels while maintaining regional focus. The concept of CA support to the JSOTF is that a CA battalion (minus) with two CA companies supports the JSOTF. The CA battalion CA planning team is collocated with the JSOTF HQ to assist in CMO planning within the joint special operations area. A CA company HQ will be collocated with each SOTF and is capable of providing a civil-military operations center (CMOC) outside of each SOTF. A CA team is designated to support each SF advance operational base, as directed. The remaining CA teams are designated as a surge capability for the SOTF commander.

2-88. The CMOC is a standing capability formed by all CA units. The CMOC serves as the primary coordination interface for the U.S. armed forces and indigenous populations and institutions, humanitarian organizations, intergovernmental organizations, nongovernmental organizations, multinational military forces, and other civilian agencies of the USG. The CMOC facilitates continuous coordination among the key participants with regard to CMO and CAO from local levels to international levels within a given operational area, and develops, manages, and analyzes the civil inputs to the common operational picture. The CMOC center is the operations and support element of the CA unit as well as a mechanism for the coordination of CMO.

2-89. CA teams are typically four-Soldier elements consisting of a team leader, team sergeant, engineer, and medic. Besides planning, coordinating, and supporting civil reconstruction projects, CA teams can conduct medical civilian action programs, veterinary civilian action programs, and humanitarian assistance missions to provide quick-impact contributions to local populace quality of life. A CA teams' performance in a given area can affect the public perception in the local area. MISO can support these with radio broadcasts and other means to advertise the events and later exploit their success. PA can also exploit the success of these missions through press releases. It may be useful to attach COMCAM to a CA team to

document civil contributions or to provide photographs for intelligence analysis. If COMCAM assets are not available, any available Soldier with knowledge of the command's intent for the photographs may take pictures.

2-90. If friendly-force military operations create collateral damage and casualties among the populace, CA teams may conduct consequence management to mitigate the negative impact of such operations on the populace through payments or other types of reimbursement. The unit's CA officer may be a conduit to a provincial reconstruction team or other similar entities that have developed relationships with local leaders.

PUBLIC AFFAIRS

2-91. PA units provide timely and accurate information so that both U.S. and international audiences may assess and understand the facts concerning military operations. PA units have the following responsibilities:

- *Internal.* PA provides command information to inform the force and counter effects of adversary propaganda and misinformation.
- *External.* PA provides information regarding military operations to external agencies, governments, media, and populaces.

2-92. Although PA personnel strive to be separate from IO, there is no denying the impact of timely, relevant PA press releases on a given audience. This impact can be multiplied substantially and used to support command objectives when PA personnel are included in IO planning and able to prepare consequence-management activities by preparing press releases beforehand.

2-93. Adversary forces may review PA release information to cue intelligence and provide battle damage assessments. Additionally, PA may be an information conduit to adversary decisionmakers. Extreme care should be taken when employing PA, as successful and effective public relations depends on credibility, and credibility relies on truthful reporting. PA can support IO by—

- Getting ahead of enemy propaganda with the truth.
- Countering adversary misinformation and disinformation by publishing accurate information.
- Ensuring media awareness of the implications of premature release of certain information.
- Playing a key role in establishing ground rules for embedded reporters.

2-94. MISO and PA are separate capabilities that support the commander's objectives. Coordination must be conducted between both. For IO planners, it is important to understand that rural populations generally do not have access to PA release material. Further, PA is wholly dependent on local, regional, and international media to carry their messages. These rural and isolated groups are best informed through MIS assets, which do have organic production and dissemination capabilities. IO planners can facilitate this by ensuring PA releases and articles are sent to MISO planners for dissemination to the local populace. PA planners should review and deconflict messaging with MISO planners to ensure that tactical, operational, and strategic messages are mutually supporting or, at the very least, not contradictory.

Note. The best way to influence the populace through themes and messages is to use the most influential people in the area—the key communicators. Local leaders, FID partner forces, and religious leaders are just some examples of the types of personnel who can spread the message amongst the populace. Whoever is viewed as the most influential, trustworthy source (key is credibility of the messenger) should be the individual serving as a conduit to the target audience.

DEFENSE SUPPORT TO PUBLIC DIPLOMACY

2-95. DSPD are those activities and measures taken by Department of Defense components to support and facilitate public diplomacy efforts of the USG. DSPD is a key military role in supporting the USG's strategic communication program. It includes peacetime military engagement activities conducted as part of the combatant commanders' theater security cooperation plans.

2-96. The focus of defense support to the public diplomacy is to understand, engage, influence, and inform critical foreign audiences through words and actions to foster understanding of U.S. policy and advance U.S. interests. The decisions and actions executed by the SFODA on the ground can have a profound effect on U.S. public diplomacy efforts.

2-97. Figure 2-11, pages 2-32 through 2-35, and Figure 2-12, pages 2-36 through 2-38, provide an overview of IO capabilities. Figure 2-13, pages 2-39 and 2-40, outlines the support roles of IO, CMO, and PA.

OPSEC Supports By:	
MILDEC	• Concealing competing observables. • Degrading general situation information to enhance effect of observables. • Limiting information and indicators that could compromise military deception operations.
MISO	• Concealing contradicting indicators while conveying selected information and indicators. • Ensuring products do not contain classified information.
Physical Destruction	• Concealing friendly delivery systems from enemy offensive IO until it is too late for the adversary to react. • Denying information to the enemy on the success of offensive IO.
EW	• Concealing EW units and systems to deny information on extent of EA and EW support capabilities.
Physical Security	• Concealing EEFI. • Reducing the activities requiring physical security. • Hiding tools of physical security, thus preventing adversary from gaining access.
IA	• Concealing physical and electronic information system locations.
CI	• Ensuring EEFI are concealed from enemy collection assets.
Computer Network Attack (CNA)	• Concealing CNA capabilities.
CND	• Denying enemy knowledge about CND capabilities.
MILDEC Supports By:	
OPSEC	• Influencing adversary not to collect against protected units/activities. • Causing adversary to underestimate friendly operations security capabilities.
MISO	• Providing information compatible with MISO theme.
Physical Destruction	• Influencing adversary to underestimate friendly physical-destruction capabilities. • Influencing adversary to defend C2 element/systems that friendly forces do not plan to destroy.
EW	• Influencing adversary to underestimate friendly EA and EW support capabilities.
Physical Security	• Masking troop activities requiring safeguards.
IA	• Overloading adversary intelligence and analysis capabilities. • Protecting and defending friendly information systems.
CI	• Giving the adversary a cover story so his intelligence system collects irrelevant information.
CNA	• Providing MILDEC targets and deception stories to enhance CNA.

Figure 2-11. Mutual support within information operations capabilities

MILDEC Supports By (continued):	
CND	• Causing the enemy to believe U.S. CND defense is greater than it actually is. • Causing the enemy to believe all CND tools are in place.
MISO Supports By:	
OPSEC	• Disseminating rules of engagement. • Assisting in the countering of propaganda and misinformation. • Minimizing resistance and interference by local population.
MILDEC	• Creating perceptions and attitudes that MILDEC can exploit. • Integrating MISO actions with MILDEC. • Reinforcing the deception story with information from other sources.
Physical Destruction	• Causing populace to leave targeted areas to reduce collateral damage.
EW	• Broadcasting MISO products into adversary civilian and military frequencies. • Developing messages for broadcast on other service EW assets.
Physical Security	• Targeting adversary audiences to reduce the need for physical security.
IA	• Enhancing the ability of IA in the minds of the enemy.
CI	• Providing messages in enemy decisionmaker's mind that can be revealed by CI to determine enemy true intentions.
CNA	• Convincing enemy to not do something by describing effects of a CNA if they take undesirable actions. • Providing MISO messages for dissemination by CNA means.
CND	• Providing information about nonmilitary threat to computers in the AO.
Physical Destruction Supports By:	
OPSEC	• Preventing or degrading adversary reconnaissance and surveillance.
MILDEC	• Conducting physical attacks as deception events.
MISO	• Degrading adversary's ability to see, report, and process information. • Isolating target audience from information.
EW	• Destroying adversary C2 targets.
Physical Security	• Reducing physical security needs by attacking adversary systems able to penetrate information systems.
IA	• Attacking adversary systems capable of influencing friendly information systems availability and integrity.
CI	• Destroying appropriately nominated adversary collection assets.
CNA	• Supplementing computer network attack by destroying or degrading hard targets.
CND	• Destroying or degrading enemy CNA facilities before they attack friendly computers.
EW Supports By:	
OPSEC	• Degrading adversary electromagnetic intelligence, surveillance, and reconnaissance operations against protected units and activities. • Creating barrier of white noise to mask unit maneuvers.
MILDEC	• Using EA and EW support as deception measures. • Degrading adversary capabilities to see, report, and process competing observables causing the enemy to misinterpret information received by electronic means.

Figure 2-11. Mutual support within information operations capabilities (continued)

EW Supports By (continued):	
MISO	• Degrading adversary's ability to see, report, and process information. • Isolating target audience from information and herding that target audience onto MISO broadcast frequencies.
Physical Destruction	• Providing target acquisition through EW support.
Physical Security	• Using electronic protection to safeguard communications used in protecting facilities.
IA	• Using electronic protection to protect equipment.
CI	• None.
CNA	• Supplementing CNA with EA.
CND	• Using electronic protection to protect personnel, facilities, and equipment.
Physical Security Supports By:	
OPSEC	• Protecting operation plans and operation orders.
MILDEC	• Restricting access by level of security and number of personnel.
MISO	• Protecting inventory of sensitive products to prevent premature dissemination of messages.
Physical Destruction	• Safeguarding availability of information systems to use in physical destruction.
EW	• Safeguarding equipment used in electronic warfare.
IA	• Safeguarding information systems by implementing security procedures.
CI	• Safeguarding personnel, and preventing unauthorized access to equipment, installation, materiel, and documents.
CNA	• Safeguarding information systems from sabotage, espionage, damage, or theft.
CND	• Determining applicable risk and threat levels.
IA Supports By:	
OPSEC	• Ensuring information system confidentiality.
MILDEC	• Providing information system assets for conducting MILDEC operations.
MISO	• Ensuring availability of information systems for MISO.
Physical Destruction	• Ensuring information systems are available for physical destruction tasks.
EW	• Ensuring EW assets are available.
Physical Security	• Providing for information system authentication.
CI	• Ensuring information systems are available to conduct CI.
CNA	• Ensuring links with higher HQ to pass CNA.
CND	• Taking actions to ensure availability, integrity, authentication, confidentiality and nonrepudiation of computer.
CI Supports By:	
OPSEC	• Countering foreign human-intelligence operations.
MILDEC	• Countering foreign human-intelligence operations. • Identifying threat intelligence, surveillance, and reconnaissance capabilities.
MISO	• None

Figure 2-11. Mutual support within information operations capabilities (continued)

Page 2967 of 3957

CI Supports By (continued):	
Physical Destruction	• None.
EW	• Providing electronic countermeasures. • Conducting countersignal operations to allow broadcast of MISO messages.
Physical Security	• Countering foreign human-intelligence operations.
IA	• At certain echelons, helping ensure information integrity.
CNA	• Confirming results of CNA.
CND	• Detecting, identifying, assessing, countering, and neutralizing enemy intelligence collection.
CNA Supports By:	
OPSEC	• Attacking enemy computers before they can detect U.S. EEFI.
MILDEC	• Providing the deception story through computers.
MISO	• None.
Physical Destruction	• Attacking selected targets by nonlethal means, which allows lethal attacks on other targets.
EW	• Using with EA.
Physical Security	• Conducting risk assessment to determine consequence of second- and third-order computer network attack effects.
IA	• Attacking enemy computers before the enemy attacks friendly computers.
CI	• Exploiting enemy intelligence collection.
CND	• Attacking the enemy's ability to attack friendly computers.
CND Supports By:	
OPSEC	• Detecting enemy attempts to acquire information.
MILDEC	• Protecting the MILDEC plan resident inside computers.
MISO	• Preventing the compromise of MISO message before release.
Physical Destruction	• Protecting fire support C2 systems.
EW	• Using in conjunction with electronic protection.
Physical Security	• Erecting firewalls to protect intrusion into networks.
IA	• Supporting information assurance of information passed via computer networks.
CI	• Detecting, identifying, and assessing enemy collection efforts against computers.
CNA	• Protecting CNA weapons from enemy detection.

Figure 2-11. Mutual support within information operations capabilities (continued)

OPSEC Can Conflict By:	
MILDEC	• Limiting information that can be revealed to enhance deception story credibility.
MISO	• Limiting information that can be revealed to develop MISO messages.
Physical Destruction	• Limiting information that can be revealed to enemy to develop targets.
EW	• Electronic protection and operations security may have different goals.
Physical Security	• Should be no conflict.
IA	• Should be no conflict.
CI:	• Should be no conflict.
CNA	• Should be no conflict.
CND	• Should be no conflict.
MILDEC Can Conflict By:	
OPSEC	• Revealing information OPSEC normally seeks to conceal.
MISO	• Limiting MISO theme selection. • Limiting information that can be revealed to develop military information themes. • Undermining the credibility of overt messages and other MISO efforts.
Physical Destruction	• Limiting targeting to allow survival and conduct of critical adversary C2 functions.
EW	• Limiting EA targeting of adversary information systems to allow survival and conduct of critical adversary C2 functions.
Physical Security	• Negating the deception story by physical security preventing transmission of a realistic deception story.
IA	• Presenting data the enemy will believe versus assuring data is not revealing to enemy.
CI	• Giving the adversary a cover story that inadvertently supports his collection plan.
CNA	• Should be no conflict.
CND	• Should be no conflict.
MISO Can Conflict By:	
OPSEC	• Revealing information OPSEC normally seeks to conceal.
MILDEC	• Limiting deception story selection if deception story contains untruths.
Physical Destruction	• Limiting targeting of adversary C2 infrastructure to allow conveying of MISO messages.
EW	• Limiting EA against adversary communications frequencies to allow MISO messages to be conveyed.
Physical Security	• Should be no conflict.
IA	• Should be no conflict.
CI	• Should be no conflict.
CNA	• Should be no conflict.
CND	• Should be no conflict.

Figure 2-12. Potential conflicts within information operations capabilities

Physical Destruction Can Conflict By:	
OPSEC	• Causing firing systems to reveal their locations.
MILDEC	• Limiting selection of deception means by denying or degrading elements of adversary C2I command infrastructure necessary to process deception story.
MISO	• Limiting means available to convey MISO messages by denying or degrading adversary C2 systems and civilian communications infrastructure.
EW	• Limiting opportunities for communications intrusion by denying or degrading elements of adversary information systems.
Physical Security	• Limiting access to targeting data (consider need to know).
IA	• Attacking incorrect adversary systems capable of influencing friendly information system availability and integrity.
CI	• Destroying insufficient number of adversary collection assets.
CNA	• Should be no conflict.
CND	• Should be no conflict.
EW Can Conflict By:	
OPSEC	• Revealing EW assets prematurely.
MILDEC	• Limiting selection of deception measures by denying or degrading use of adversary C2 systems.
MISO	• Reducing frequencies available to convey MISO messages. • Jamming military and commercial frequencies used by MISO for electronic dissemination.
Physical Destruction	• Limiting targeting of adversary C2 systems.
Physical Security	• Revealing what physical security is trying to protect (EA). • Electronic protection should not conflict.
IA	• Should be no conflict.
CI	• Should be no conflict.
CNA	• Should be no conflict.
CND	• Should be no conflict.
IA Can Conflict By:	
OPSEC	• Should be no conflict.
MILDEC	• Reinforcing the deception story.
MISO	• Should be no conflict.
Physical Destruction	• Should be no conflict.
EW	• Deconflicting electronic protection and information assurance.
Physical Security	• Should be no conflict.
CI	• Having insufficient information systems available to conduct CI.
CNA	• Having no available links with higher HQ to pass CNA requests.
CND	• Should be no conflict.

Figure 2-12. Potential conflicts within information operations capabilities (continued)

CI Can Conflict By:	
OPSEC	• Should be no conflict.
MILDEC	• Should be no conflict.
MISO	• Should be no conflict.
Physical Destruction	• Killing sources.
EW	• Needing EW support for other activities.
Physical Security	• Should be no conflict.
IA	• Negating information integrity with ineffective CI.
CNA	• Should be no conflict.
CND	• Revealing CI on how networks are protected.
CNA Can Conflict By:	
OPSEC	• Attacking selected enemy targets may provide information on friendly activities.
MILDEC	• Resulting in attacks on wrong target if coordination is not made with MILDEC.
MISO	• Preventing the enemy from receiving MISO messages.
Physical Destruction	• Attacking same target with nonlethal and lethal weapons wastes both time and ammunition.
EW	• Needing to deconflict which systems attack which targets.
Physical Security	• Revealing computer network attack sources that should be protected.
IA	• Should be no conflict.
CI	• Attacking enemy computers before exploiting hostile intelligence collection efforts.
CND	• Should be no conflict.
CND Can Conflict By:	
OPSEC	• Should be no conflict.
MILDEC	• Reinforcing the deception story.
MISO	• Should be no conflict.
Physical Destruction	• Should be no conflict.
EW	• Should be no conflict.
Physical Security	• Should be no conflict.
IA	• Should be no conflict.
CI	• Should be no conflict.
CNA	• Should be no conflict.

Figure 2-12. Potential conflicts within information operations capabilities (continued)

IO Supported By:	
CMO	• Influencing informing populace of civil-military activities and support. • Neutralizing misinformation and hostile propaganda directed against civil authorities. • Controlling electromagnetic spectrum for legitimate purposes.
PA	• Countering adversary information and protecting from misinformation/rumor. • Developing EEFI to preclude inadvertent public disclosure. • Synchronizing MISO and OPSEC with PA strategy.
DSPD	• Ensuring accuracy of information. • Maintaining relevance of information. • Timeliness of information. • Usability of information. • Completeness of information. • Security of information.
COMCAM	• Coordinating guidance to COMCAM teams with commander's information/objectives. • Assisting in expeditious transmission of critical COMCAM images.
CMO Supported By:	
IO	• Providing information to support friendly knowledge of information environment. • Synchronizing communications media and assets and messages with other information capabilities. • Coordinating C2 target sets with targeting cell. • Establishing and maintaining liaison or dialogue with indigenous personnel and nongovernmental organization. • Supporting MISO with feedback on MISO themes. • Providing news and information to the local people.
PA	• Providing information on CMOC activities to support PA strategy. • Synchronizing communications, media, and message. • Identifying, coordinating, and integrating media, public information, and HN support.
DSPD	• Providing information to inform interagency elements on local information environment. • Synchronizing communications media and messages with other IO capabilities. • Establishing and maintaining liaison or dialogue with indigenous personnel and nongovernmental organizations. • Supporting DSPD with feedback on strategic communications themes.
COMCAM	• Using COMCAM capabilities to record priority civic action projects. • Synchronizing imagery assignments with COMCAM team leader.
PA Supported By:	
IO	• Coordinating with IO planners to ensure a consistent message and maintain OPSEC. • Supporting counter adversary information. • Providing assessment of effects of media coverage to OPSEC planners. • Providing assessment of essential nonmedia coverage of deceptions story.

Figure 2-13. Support roles of information operations, civil-military operations, public affairs, defense support to public diplomacy, and combat camera

PA Supported By (continued):	
CMO	• Providing accurate, timely, and balanced information for the public. • Coordinating with civil affairs specialist to verify facts and validity of information.
DSPD	• Coordinating with interagency planners to ensure a consistent message. • Proving assessment of media coverage.
COMCAM	• Managing release of key images through PA channels. • Coordinating for COCAM coverage and access to key events and operation.
DSPD Supported By:	
IO	• Providing a link to interagency for coordination and guidance on strategic communications themes and activities.
CMO	• Providing a link to interagency for coordination and guidance on strategic communications themes and activities.
PA	• Providing a link to interagency for coordination and guidance on strategic communications themes and activities.
COMCAM	• Providing a link to interagency for coordination and guidance on strategic communications themes and activities.
COMCAM Supported By:	
IO	• Providing responsive imagery coverage of events in the operational area.
CMO	• Providing responsive imagery coverage of events in the operational area.
PA	• Providing responsive imagery coverage of events in the operational area.
DSPD	• Providing responsive imagery coverage of events in the operational area.

Figure 2-13. Support roles of information operations, civil-military operations, public affairs, defense support to public diplomacy, and combat camera (continued)

Page 2973 of 3957

Chapter 3

Planning Information Operations

IO are planned as part of the planning process, whether it is the military decisionmaking process, the joint planning process, or some abbreviated planning method. However, in comparison with planning other operations, there are two noticeable differences:

- A longer lead time is required for planning IO. Many IO capabilities have time requirements for preparation (notably MILDEC, MISO, and CNO).
- The threat of hostile information from outside the operational area is great. The ease of information flow through information networks and the media means that operating boundaries are porous to outside influences.

The focus of mission planning for IO is to gain information superiority. Information superiority is an operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Because absolute information superiority is rarely possible to gain or maintain, IO should seek information superiority at or before the operation's decisive point. If the operation is phased, it may be necessary to achieve a form of information superiority in each phase. If the operation is not phased, planners may determine that operational advantages are needed before, during, and after the operation.

Successful IO Plan

The primary role of the IO planner is to coordinate, synchronize, and deconflict while ensuring the appropriate capabilities are employed based on the desired effect. An example of this is an information operation that took place in the Basra Province of Iraq in 2009.

The mission was to conduct an information operation with and through the HN forces to bolster popular support for a partner unit and decrease the influence of extremist groups in the province to set conditions for a safe and secure environment.

The concept was broken down into three phases and focused on four information capabilities: PSYOP, PA, COMCAM, and CMO. The first phase was education and training; the focus of this phase was to provide the partner unit with training on how to interact properly with the populace and the media. The PSYOP teams took the lead during this phase by providing information team training based on various approved courses. This was also an assessment phase for the PAO and the CA officer on the partner unit's media relations and CMO capabilities. In addition to conducting assessments, the PAO, in cooperation with COMCAM, published numerous press releases highlighting the successes of the partner unit's direct action missions. The second phase was planned engagements; the focus of this phase was to assist the partnered unit with providing the locals with much-needed supplies and materials. The CA planner took the lead during this phase by working with the SFODA to determine the best areas to deliver goods and in which areas the SFODA wanted to increase their influence. (*continued)*

Page 2974 of 3957

The PAO and COMCAM supported this phase by highlighting the engagements via press releases and photos. They also utilized a broadcaster to gather video footage of the successful engagements. Based on the relationships developed during phase two, the SFODA transitioned to phase three—planned operations. The SFODA used the information gathered during the planned engagements to assist with targeting efforts, and focused on decreasing the influence of the insurgent groups in the region.

By incorporating multiple capabilities of IO into a focused, coordinated effort, the plan achieved the desired effects to bolster popular support for a partner unit and decrease the influence of extremist groups in the province.

THE STAFF ESTIMATE FOR INFORMATION OPERATIONS

3-1. The staff estimate is an assessment of the situation and an analysis of the COAs a commander is considering. It includes an evaluation of how factors in a staff section's functional area influence each COA or assigned mission, and includes conclusions and recommendations. Staff estimates are developed as part of the planning process. These estimates normally are text documents; however, they may be formatted as maps, graphics, or charts. Whatever form they take, the estimate should be as comprehensive as possible without becoming overly time-consuming.

3-2. The staff estimate for IO is an estimate focused on the information environment and the use of information by adversary and friendly forces. It assesses the situation in the information environment and analyzes the best way to achieve information superiority for the assigned mission.

3-3. Staff sections, particularly at the tactical level, rarely have the time to complete all five paragraphs of a formal doctrinal estimate. In that case, the estimate should concentrate on situation assessment rather than COA development, and only paragraphs 1 and 2 need be produced and updated as operations progress.

3-4. Figure 3-1, page 3-3, provides a format for an IO staff estimate. Figure 3-2, page 3-4, provides an example of a graphic IO estimate.

PLANNING CONSIDERATIONS DURING MISSION ANALYSIS

3-5. The purpose of mission analysis for IO is to assist planners in seeing the information environment, the adversary, and friendly forces in the context of the assigned mission. At the end of mission analysis, IO personnel should have—

- The intelligence preparation of the operational environment (IPOE) products, such as a combined information overlay (CIO) and a template of adversary operations in the information environment.
- The essential tasks for IO.
- The capabilities in the information environment.
- The constraints for IO.
- The critical information requirements for IO.
- The EEFI.

ESSENTIAL TASKS FOR INFORMATION OPERATIONS

3-6. Units rarely conduct an information operation autonomously. There will always be higher HQ and tasks. Although some tasks may have been specifically assigned by the higher HQ, others may be implied (meaning they are necessary to accomplish specified tasks or the overall mission). Implied tasks should require resources and not be administrative in nature. From the specified and implied tasks, planners should identify tasks that the command must successfully accomplish to affect adversary and friendly use of information. These are the unit's essential tasks for IO.

1. **MISSION.** The unit mission.
2. **SITUATION AND CONSIDERATIONS.**
   - **a. Characteristics of the Information Environment.** Summarize significant characteristics of the information environment and the impact on military operations.
     - **(1)** Subinformation environments. How terrain and weather, populace, civilian information infrastructure, civilian population, third-party organizations, and other physical and cognitive features of the information environment create subinformation environments.
     - **(2)** Information nodes. Identify what places, persons, or infrastructure in each subinformation environment shape information contact and flow by creating or transmitting information.
   - **b. Adversary Forces.** Adversary capabilities, vulnerabilities, and activities in the information environment.
   - **c. Friendly Forces.**
     - **(1)** Friendly COA. IO concept of support for each COA.
     - **(2)** Current status of resources. The availability of organic IO capabilities and assets (as translated into capabilities to operate in the information environment).
     - **(3)** Current status of other resources. The availability of supporting IO capabilities and assets from higher HQ, other commands, agencies, and organizations.
     - **(4)** Friendly-force vulnerabilities in the information environment.
     - **(5)** Comparison of requirements versus capabilities and recommenced solutions.
     - **(6)** Key considerations (evaluation criteria) for COA supportability.
   - **d.** Assumptions. Assumptions for IO developed during mission analysis.
3. **COURSES OF ACTION.**
   - **a.** List the COAs that were war-gamed.
   - **b.** List evaluation criteria identified during COA analysis.
4. **COA ANALYSIS.** Analyze each COA using the evaluation criteria. Estimate the likelihood of accomplishing the IO objectives given the available time and capabilities. Determine the potential for unintended consequences of IO tasks and the possible impacts on friendly and adversary forces' COAs.
5. **COMPARISON.** Compare COAs using evaluation criteria. Rank-order COAs for each criterion. If possible use a decision matrix to support.
6. **CONCLUSIONS AND RECOMMENDATION.** Recommend COA based on the comparison (most supportable by IO). Identify IO issues, deficiencies, risks, and recommendations to reduce their impacts.

Figure 3-1. Information operations staff estimate

3-7. Typically, essential tasks for IO number between three and five. More than five essential tasks present the risk of overtaking subordinate elements or having an information operation that is too complex to execute.

3-8. One useful technique for validating an essential task is to ask the following question: "If the unit accomplishes all other tasks marginally and does this one well, will it accomplish the mission?" If the answer is "no," then the task is not essential. If more than five essential tasks are identified, planners should question the validity of each essential task or the nature of the requirements levied on the unit by higher HQ.

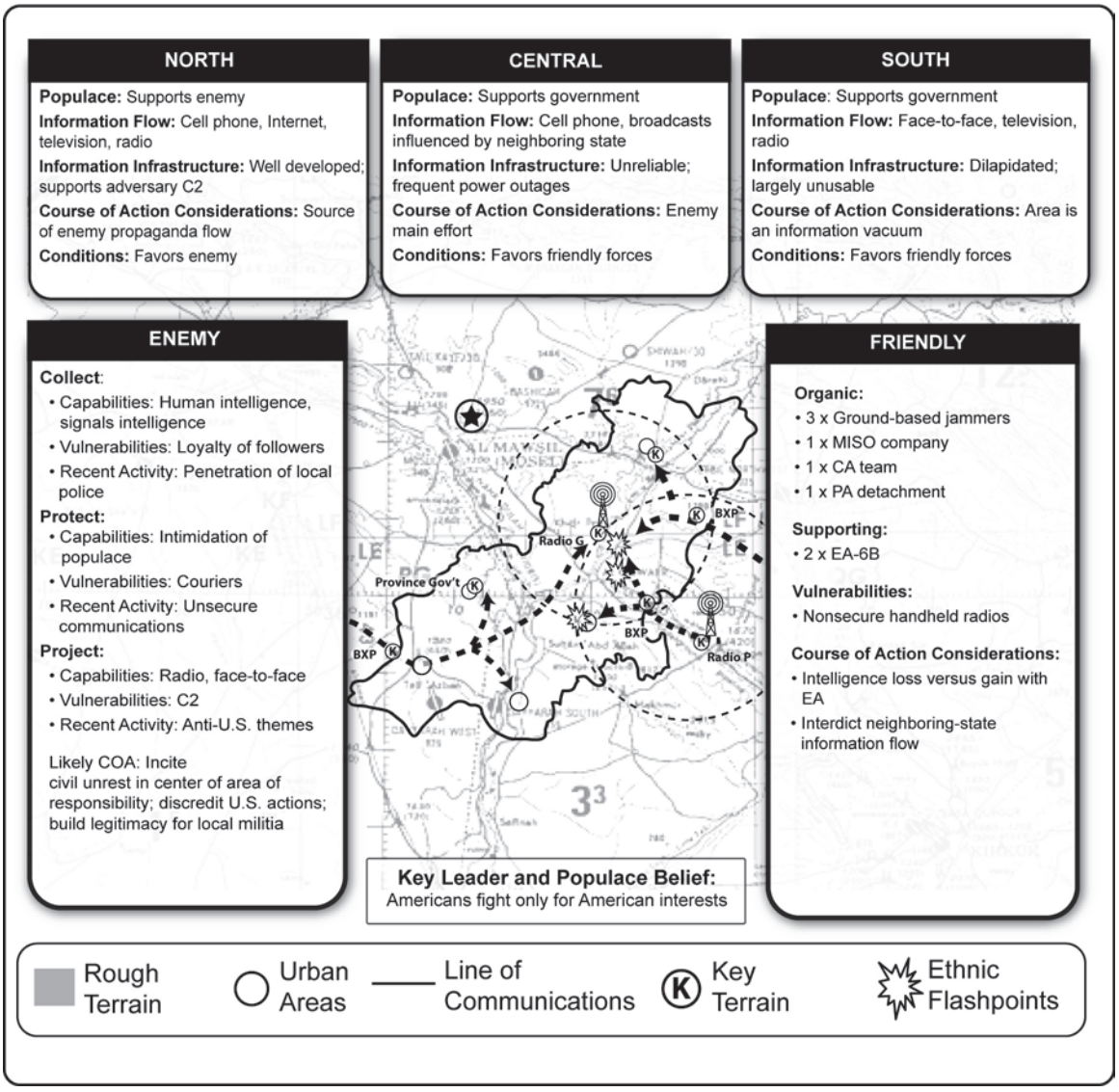


Figure 3-2. Example graphic information operations estimate

CAPABILITIES IN THE INFORMATION ENVIRONMENT

3-9. IO planners should determine if the command has the assets to perform assigned tasks. This is done by identifying any or all organic and supporting IO-capable assets. Organic assets are resident in assigned or attached forces. Supporting assets are available to the command from a higher HQ or government agency. Available assets are then compared with the IO mission requirements (specified and implied tasks) to identify capability shortfalls and any additional assets that are required. It is important to keep in mind that IO planners do not possess any of the individual IO capabilities; these assets all reside within the supporting elements. To ensure use of these assets, IO personnel must start coordination early.

3-10. IO planners face a challenge in expressing IO capabilities to the commander and staff. A simple list of IO capabilities (that is, three ground-based jammers, nine MIS teams, two COMCAM teams, and so on) does not help the commander visualize the command's capabilities in the information environment. In developing its staff estimate. IO planners should consider the following basic questions:

- What can the command do using organic assets?
- What can supporting assets from the higher HQ do?
- What can not be done?

3-11. One possible solution to this problem is to organize IO capabilities by elements, asset, and means in terms of their contributions to friendly-force operations in the information environment. Figure 3-3 shows a sample asset list.

Element	*Assets*	*Means*	*Supported Essential Tasks for IO*	*Effect*	*Targets*
MIS detachment	• 4 x MIS teams	• Loudspeaker operations • Handbills and posters • Radio and TV broadcasts • Face-to-face • Key-leader engagement	• Degrade adversary morale • Influence local populace to not interfere with friendly operations	• Degrade • Influence • Inform	• Insurgent cell • Local populace • Key leaders
SF detachment	• SF teams	• Direct action • Face-to-face	• Disrupt adversary C2 • Build legitimacy of HN security forces	• Disrupt • Destroy • Degrade • Influence	• Insurgent leaders • Insurgent cells • Local populace
EA	• 2 x EA-6B	• Jammer	• Disrupt adversary C2 • Degrade adversary morale	• Disrupt • Degrade • Isolate • Influence	• Insurgent leaders • Insurgent cells

Figure 3-3. Sample information operations asset list

CONSTRAINTS ON INFORMATION OPERATIONS

3-12. Constraints are restrictions placed on the command by a higher HQ that either require the use of resources to execute a specific task or prohibit the commander from taking specific actions. In either case, constraints reduce the commander's freedom of action.

3-13. Like most other operations, IO are constrained by rules of engagement, U.S. national policy, international politics, and other legal, moral, cultural, or operational factors. Additionally, IO planners should consider that IO capabilities have constraints of their own, particularly MILDEC, MISO, CNO, and EW. Common constraints include approval authority for deception operations, MISO themes to avoid, allied forces' national policies and capabilities, restricted targets and frequencies, and PAO guidance.

3-14. To enhance understanding, IO constraints are organized in terms of information content and flow, as shown in Figure 3-4, page 3-6.

Information Content	• Themes should avoid favoring any ethnic group. • Themes should stress highlighted cooperation. • During current operations, approval authority is delegated down to the JSOTF and brigade combat team commanders. • Joint task force commander approves deception.
Information Flow	• No cross-boundary EA. • All EA must be coordinated with the JSOTF. • Non-U.S. allies may not disseminate U.S. MISO products. • PA posture is passive. • Mosques are on the restricted-target list. • COMCAM priorities.

Figure 3-4. Example of information content and flow organization

CRITICAL INFORMATION REQUIREMENTS FOR INFORMATION OPERATIONS

3-15. Commander's critical information requirements (CCIRs) identify information needed by the commander to visualize the operational area and make critical decisions. CCIRs also filter information to the commander by defining what is important to mission accomplishment. If the information operation is important to the mission, then there should be IO input to the CCIR.

3-16. The staff nominates information requirements to become CCIRs based upon the commander's guidance, higher HQ CCIRs, the essential-task list, and the J-2/G-2/S-2 IPOE (situation template). There are two types of CCIRs—

- *Priority intelligence requirements (PIRs).* PIRs are information the commander must know about the adversary. For IO, PIRs should focus on conditions in the information environment and adversary actions that affect the information environment. PIRs that may be required for IO include the following:
  - What media outlets are producing or disseminating hostile propaganda?
  - What propaganda themes are being disseminated to the populace by adversary forces?
- *Friendly-force information requirements (FFIRs).* FFIRs are items of information the commander must know about the friendly force. For IO, FFIRs provide information on critical aspects of the command's information system, IO-capable assets, and execution of the information operation. FFIRs that may be required for IO include the following:
  - Death or serious injury of noncombatants by friendly forces.
  - Media coverage of alleged friendly-force misconduct.

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

3-17. EEFI are the critical aspects of a friendly operation that—if known by the adversary—would subsequently compromise, lead to failure, or limit success of the operation, and therefore must be protected from detection. In other words, EEFI is a list of information that must be protected from the adversary's intelligence system to prevent the adversary from making timely decisions and allowing friendly forces to retain the initiative. Typically, EEFI include the command intentions, subordinate element status, or the location of critical assets (such as command posts and signal nodes). EEFI should be refined throughout the planning process, as some information may not be identified until COA development. Once EEFI are developed, specific measures (in the form of tasks to subordinate units) are developed to protect the information (OPSEC process). Two examples of EEFI are—

- Friendly forces' means of intelligence collection.
- Tribal leaders assisting friendly forces.

Note. Chapter 4 provides additional information on how to develop EEFI.

MISSION ANALYSIS WORK SHEET

3-18. A mission analysis work sheet (Figure 3-5) guides planners through the critical parts of mission analysis. The format to conduct a mission analysis brief to the commander is identical to the mission analysis brief format.

1. **Facts.** Statements of known data concerning the situation, including adversary and friendly disposition, available troops, unit strengths, and material readiness that will directly affect the mission.
2. **Assumptions.** Suppositions on the current or future situation assumed to be true in the absence of facts and which will typically describe future eventualities on which success of the operation depends.
3. **Tasks.**
   - a. **Specified.** Tasks specifically assigned to the command by higher HQ (extracted from paragraphs 1, 2, and 3 of the higher HQ base order, annexes, and overlays).
   - b. **Implied.** Tasks that must be performed to accomplish specified tasks of the overall mission (developed from an analysis of specified tasks).
   - c. **Essential.** Tasks that must be executed to accomplish the mission (derived from analyzing specified and implied tasks lists: essential tasks are included in the mission statement).
4. **Constraints.** Restrictions placed on the command by higher HQ that dictate an action or inaction, thus restricting the command's freedom of action (extracted from higher HQ guidance, concept of operations, coordinating instructions, and annexes—especially IO, rules of engagement, themes to avoid, CMO, and PA).
5. **Available Assets.** Organic and supporting troops and equipment available for the operations (derived from higher HQ order, current tasks organization, and unit status reports).
6. **Risk Assessment.** Hazards that may be encountered during the mission because of the presence of the adversary or hazardous condition in the AO (developed from staff experience and SOPs).
7. **CCIRs.** Information the commander needs to make critical decisions, especially to determine or validate COAs.
   - a. **PIR.** Information the commander must know about the adversary (derived from known gaps in information required to accomplish the operations).
   - b. **FFIRs.** Information the commander must know about the friendly force (developed form knowledge of the friendly force and mission).
8. **EEFI.** Critical aspects of the friendly operation that—if known by the adversary—will compromise, lead to failure, or limit success of the operation and, therefore, must be protected from detection (derived from higher HQ order and developed by using the OPSEC process).

Figure 3-5. Mission analysis work sheet

COURSE OF ACTION DEVELOPMENT

3-19. A COA is a possible plan to accomplish the assigned mission. The IO planner's goal is to develop a concept of support that will generate effects that create information superiority over the adversary at the proper time and place. An IO concept of support should be—

- *Suitable.* The concept must create information superiority over the adversary.
- *Feasible.* The COA must be practical in terms of time, space, and resources. Considerations include time available to shape the information environment and availability of IO capabilities.
- *Acceptable.* The command's information operation must consider the cost of resources, as well as the operational and accidental risks associated with the proposed concept.

- *Distinguishable.* Each COA should be supported with a unique information operation, although the differences may be subtle. These differences include the use of different IO capabilities, changes to the allocation of the capabilities, or changes in the time or sequence of IO tasks.
- *Complete.* The COA should provide information superiority and address friendly-force actions in the case of undesirable results.

3-20. Successful IO give subordinates maximum latitude for initiative and postures the unit for follow-on missions. Likewise, with a little foresight, IO planners can use one information operation to jump-start another. Occasionally, a tactical-level information operation may just be the perfect catalyst for an operational-level information operation (and so on).

STRENGTHS AND WEAKNESSES: INFORMATION ADVANTAGE

3-21. The first step in developing an IO concept of support is to determine whether friendly or adversary forces have the information advantage. A nondoctrinal term, *information advantage* means being in a superior position (able to operate better) in the information environment relative to one's opponent. Information advantage is relative, meaning that although two opposing forces are operating in the same information environment, how each force operates in the information environment is different.

3-22. To determine relative information advantages, leaders compare friendly and adversary forces' strengths (capabilities) and weaknesses (vulnerabilities) in the information environment. This analysis is an asymmetric evaluation, meaning that there will unlikely be a direct correlation between the assets used by either friendly or adversary forces, and how those forces employ the assets. Therefore, IO planners should attempt to relate similar capabilities and attributes in terms of how information is—

- *Collected.* Information collection describes how friendly and adversary forces' means and capabilities are used to collect information about the opponent. Leaders must consider capabilities in terms of HUMINT, SIGINT, imagery intelligence, measurement and signature intelligence (MASINT), and OSINT.
- *Protected.* Information protection describes friendly and adversary forces' means and capabilities to protect critical information and maintain means of communication.
- *Projected.* Information projection describes friendly and adversary forces' means and capabilities to put information into the operational area's information environment. Leaders must consider the type and number of information systems possessed by each side (for example, face-to-face, radio, or TV).

3-23. The adversary forces' capabilities and weaknesses can be derived from IPOE, whereas friendly-force capabilities come from mission analysis, and vulnerabilities from a center-of-gravity (COG) analysis of friendly forces. The results are compared to determine which side is at an advantage or disadvantage in each function. If no apparent advantage or disadvantage exists, then that aspect of operations in the information environment is neutral for both sides. The end result is a subjective determination of whether friendly or adversary forces have the overall advantage in the information environment, and in what way one side has the advantage. Once the analysis is concluded, IO planners should have insight into the following:

- The friendly forces' information capabilities needed for the operation.
- The friendly and adversary forces' vulnerabilities in the information environment.
- The type of operations in the information environment that may be possible from both the friendly and adversary forces' perspectives.
- The additional IO capabilities and resources required to execute the operation.
- The allocation of existing IO capabilities and resources.

The information advantage work sheet (Figure 3-6, page 3-9) is a tool for estimating information advantage.

Page 2981 of 3957

Capabilities in the Information Environment	Strength/Weakness		Relative Advantage	
	Enemy	Friendly	Enemy	Friendly
Information Collect	• OSINT • Couriers	• Overhead and night capabilities • HUMINT sources		X
Information Protect	• Centralized leadership • Unsecure communications	• Secure communications • Internet leaks	X	
Information Project	• Face-to-face • Inconsistent messages	• Radio broadcasts • Lack of credibility with populace	X	
Overall Information Advantage			X	

Figure 3-6. Information advantage work sheet

GENERATING INFORMATION SUPERIORITY

3-24. Once a thorough understanding of each side's capabilities and vulnerabilities is established and apparent advantages and disadvantages are determined, IO planners can begin generating options (COAs) to achieve information superiority.

3-25. Information superiority is an operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority can be achieved by attacking the adversary force with information or shaping the information environment (or both). These attacks are directed at reducing any relative advantages the adversary has and exploiting its relative vulnerabilities in the information environment.

3-26. This duality of information operations—attacking the adversary and shaping the information environment—is analogous to fires and maneuver, where fires equate to attack of the adversary's ability to use information for C2 and as a weapon against friendly forces, and maneuver is an activity to seize and retain information nodes for the purpose of gaining a positional advantage in the information environment. To be effective, an information operation balances activities to attack the enemy force with those that shape the information environment. Through a combination of both, a military force seeks information superiority over the adversary. Figure 3-7 shows examples of information superiority.

Focus of IO	Cognitive Dimension	Physical Dimension
Adversary Force	• Slow decisionmaking • Reduce morale	• Misemployment of forces
Information Environment	• Change populace support	• Change populace behavior

Figure 3-7. Examples of information superiority

3-27. Once identified, information superiority becomes the purpose of the information operation, and as COAs are developed, they must be nested to the unit's main operation. To do this, IO planners determine the operational advantage (that is, information superiority) that will be sought in the information environment and ensure its purpose supports the purpose of the mission statement.

CONCEPT OF SUPPORT STATEMENTS AND SKETCHES

3-28. The IO concept of support describes how available forces will achieve information superiority. It states when and where information superiority needs to be achieved and describes how IO will support the operation and how IO capabilities will be employed. IO planners develop an IO concept of support for

each assigned mission or COA based on what the command's assets and resources can do to achieve the IO objectives. To build an IO concept of support, the IO planner develops the—

- Purpose of the information operation (information superiority).
- IO objectives or essential information operations tasks (EIOTs) that will create the effects in the information environment to achieve information superiority.
- Tasks to subordinate units and staff elements that assign specific actions that will achieve the IO objectives' desired effects.
- Target nominations. Certain IO tasks may result in the identification and nomination of targets.
- Request for support from higher HQ.
- Assessment plan to measure progress.

INFORMATION OPERATIONS OBJECTIVES

3-29. IO objectives describe the effects that will achieve information superiority. IO objectives do not stand alone, but support the commander's operational intent. As such, an IO objective is a statement of what IO will do to attack the adversary or shape the environment to achieve information superiority. For example, if information superiority for an operation is "prevent target from moving from Objective Black prior to attack," then IO objectives could be "disrupt adversary communications within Operational Area Blue to prevent early warning," "deceive adversary decisionmakers on Objective Black to prevent relocation of C2," or "influence local populace in Operational Area Blue to support friendly-force operations with preventing populace reporting of friendly-force activities."

3-30. For each mission or COA considered, IO planners develop IO objectives based on the tasks for IO identified during mission analysis. Depending upon the complexity or duration of the mission (for example, a tactical direct-action mission versus a long-term FID defense mission) there may be only one IO objective or there may be numerous IO objectives developed for each phase of the overall operation. Generally, regardless of the mission, no more than five objectives are planned for execution at any one time in the operation.

3-31. When possible, IO objectives should be observable (the desired effect is detectable), achievable (assets and time are available to accomplish the objective), and quantifiable (the desired effect can be measured). The effects describe a physical or cognitive condition either in the information environment (focus on information content and flow) or against adversary forces (focus on cognition and behavior). IO objectives should not specify ways or means (that is, IO capabilities).

3-32. There is no doctrinal format for an IO objective. One possible format uses target, action, purpose, effect:

- *Target* describes the object of the desired effect.
- *Action* describes the capability or cognitive function of the target.
- *Purpose* describes what will be accomplished for the friendly force.
- *Effect* describes the outcome (for example, destroy, degrade, disrupt, or deceive).

3-33. It is important that IO objectives are written in terms of effects, because it is the desired effect that focuses the activities (tasks) of IO capabilities. For IO, a proper effect falls into one of the three following categories:

- *Effects against the adversary.* IO effects against the adversary focus on the adversary's ability to collect, protect, and project information. An example IO objective is to **disrupt** (effect) **insurgent** (target) abilities to **conduct C2** (action) to **surprise** adversary forces in and around Village X (purpose).
- *Effects to shape the information environment.* IO effects shape information content and flow within the operational area's information environment. An example IO objective is to **influence** (effect) **local populace** (target) **perception** of the insurgents (action) to **increase reporting** of insurgent activity and locations to coalition forces (purpose).
- *Effects to protect friendly forces.* IO effects regarding friendly forces seek to prevent adversary interference with friendly abilities to collect, protect, and project information. An example IO

objective is to **deny** (effect) **insurgent** (target) ability to **exploit** negative effects of friendly-force operations (action) to **prevent support** to adversary efforts (purpose).

Note. Figure 3-8 provides an example of directed effects.

3-34. Because it is impossible to anticipate all possible effects, terms other than those presented in this TC may be used to describe the desired effects for IO. Effects terms should describe a condition—not a task. Definitions may vary for the same effect based on the physical and cognitive nature of the effect and the target of the specific effect.

3-35. As IO objectives are developed, IO planners should consider the indications of success (MOEs) and how the indications will be collected. If adequate indications and collection means cannot be identified, the objective may have to be refined to produce measurable and detectable results. If an objective's MOE is focused on behavior or beliefs, planners must consider physical actions that are a result of the desired behavior, or belief, as an indicator.

Effects Against the Adversary		***Effects to Shape the Environment***	
Physical Effects	Cognitive Effects	Information Content	Information Flow
Destroy – Use lethal or nonlethal means to render adversary capabilities to collect, protect, or project information ineffective, unless reconstituted. **Degrade** – Use nonlethal or temporary means to reduce the adversary's effectiveness or efficiency to collect, protect, or project information. **Disrupt** – Interrupt the flow of information to and from the adversary and within the adversary organization. **Isolate** – Seal off an adversary from sources of support or contact with other adversarial elements.	**Deceive** – Mislead the adversary decision-makers, causing them to take specific actions or inactions that contribute to friendly-force mission accomplishment. **Influence** – Cause adversaries or others to behave in a manner favorable to friendly forces. **Isolate** – Prevent effective adversary decisionmaking by impeding the adversary's efforts to collect and project information.	**Destroy** – Use lethal or nonlethal means to render adversary information or information systems ineffective, unless reconstituted. **Degrade** – Use nonlethal or temporary means to reduce the effectiveness or efficiency of adversary message content. **Exploit** – Gain advantage of an adversary action that has negative effects on the populace. **Influence** – Cause adversaries or others to behave in a manner favorable to friendly forces.	**Degrade** – Use nonlethal or temporary means to reduce the effectiveness or efficiency of adversary communication methods with the populace. **Exploit** – Take advantage of gained access to a populace. **Isolate** – Prevent populace groups from communicating with each other. **Influence** – Cause information to move faster or slower, resulting in populace behavior that is favorable to friendly forces. **Disrupt** – Break or interrupt the flow of information between selected key-information nodes.
Effects to Protect Friendly Forces			
Deny – Withhold information about friendly-force capabilities and intentions that adversaries need to make effective and timely decisions. **Mitigate** – Reduce negative effects of friendly-force operations on the populace. **Neutralize** – Render an adversary's collection capability ineffective with regard to time, space, and purpose.			

Figure 3-8. Effects for information operations

ESSENTIAL INFORMATION OPERATIONS TASKS

3-36. At the tactical level, in a time-constrained environment, it is sometimes more straightforward to write IO objectives as EIOTs. EIOTs serve the same function as objectives; specifically, they focus the activities

(tasks) of the various IO capabilities. One difference is that EIOTs include the methods or means that will be used to perform the EIOT. A possible format for an EIOT uses task, purpose, method, effect:

- *Task* (for example, jam adversary's C2 communications).
- *Purpose* (for example, prevent coordinated efforts against friendly forces).
- *Method* (for example, EW EA-6B).
- *Effect* (for example, disrupt).

INFORMATION OPERATIONS TASKS TO SUBORDINATE UNITS AND STAFF ELEMENTS

3-37. Once IO objectives or EIOTs are written, IO planners develop tasks to subordinate units and staff elements that possess the IO capabilities needed to accomplish the IO objectives or EIOTs. Therefore, the aggregate execution of assigned tasks should achieve the effect of the IO objective or EIOT. Tasks for IO capabilities to subordinate units translate the broad concepts of the objectives and EIOTs into discreet actions. Tasks are often written as—

- *Task.* The task is the action to be performed and the location of the task (for example, prevent local populace interference in Village X).
- *Purpose.* The purpose is the reason why the task is assigned (for example, prevent civilian casualties).
- *Method.* The method describes what unit or capability will conduct the task (for example, MIS Team C121).

3-38. To develop tasks, IO planners should consider all available organic and supporting IO capabilities and resources that can help achieve each IO objective. As a matter of course, it is best to have representatives for each IO capability write their own tasks.

3-39. Similar to effects, tasks can be organized into three categories (Figure 3-9, page 3-13). These tasks are as follows:

- *Tasks against the adversary.* These tasks target adversary capabilities and vulnerabilities to collect, protect, and project information (as identified during the COG analysis). An example task is C*ounter insurgent propaganda to maintain populace support for capture/kill missions*.
- *Tasks to shape the information environment.* These tasks shape information content and movement by impacting the key nodes in each subinformation environment to influence local populace perceptions and behavior. An example task is *Engage religious leaders to stop inflammatory rhetoric.*
- *Tasks to protect friendly forces.* These tasks seek to protect friendly-force vulnerabilities in the information environment from adversary capabilities to collect and project information. An example task is *Detect intrusions into friendly-force information systems to prevent adversary collection of critical information.*

3-40. An IO planning work sheet (Figure 3-10, page 3-14) is a tool that can be used to develop an IO concept of support for input to COA development. One work sheet is filled out for each IO objective.

INFORMATION OPERATIONS CONCEPT OF SUPPORT

3-41. The IO concept of support is a word picture that explains how the information operation supports the operation from beginning to end, and how IO capabilities will be employed to provide information superiority. The IO concept requires defining information superiority for the operation. A well-written concept is concise and understandable. Although there is no doctrinally prescribed formula for an IO concept of support, leaders should consider the following:

- *Commander's intent for IO* describes what the commander wants IO to do to the adversary or to shape the information environment.
- *Information superiority* is described in the context of the operational situation and the command's mission; this should include the specific time and place for it to be achieved (should be linked to decisive points in the operation).

- *General plan for IO* lists the IO objectives, tasks to be executed, capabilities that will execute, associated MOEs for the objectives, and collection methods that will be used for assessment.
- *Priority of support* designates which subordinate unit or element has the priority of IO assets and capabilities. *Restrictions on the employment of IO* lists prohibited and directed actions that affect the employment of IO.
- *General scheme for IO* uses doctrinal concepts and terms to explain how the IO objectives will be achieved, who will perform them (that is, the tasked units), and the sequencing of key tasks; it relates the key tasks to the achievement of information superiority.

Tasks Against the Adversary	*Tasks to Shape the Environment*
Counter – Diminish adversary information to correctly portray friendly intent and actions. **Demonstrate** – Show or reveal. MILDEC typically conducts tasks to demonstrate. **Deter** – Prevent action through the existence of a credible threat of unacceptable counteraction. MISO forces typically conduct tasks to deter. **Disseminate** – Spread or disperse. MISO and CMO typically conduct tasks to disseminate. **Jam** – Interfere with or prevent the clear reception of signals by electronic means. EW typically conducts tasks to jam. **Persuade** – Induce to believe something or convince. MISO forces typically conduct tasks to persuade. **Prevent** – Keep from happening or avert. OPSEC typically conduct tasks to prevent.	**Broadcast** – Transmit and make public by means of radio or TV. Typically MISO forces conduct tasks to broadcast. **Demonstrate** – Show or reveal. MILDEC typically conducts tasks to demonstrate. **Disseminate** – Spread or disperse. MISO and CMO typically conduct tasks to disseminate. **Engage** – Initiate contact to open dialogue with or communicate a message to a target. MISO and CMO typically conduct tasks to engage; however, any friendly-force asset with access to the target has potential to conduct face-to-face engagements. **Inform** – Provide information or educate a specific target audience. MISO, PA, and CMO typically conduct tasks to engage; however, any friendly-force asset with access to the target has potential to inform through face-to-face engagements. **Persuade** – Induce to believe something or convince. MISO forces typically conduct tasks to persuade. **Publicize** – Bring to the attention of the public. PA typically conducts tasks to publicize.
Tasks to Defend Friendly Forces	
Detect – Discover or discern the existence, presence, or fact of an intrusion into information systems. IA, CI, and EW typically conduct tasks to detect. **Protect** – Guard against espionage or capture of sensitive equipment or information. OPSEC, IA, CNO, physical security, EW, and CI typically conduct tasks to protect. **Respond** – React quickly and appropriately to an adversary attack or intrusion in the information environment. All IO capabilities have potential to respond, depending on the specific incident. **Restore** – Bring information systems or conditions in the information environment back to their original state. IA typically conducts tasks to restore.	

Figure 3-9. Tasks for information operations capabilities

<table>
<tr><td colspan="3">COA: Conduct raid at Objective LIMA to remove insurgents and return control of the area and populace to the existing government.

IO Objective: Disrupt communications by jamming insurgent communications. This will prevent coordinated efforts against friendly forces.</td></tr>
<tr><td>EW Tasks:
Provide electronic jamming of mission command communications used by the insurgents.</td><td rowspan="3">Information Operations Targets:
Insurgent command and communications nodes.</td><td rowspan="3">Protect Assets:
Protection of friendly communications is essential.</td></tr>
<tr><td>MISO Tasks:
None</td></tr>
<tr><td>OPSEC Tasks:
Protection of the essential elements of friendly information is imperative to ensure success of electronic warfare plan.</td></tr>
<tr><td>MILDEC Tasks:
None</td><td colspan="2">MOEs:
Inability of insurgent forces to send early warning and inability to communicate during the mission.</td></tr>
<tr><td>CMO Tasks:
None</td><td colspan="2" rowspan="2">Intelligence Requirements:
Insurgent key personnel and frequencies used by key communicators in the area of operations.</td></tr>
<tr><td>PA Tasks:
None</td></tr>
<tr><td>Other Tasks:
None</td><td colspan="2">Coordination:
Coordinate with the spectrum manager and adjacent and higher headquarters.</td></tr>
</table>

Figure 3-10. Example of an information operations planning work sheet

INFORMATION OPERATIONS CONCEPT OF SUPPORT SKETCH

3-42. The IO concept of support sketch is a visual graphic (Figure 3-11, page 3-15) of the information operation. It is the product used to brief the commander and staff on what IO capabilities will do during the mission. The format or medium used for the sketch is not as important as ensuring the correct elements of information are presented, that the sketch shows that the information operation is synchronized with other operations, and that it clearly depicts the synchronization of the IO capabilities involved with the operation. The sketch should answer the following questions:

- *Who?* What capabilities will be employed to perform the IO tasks?
- *What?* What operational advantage is provided by the information operation (that is, information superiority)? What objectives (or EIOTs) must be achieved and what are the required tasks to IO capabilities?

- *When?* What time during the operation will tasks be performed?
- *Where?* Where in the operating area will the IO tasks be performed?
- *Why?* What is the purpose of each IO task?

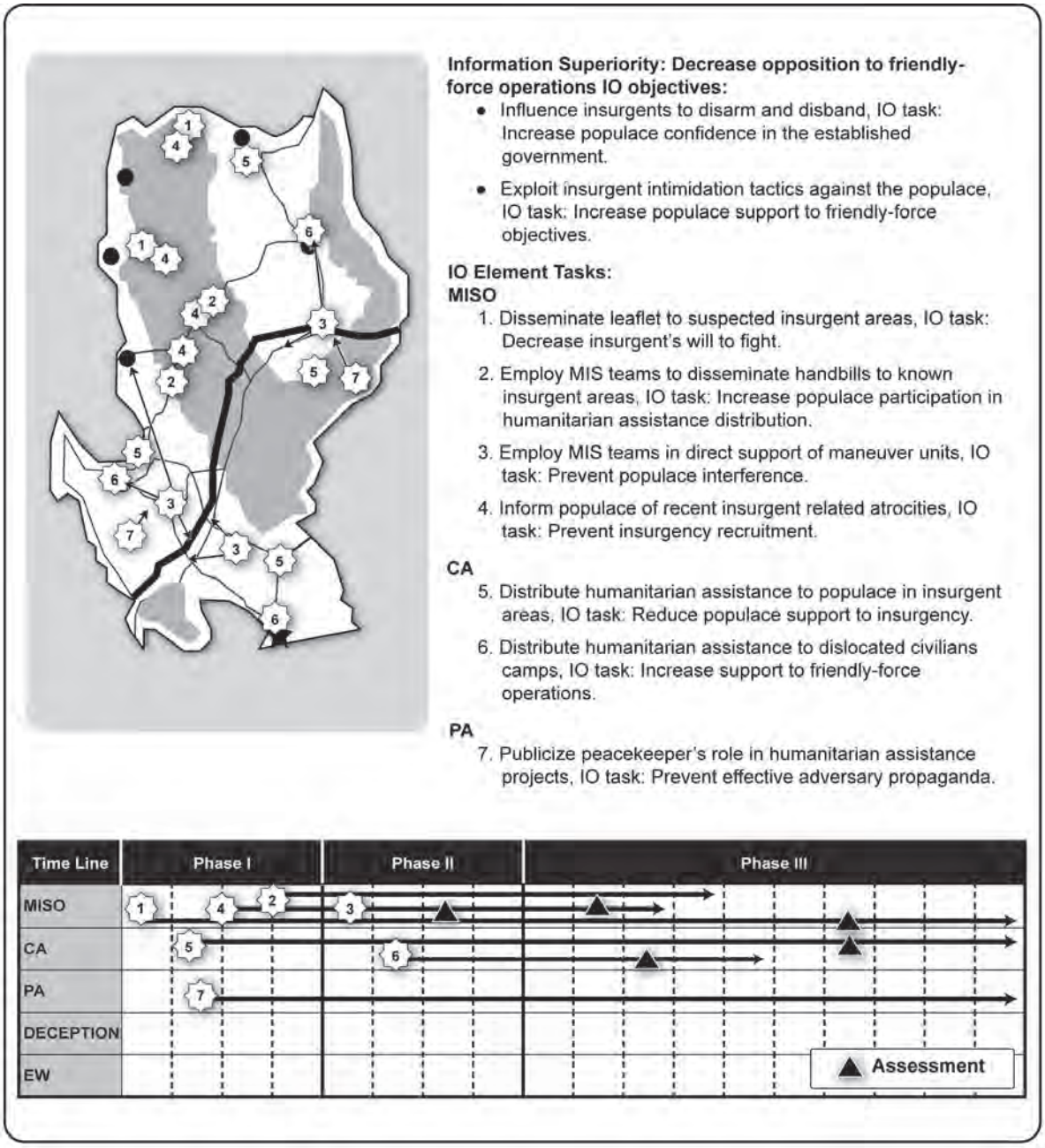


Figure 3-11. Example information operations concept of support sketch

ORDERS PRODUCTION

3-43. Plans and orders are as detailed as time permits. The size of these documents depends on the command and mission; they can run the gamut—from a series of overlays with written comments to voluminous documents of hundreds of pages. Regardless of the format used, an order must be clear, concise, timely, and useful to the implementing commands and units.

3-44. The IO annex (Army orders format) or appendix (joint orders format) describes the complete IO mission and how IO will gain information superiority in support of the scheme of the maneuver. This approach places a lesser emphasis on individual IO assets and capabilities and greater emphasis on the aggregate IO effects needed to achieve information superiority. The IO staff must be careful to not let the requirement to develop and explain IO capabilities contribution to the operation overwhelm the primary purposes of the IO annex, which are to—

- Provide operational details on the information operation.
- Focus element and unit tasks on achieving specific effects in the information environment.
- Provide the information needed to assess the information operation.

3-45. There are two basic formats for an IO annex: a five-paragraph (Figure 3-12, pages 3-16 and 3-17) and a matrix annex. The five-paragraph annex is used when sufficient planning time is available. The matrix annex is used when time is limited or when directed by the J-3/G-3/S-3 or unit SOP.

ANNEX P (INFORMATION OPERATIONS) TO OPERATIONS ORDER NO ##

1. SITUATION.

a. AO. Describe the information environment's subenvironments. Identify significant characteristics (for example, terrain, weather, populace, civilian information infrastructure, civilian population, and third-party organizations). State the aggregate impact on adversary and friendly operations. Identify aspects of the information environment, to include key information nodes that favor adversary and friendly operations.

b. Adversary Operations in the Information Environment. Describe how, when, where, and why adversary forces will operate in the information environment. Describe likely objectives and activities and how information capabilities will be employed. Identify adversary capabilities and vulnerabilities in the information environment in terms of information collection, protection, and projection.

c. Friendly Capabilities and Vulnerabilities in the Information Environment. Identify friendly-force capabilities to shape the information environment and attack adversary forces with information.

d. Civil Considerations. Identify key people, groups, and organizations that operate in the information environment and will affect friendly and adversary forces' operations. Describe likely objectives and activities in the information environment.

e. Attachments and Detachments. List organic and supporting assets that are available to execute the information operation.

2. MISSION. State the unit mission.

3. EXECUTION.

a. Concept of Support. Describe how IO will be conducted and who will perform it from beginning to end, to include adversary capabilities and vulnerabilities to be attacked and friendly critical vulnerabilities to be protected. Define information superiority (that is, the operational advantage derived from operating in the information environment) and explain how and when IO will achieve it. Include IO effects (that is, objectives or EIOTs), sequencing of key tasks, and IO capacities priorities by phase.

b. Assessment. Describe the assessment plan for the information operation.

c. Tasks to Subordinate Units. List subordinate units and assigned IO tasks.

d. Coordinating Instructions. List IO instructions common to two or more units. State any rules of engagement applicable to IO capability. List constraints not contained in the concept of support.

4. SERVICE SUPPORT. Identify requirements for support pertaining to IO as a whole. Identify service support to individual IO elements in their respective appendixes or annexes.

5. COMMAND AND SIGNAL. Significant command and signal information related to IO not covered in the base order. Include arrangements needed to exchange information among IO capabilities.

ACKNOWLEDGE: (If distributed separately from base plan/order)

Figure 3-12. Format for a five-paragraph information operations annex (Army orders format)

[Authenticator's last name]
[Authenticator's rank]

APPENDIXES:

1. OPSEC
2. MISO
3. MILDEC
4. EW
5. IO Execution Matrix

Figure 3-12. Format for a five-paragraph information operations annex (Army orders format) (continued)

3-46. Typically, at the tactical level, the information operation can be adequately described on a matrix order format (Figure 3-13). When combined with a copy of the IO concept of support sketch, most IO capabilities can understand and execute accordingly. There is no specific format for an execution matrix. Figures 3-14 and 3-15, pages 3-18 and 3-19, are two examples.

Enemy Situation: See Appendix 1 to Annex B	**Friendly Situation:** XXI Corps EC-130H, EC-130E, EA-6B, F-16CJ (HARM), AC-130 (Specter)
Mission: Prevent preemption of air assault; influence local population to not interfere in and around the objective; shape the information environment to establish order and provide basic services.	**Information Superiority:** Dominance of the information environment which permits mission success without effective opposition and minimal civil interference.
Concept of Support: Prevent preemption of the air assault and minimize civil interference in and around the objective by destroying, degrading, disrupting, and exploiting adversary mission command and fire support systems; deceiving adversary decisionmakers; destroying, degrading, disrupting, and deceiving enemy information systems; denying adversary decisionmakers information about XXI Corps intentions and capabilities; protecting mission command and information systems.	
IO Objectives/Tasks: Prevent compromise of the operation; protect XXI Corps mission command; disrupt 109th Division air defense and targeting systems during critical periods of the operation; minimize civilian interference.	**Assessment:**
Coordinating Instructions: XXI Corps: Contact counterparts to coordinate and synchronize efforts to identify suspected SPF locations.	
Service Support: No change.	
Command and Signal: XXI Corps IO cell is located in the Main CP.	
Appendixes: Appendix 1 (OPSEC), Appendix 3 (EW), Appendix 4 (IO Execution Matrix).	

Figure 3-13. Example of a format for a matrix information operations annex (Army orders format)

Capability	*Phase I*	*Phase II*	*Phase III*	*Phase IV*
EW	Monitor signals of interest. Electronic protection for personnel and equipment.	Electronic attack to disrupt enemy communications. Electronic protection for personnel and equipment.	N/A	N/A
MISO	Broadcast harassment messages for enemy. Broadcast noninterference messages for local populace.	N/A	Broadcast via mobile radio to keep population informed on mission.	Broadcast on mission success. Coordinate with combat camera crews for post-mission propaganda and counter-propaganda.
OPSEC	Determine essential elements of friendly information for mission.	Implement measures to protect essential elements of friendly information to protect movement routes, mission command, and objective.	N/A	N/A
CNO	Maintain computer network defense to protect friendly communications and information.	Maintain computer network defense to protect friendly communications and information.	Maintain computer network defense to protect friendly communications and information.	Maintain computer network defense to protect friendly communications and information.
MILDEC	N/A	N/A	N/A	N/A
CMO	Prepare Commander's Emergency Response Program paperwork for funds disbursement. Coordinate with provincial reconstruction team.	N/A	N/A	Assist personnel returning to villages. Assess small-scale immediate projects.
PA	Prepare press releases.	N/A	N/A	Send press releases. Control local and national media.
COMCAM	Document operation.	Document operation.	Document operation.	Document operation.
HN Forces	Take lead in all lethal actions on the objective.	Take lead in all lethal actions on the objective.	Take lead in all lethal actions on the objective.	Take lead in all lethal actions on the objective.
Other	N/A	N/A	N/A	N/A

Figure 3-14. Example 1 of an information operations execution matrix

Tasked Unit or System	*IO Task*	*Time on Target or Time of Effect*	*Location*	*Remarks*
EA6B	EW-01	H–1 through H-hour	Throughout area of operations	Successful if enemy is unable to send early warning
TPT	PSY-01	H–24 and continue	Objective LION	Successful if no civilian interference
95th Civil Affairs Brigade	CMO-01	H–24 though H-hour	Through area of operations	N/A
Special Instructions: None				

Figure 3-15. Example 2 of an information operations execution matrix

CONSIDERATIONS

3-47. IO planning can be initiated at the SFODA typically by the attached MIS element as the only information capability at that echelon, and finalized at the SOTF. Typically, an SFODA will not have access to all of the IO capabilities. When developing a concept of operations, planners must consider and include the applicable capabilities in Figure 3-14, page 3-18. The SOTF IO planner will coordinate for assets and synchronize and deconflict the effects. It is important for the SFODBs and SFODAs to understand the JSOTF/SOTF IO plans to ensure the higher HQ intent is nested within their plans.

CONSEQUENCE MANAGEMENT

3-48. When planning, the SFODAs should consider what actions to take if the operation does not go as planned. In the event that an operation does go awry, it is important to understand the information environment, to include the influential leaders that SFODAs and their FID partnered units should engage to assist in getting the appropriate information and messages to the populace. Also, it is important to note what media outlets are available to assist with getting ahead of the news cycle. Key consideration is that the first voice is the loudest. If the SFODA or the HN provides the facts of an operation or event in a timely manner, the adversary will be forced into defense and will have to react and counter the information as they fight to influence the population.

This page intentionally left blank.

Chapter 4
Execution of Information Operations

This chapter focuses on the key staff tasks IO planners must accomplish during execution of an information operation. Once execution begins, IO planners monitor the adversary and friendly situations, track IO task accomplishment, determine the accomplishment of the IO objectives and tasks, and detect and track any unintended consequences. Three staff tasks critical to execution include the following:

- *Monitor.* Planners must maintain situational awareness and monitor the progress of operations to determine if the operation is going according to plan.
- *Evaluate.* Planners analyze the progress of the information operation, the status of the adversary, and the effects in the information environment to determine if there are variances from the plan and the significance of the variances.
- *Adjust.* Planners estimate the effectiveness of task execution and the effectiveness of IO on the adversary, the local populace, and friendly operations. If an unexpected incident occurs, IO planners—in coordination with current operations staff—coordinate with subordinate units and staff elements to develop an appropriate task for that incident.

MONITORING

4-1. The key to monitoring is the collection of information critical to execution of the information operation. The first step is determining what information is needed to evaluate and adjust the information operation. Two sources for deriving the information are the CCIR and the J-2/G-2/S-2 decision support template. From these sources, IO planners can determine their own information requirements; notably, intelligence requirements and FFIRs that will help guide the information collection effort.

4-2. Next, IO planners monitor both the command's overall operation and the IO tasks and activities as spelled out in the operation order, IO appendixes, annexes, and execution matrices. Then, operations reports and intelligence summaries are reviewed for IO-relevant information and paired against the IO objectives to evaluate progress of the information operation. If necessary, requests for information are submitted and tracked for clarification or additional information.

EVALUATING

4-3. The purpose of the assessment is to judge success or progress of the information operation. Progress is determined by analyzing relevant information and intelligence from unit operations and intelligence reports. The information is then applied against current IO objectives to determine whether the desired effects are being achieved. However the assessment is conducted, planners should consider the following principles:

- The assessment should lead to recommendations to the commander to continue, end, or change the operation.
- The assessment must detect situation changes quickly enough for commanders to respond effectively.

Page 2994 of 3957

- A balanced assessment considers changes in both the friendly and adversary forces' information environment.
- The assessment of an information operation should focus on collective rather than individual tasks and targets, because changes in the information environment or adversary force usually are not the result of any single task or target.

4-4. Assessing IO can appear complex and difficult, but it need not be burdensome if IO planners use a simple methodology to assess the information operation. In principle, assessing an operation consists of evaluating the operations against measures of performance (MOPs) and MOEs.

Note. IO planners must be careful not to over assess by becoming bogged down in formal assessment procedures for numerous tasks and effects, or to overwhelm subordinate units or staff elements with requirements for numerous reports, questions, and information requirements.

4-5. MOPs measure friendly actions in terms of task accomplishment and performance. IO cannot generate effects if the planned tasks are not successfully executed. As such, assessment should account for task execution. Because task completion affects execution as well as assessment, it is important that the IO capability representatives and subordinate units report accomplishment of their respective tasks. MOPs are not measures of success—they gauge task completion and do not measure effect success or failure.

4-6. MOEs are used to measure the results achieved in the overall mission and execution of IO objectives. More practically, MOEs determine if a desired condition or outcome is in place (that is, effect), even if not directly caused by planned military action. Because IO objectives are written to articulate a specific condition or state in the operational environment, most MOEs are crafted and used to measure the effects generated by those tasks collectively executed to achieve each IO objective.

4-7. An assessment plan is normally developed as part of the planning process. For complex or long-term operations, it may be necessary to form an assessment working group to produce the information required to assess the information operation. Attendees to the working group may include representatives from the J-2/G-2/S-2; J-3/G-3/S-3; plans directorate of a joint staff (J-5); assistant chief of staff, plans staff section (G-5); MISO; EW; CA; and PA. During combat operations, the combat assessment board may supplant the assessment working group.

Note. One of the critical factors in a successful relief-in-place or transfer of authority between IO planners is the passing on of all historical IO data and ongoing assessment plans.

4-8. There is no standardized or doctrinal assessment process. In the absence of a doctrinal process, IO planners must develop their own methodology to guide assessment. Based on field experience, the following process is a logical approach to assessing an information operation:

- *Develop assessment criteria.* The first step in the assessment process is to develop the assessment criteria. This involves developing the items that support the MOE, indicators, and MOPs. One or more MOE is normally developed for each IO objective. Each MOE should clearly articulate the desired condition (effect) or end state that supports the associated IO objective. For example, for an IO objective to "reduce popular support for insurgents," an MOE could be "level of popular support to insurgents." Next, indicators are developed for each MOE. Multiple MOEs should be developed and used to determine if the IO objective is being achieved. Indicators for the MOE "increased reporting of insurgent activities" could include increased tips-line reporting, increased tips to patrols, and increased walk-in tips. MOPs assess task accomplishment. Example MOPs include the number of face-to-face interviews conducted, the number of handbills disseminated, and the number of radio broadcasts (all observable and measurable activities).
- *Define the measures.* Once MOEs, indicators, and MOPs are developed, IO planners establish a foundation for comparison and analysis (also known as *benchmarking*). Benchmarking determines the current state of MOEs and supporting indicators.

- *Collect and analyze data.* The next step is to identify sources of data needed to assess the MOEs, indicators, and MOPs. Data collection requirements should be kept as simple as possible. When possible, standard operations and intelligence reports are used as the means to collect the data. Figure 4-1 shows some data collection sources.
- *Provide recommendations.* Assessment should yield changes to execution (based on MOPs), changes to desired effects (based on MOEs), and changes to resource allocation. Recommendations based on the assessment should provide the commander with the bottom line, a recommended way ahead, and any issues requiring the commander's involvement.

Data Collection Sources	
Internal	Situation reports, intelligence summaries, current operations data, and other command reports.
Organic	HUMINT, CA, MISO, and PAO reports; significant acts database; subordinate unit assessments.
External	Other government agencies, international organizations, polling and populace surveys, media analysis, OSINT.

Figure 4-1. Sources of data collection

4-9. As the data is collected, it should be analyzed against the established indicators to establish the benchmarks. Follow-on data collection periods and assessments establish changes to the indicators and MOEs. The sum of indicators then provides the assessment for each MOE. Figure 4-2 shows an example of an assessment graphic.

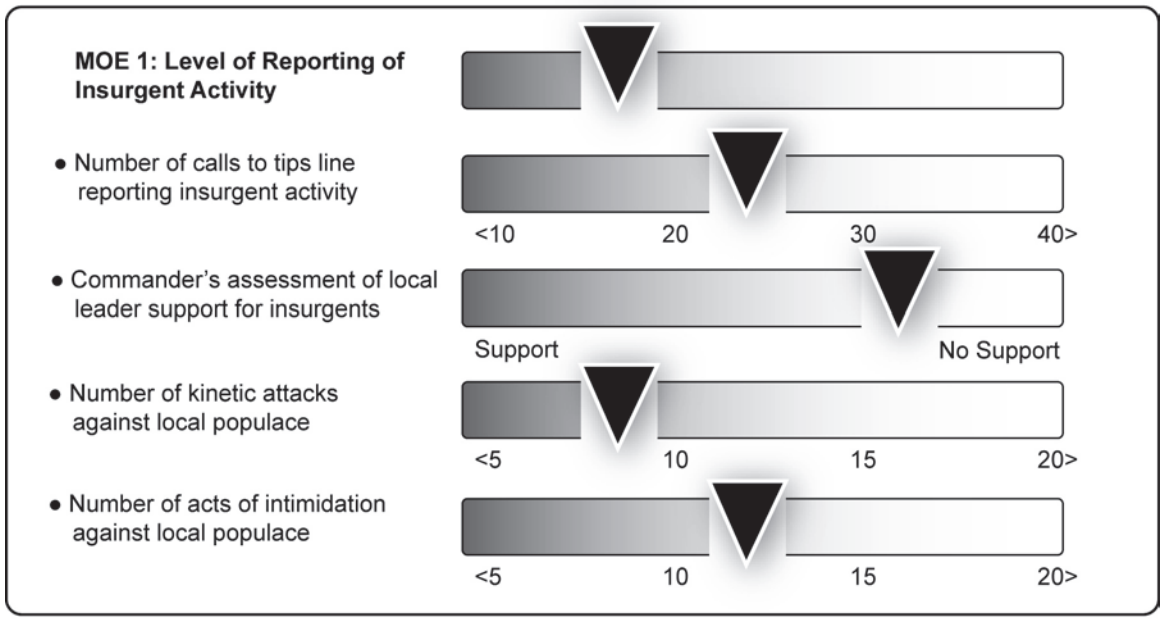


Figure 4-2. Example of an assessment graphic

ADJUSTING

4-10. The ways that IO planners can adjust the information operation in response to events in the information environment are battle drills, the IO working group, and crisis-action teams. In a best-case scenario, IO planning accounts for all possibilities and sets conditions for further operations. The information environment is never static, and planning for consequence management through battle drills and rehearsed crisis-action teams is critical to staying ahead of the adversary's information cycle. By the same token, proactive planning of synchronized IO efforts helps preclude reactive IO responses

for example, facilitating more timely and better prepared MISO and PA products and preplanned key-leader engagements.

BATTLE DRILLS

4-11. Staff battle drills are planning aids designed to speed response to crisis situations that occur during the conduct of a mission. For IO, quick responses to the adversary's actions and events in the operational area are necessary to beat the adversary in the information environment and ultimately achieve information superiority.

4-12. Battle drills are developed during the planning process; however, they are not complete and final COAs. Rather, battle drills are predeveloped concepts that anticipate crises. Once a crisis occurs, the battle drill (that is, the COA) can be quickly adjusted to address the realities of the situation at hand.

4-13. A military operation can be thought of as a series of events, planned and unplanned, that force both friendly and enemy forces to react to a changing situation. Some of these events, referred to as critical events, are keys to mission success of friendly or enemy forces. Critical events—

- Can create both intended and unintended effects and may be brought on by friendly, adversary, or third-party actions.
- Can be either negative or positive. The staff can develop drills that react to either type. For negative critical events, a battle drill should mitigate the impact of the event on the populace and friendly forces. For positive critical events, a battle drill should exploit the event to maximize the impact on the populace and adversary forces.
- Can be triggers or cues for the staff to initiate a battle drill.

4-14. An IO battle drill is a generic concept of support that addresses a friendly-force IO response to a critical event that may occur during execution of the operation. There is no established format for battle drills, though it should be recognizable to the staff and mirror existing products. Development of battle drills does not follow an established guide, but rather, they are developed to suit specific missions and potential branches and sequels of missions. Each battle drill should—

- Identify critical events.
- Define information superiority.
- Develop IO concept of support.
- Determine tasks and targets.

The information contained in a battle drill is not a final and complete plan, but rather a concept that must be refined to the realities of the situation at hand. Depending on the battle drill, productions of approved MISO products (such as radio scripts or other products) may be appropriate.

Identify Critical Events

4-15. Planners determine what critical events may result from friendly, adversary, or third-party action. During an upcoming operation, planners focus on events that will either occur in or affect the information environment and are significant enough to affect the command's mission. The following list provides some examples of critical events:

- Civilian collateral damage.
- Civilian casualties.
- Fratricide incidents.
- Populace interference with friendly-force operations (for example, civil demonstrations).
- Quick-reaction force deployment.
- Adversary or friendly forces violation of law of land warfare (for example, atrocities against civilians, mass-grave discovery).
- Environmental incident (for example, hazardous-material spill).
- Propaganda directed against friendly forces.
- EEFI or any other sensitive or classified information disclosure.

Define Information Superiority

4-16. Battle drills are designed to respond to a specific situation. Therefore, the situation must be sufficiently defined so the IO planners can adjust the battle drill's concept to compensate for the differences between the planned and actual situation. For IO, this means defining information superiority for each battle drill. Information superiority is the operational advantage provided to the commander through the control and management of information content and flow in the AO. Examples of information superiority for mitigation and exploitation battle drills are as follows:

- A mitigation battle drill:
  - *Event.* Disclosure of EEFI or classified information.
  - *Target.* Adversary.
  - *Information superiority.* Adversary decisionmakers are unable to take advantage of sensitive information about the friendly force.
- An exploitation battle drill:
  - *Event.* Destruction of key infrastructure by adversary.
  - *Target.* Populace.
  - *Information superiority.* Populace does not support the actions of enemy forces.

Develop Information Operations Concept of Support

4-17. The concept of support is a concise and easily understandable word picture describing how IO capabilities may be employed and what staff coordination must be conducted to employ the capabilities. The concept must be integrated with the overall operation, when applicable. How much information is known when the battle drill is created determines the level of detail. The IO concept of support should include the following:

- *Assumptions.* Planners list information accepted as true in the absence of facts at the time the battle drill is developed. Planners periodically review and update the battle drill by validating the assumptions.
- *Information superiority.* Planners determine and then describe the operational advantage IO will provide.
- *General scheme for IO.* Planners use doctrinal concepts and terms to explain how IO will achieve information superiority, listing any IO objectives, EIOTs, and who will perform each key task at what time.

Note. Where the tasks are performed is determined once the battle drill is put into action.

- *Priority of support.* Planners designate which subordinate unit or element has priority use of IO capabilities.
- *Constraints on IO.* Planners list prohibited and directed actions that are expected to affect the information operation, paying particular attention to information content and flow (for example, no jamming in urban areas).

Determine Tasks and Targets

4-18. Leaders develop tasks, purpose, methods, and means, and, if appropriate, targets for each participating IO capability. A purpose for each task is included to explain each capability's part in the operation. If appropriate, general target sets are identified for each tasked element or capability. All IO-relevant capabilities—maneuver units and those staff entities that may have important roles in responding to the battle drill event—are considered. A purpose for each task is included to maximize asset initiative. Supporting elements develop MOP for their assigned tasks.

Note. The formal battle drills are developed and coordinated at the SOTF level. The SOTF IO planner will use the 7-day mission tracker to ensure they are ready to provide support upon start of mission.

EXAMPLE STAFF BATTLE DRILL

4-19. There are several different battle drill formats currently in use. Figure 4-3 provides a sample format that has worked well in the field. Leaders should modify the format as needed to fit the command's needs and situation. Figure 4-4, page 4-7, provides an abbreviated staff battle drill.

SITUATION: Insurgent forces attack friendly forces, a friendly third-party organization, or an opposing faction (for example, a bombing, shooting, or mortar attack).

ASSUMPTIONS: The insurgent attack does not cause significant friendly causalities.

LIKELY FRIENDY ACTION: A response force is deployed to secure the site, and find and destroy the insurgent force. Security operations are conducted in and around the area of attack. If necessary, force protection measures are increased.

IO CONCEPT: The purpose of this IO is to gain populace support for counterinsurgency activities and identify hidden insurgent cells for targeting. IO capabilities provide direct support to the response force. MIS teams disseminate print products to the populace near the attack site. Unit leaders, MIS teams, and CA teams engage local leaders to gain support for friendly operations. PAO issues a press release to explain the command's position and counter misinformation concerning the situation. **Restrictions:** MISO products must conform to and support approved programs. **MOE:** Increased reporting of insurgent activity by populace.

Capability	*Key Tasks*	*Purpose*	*Method*	*Target*
MISO	Disseminate print products and radio broadcasts to the populace of villages in and around the attack site.	Identify hidden insurgent cells. Reduce populace support for insurgent forces and activities.	Handbills and posters. Contact radio.	Local populace. Insurgent fence-sitters.
CA	Engage local leaders.	Gain support for counterinsurgency activities.	Face-to-face.	Civil leaders.

Figure 4-3. Battle drill format for insurgent-related violence

INFORMATION OPERATIONS WORKING GROUP

4-20. An information operations working group (IOWG) consists of staff representatives who meet to coordinate and provide recommendations for the planning, execution, and assessment of IO. The IOWG also is used to synchronize the contributions of the IO capabilities. Participation in the IOWG is typically a mix of staff representatives and subject-matter experts.

Note. IOWGs are formed at the SOTF and JSOTF levels.

4-21. The frequency of IOWG meetings depends on the situation and echelon. The working group may gather daily, weekly, or monthly depending on the situation, echelon, and time available. The formality of the IOWG also varies by echelon. For purposes of organization and focus, even the simplest IOWG should have an agenda. The composition of the IOWG is tailored to the agenda. Representatives from every staff

need not attend every IOWG. Participants are selected because they either represent a critical element or capability or because they have expertise that is critical to the information operation. Typical attendees include the following:

- IO planners.
- MIS representatives.
- EW representatives.
- OPSEC representatives.
- COMCAM representatives.
- CA representatives.
- PA representatives.
- MILDEC representative.
- Representatives from the J-2/G-2/S-2.
- Representatives from the J-3/G-3/S-3, effects cell.
- Special technical operation planners.
- Fire support officer.
- Others, as required.

Note. Appendix A, pages A-1 through A-6, provides detailed information on IOWG.

1. **Situation:** React to collateral damage resulting from coalition-force action.
2. **Information Superiority:** Preempt adversary propaganda and negative media reporting.
3. **Immediate (on-site):**
   - Notify commander.
   - Document the scene (for example, COMCAM photos).
   - Conduct on-site key-leader engagement to determine facts and conduct initial mitigation.
4. **Within 2 Hours:**
   - Notify operational-area owner.
   - Notify local-government officials.
   - IO coordinates and synchronizes a public statement of the facts for broadcast by local print, radio, and TV media.
5. **Within 24 Hours:**
   - Conduct key-leader engagements with local elders using HN partner-unit commanders, coalition commanders, and local-government officials.
   - Assess damage for possible CMO projects.
6. **After 24 Hours:**
   - Coordinate for follow-up media coverage and key-leader engagement by operational-area owner.
   - Compensate family (if appropriate) and conduct CMO activities.

Figure 4-4. Abbreviated staff battle drill

CRISIS-ACTION TEAM

4-22. For significant operational matters, a crisis-action team may be activated. The crisis-action team consists of key members of the staff, to include the IO officer. When activated, the crisis-action team plans and rehearses the command's reaction to the event, and then issues a fragmentary order. To be a viable participant, IO planners should develop response options to support the crisis-action team planning process. When possible, IO planners use battle drills as the basis for adjustments to the information operation and tasks to the IO capabilities.

REPORTING

4-23. Significant events and friendly- and adversary-force activity in the information environment should be routinely reported to the J-2/G-2/S-2, J-3/G-3/S-3, and, as appropriate, the higher HQ' IO staff. The guiding principles for reports are to—

- Keep the report as simple and as short as possible.
- Include only that information which feeds a planning, assessment, or reporting requirement.

4-24. At the JSOTF, it may be useful to develop an IO intelligence summary or IO operation summary. Depending on the mission and tempo of the operation, these reports may be daily, weekly, or monthly products. The IO situation report is an event-driven report that provides basic information on significant activity in the information environment as it occurs.

INFORMATION OPERATIONS INTELLIGENCE SUMMARY

4-25. An intelligence summary is provided to subordinate commands, interested staff elements, and higher HQ. The primary focus of the report is to capture significant events in the information environment (focused on the IO planners' intelligence requirements) and assess their impact on friendly- and adversary-force operations.

INFORMATION OPERATIONS OPERATION SUMMARY

4-26. Subordinate units provide operation summary reports on the status of IO in their respective AOs. The primary focus of the report is assessment. The report provides recent significant activities, current and planned operations, capability status, and assessment of IO objectives, key tasks, and engagements.

INFORMATION OPERATIONS SITUATION REPORT

4-27. The purpose of the IO situation report is to provide an update since the last reporting period. An IO situation report is event-driven by significant changes to the characteristics of the subinformation environments with regard to information content and flow, or modifications to adversary actions that address the characteristics. The information in the situation report usually consists of the 5Ws (who, what, when, where, and why). Situation reports are rendered as needed.

4-28. At the SOTF level and below, an IO summary should be produced. The IO summary should include significant events in the information environment, focusing on—

- IO planners' intelligence requirements and assessments of their impact on friendly- and adversary-force operations.
- Recent significant activities, current and planned operations, capability status, and activities and assessment of IO objectives and key tasks.
- Engagements and significant changes to the characteristics of the subinformation environments with regard to information content and flow.
- Modifications to adversary actions that address the characteristics.

Chapter 5

Intelligence Support to Information Operations

Intelligence is the product resulting from the collection, processing, and integration of information and knowledge about adversaries and their networks obtained through observation, investigation, analysis, or understanding. IO planning and execution rely on the existing intelligence capabilities of the command to provide support. IO significantly increase the demand for intelligence and require detailed analysis of the information environment and the adversary's use of the information environment.

Intelligence support to IO is not solely an intelligence-community task. The intelligence staff is responsible for coordinating and overseeing all command intelligence; however, each staff section and element involved in planning and execution has a responsibility to assist in this task. Thus, IO planners should work closely with intelligence personnel throughout the intelligence cycle to ensure effective intelligence support, but they must also conduct their own research and analysis.

Intelligence support to IO is continuous and requires long lead times. The intelligence necessary to affect the perceptions and decisionmaking of adversaries or other audiences often requires that specific sources and methods be positioned and employed to collect the information and conduct the analyses needed for the information operation. The challenge is to get the right information and intelligence at the right time.

As in other intelligence activities, analysts should be careful not to describe or portray the adversary's actions in the information environment as a mirror image of U.S. IO concepts, doctrine, and TTP. Culturally, the adversary is unlikely to think or act as the United States does.

The key terms used in this chapter are defined below:

- *Information requirement.* Information requirements are information elements required for planning, executing, and assessing operations.
- *Intelligence requirement.* An intelligence requirement is a requirement for the intelligence system to fill a gap in the commander's and staff's knowledge or understanding of the operational environment or threat.
- *Priority intelligence requirement.* The commander designates PIRs. PIRs are requirements associated with a decision that affects mission accomplishment. Information requirements not designated by the commander as PIRs become intelligence requirements.
- *Intelligence estimate.* An intelligence estimate is an appraisal of available intelligence relating to a specific situation or condition with a view to determining the COAs open to the enemy or adversary and the order of probability of their adoption.
- *Intelligence preparation of the operational environment.* IPOE is an analytical methodology employed to reduce uncertainties concerning the enemy,

Page 3002 of 3957

environment, and terrain for all operations. IPOE builds an extensive database of potential areas where units may be required to operate. The database is analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and then presents the analysis in a graphic form. IPOE is a continuing process. In joint doctrine, IPOE is referred to as joint intelligence preparation of the operational environment.

INFORMATION OPERATIONS AND THE INTELLIGENCE CYCLE

5-1. All intelligence for the command and staff, to include that needed for IO, is produced as part of the intelligence cycle. By working closely with the J-2/G-2/S-2 during the intelligence cycle, IO planners can minimize intelligence gaps and maximize available intelligence and collection assets to develop a reasonably accurate understanding of the information environment and a representative and reliable model of adversary operations in the information environment. To integrate into the intelligence cycle, IO planners—

- Identify intelligence gaps (IO-specific) concerning the information environment and adversary operations in the information environment, develop PIRs, and submit requests for information to fill the gaps.
- Become familiar with available collection assets, capabilities, and support relationships (direct support or general support). Planners determine time requirements for each collection asset and consider the capabilities and limitations of the assets that will perform the mission.
- Coordinate with the collection manager to ensure information requirements for IO are considered for inclusion as collection tasks.
- Establish relationships with key intelligence personnel. Planners should not go directly to an analyst without awareness or concurrence of J-2/G-2/S-2 leadership.
- Vet all intelligence products developed from reachback support and other external sources through the J-2/G-2/S-2 to avoid disconnected analysis.
- Provide feedback on the quality of intelligence provided and its usefulness to facilitate refinement.
- Assess the intelligence support that is provided to improve the working relationship with the intelligence staff while providing feedback to the intelligence analyst for improvements.

INTELLIGENCE “PUSH” AND “PULL”

5-2. Intelligence is disseminated by either the “push” or “pull” principle. For “push,” IO planners must coordinate with the J-2/G-2/S-2 staff to get access to the dissemination means that have IO-pertinent products. This is accomplished by working with the intelligence analysts to get IO-specific information requirements injected into the collection cycle, nominating PIRs for either the information environment or adversary actions in the information environment, and coordinating with higher HQ IO staffs to get routine access to their intelligence products. To “pull” intelligence from the J-2/G-2/S-2 staff, IO planners should coordinate for access to those assets and systems that have IO-relevant information and intelligence, attend J-2/G-2/S-2 staff updates and fusion meetings, and coordinate with troop units and specialized teams (SFODAs, MIS teams, CA teams, and so on) to collect and report collateral information that is relevant to IO.

5-3. OSINT is an often overlooked way to get information and intelligence. Much useful information about the populace and media is available from public sources. This information often addresses the IO’s information and intelligence requirements. Like other aspects of planning, IO planners must be prepared to conduct their own OSINT gathering.

REQUESTS FOR INFORMATION

5-4. Intelligence production is requirements-driven. Requests for information are used to request specific information and intelligence. Each command has its own requests for information format and procedures; however, the following rules should be observed when developing requests for information:

- *Conduct initial research.* Units should try to find the information or intelligence on their own, using requests for information to get information that is not readily available. Sources already checked should be listed so the intelligence analyst does not waste time working with materials and products that do not have the requested information.
- *Clearly state the requirement.* Units should describe—as specifically as possible—what information is needed. Language and terms associated solely with IO should be avoided, as should requests for a particular type of intelligence (for example, SIGINT or HUMINT). Requests for information should be restricted to one question.
- *Justify the request.* Units must articulate why the request is important. For greater priority, units may try to tie the requests for information to a PIR.
- *State accurately the latest time the information will be of value.* Units should state when information will no longer be useful, being truthful about the date. The information that units provide affects collection management and assets dedicated for higher-priority missions.

INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

5-5. The basis of intelligence support to IO is the IPOE process, a prerequisite to planning any operation. The mechanics of analyzing the information environment and adversary operations in the information environment are generally the same as those established to support IPOE for other military planning. Ideally, the J-2/G-2/S-2 has the lead on conducting IPOE and will include IO considerations in the analysis. However, IO planners can expect to assist in the process or conduct portions of the IPOE that are specific to IO. In such a case, J-2/G-2/S-2 products should be used as the basis for any IO-oriented analysis.

5-6. Information IPOE differs from traditional IPOE in purpose, focus, and end state. The purpose of IPOE is to gain an understanding of the information environment in a specific geographic area and to determine how the adversary will operate in that environment. The focus is on analyzing the adversary's use of information to gain an advantage. The end state is the identification of adversary vulnerabilities that friendly forces can exploit with IO, and adversary capabilities in the information environment against which friendly forces must defend.

5-7. For IO, IPOE results in the production of a graphic visualization product known as the CIO. The CIO is a map of the information environment that shows where and how information content and flow will affect military operations.

VISUALIZING THE INFORMATION ENVIRONMENT

5-8. To employ IO properly, commanders and staffs must grasp the character and impact of the information environment in their operational area. To do this, it is necessary to rationally analyze the information environment using the IPOE process and the three-dimensional model of the information environment (as described in Chapter 1).

5-9. Every operational area has an information environment with information moving through it. This information flow (the information domain) creates tangible, real-world effects by converting real-world situations (the physical dimension) into human perceptions that form the basis of individual and organizational behavior (the cognitive dimension).

5-10. Visualization of the information environment begins with the identification of its significant characteristics. To do this, planners must examine the operating area and identify the existing and projected characteristics that are relevant to the content and flow of information (for example, Step 1 of IPOE).

Although there is no single set of characteristics useful for analyzing every information environment, some broad characteristics that can serve as starting points are terrain (weather), populace, civilian information infrastructure, civilian population, and third-party organizations. Figure 5-1 provides a broad list of characteristics of the information environment.

Significant Characteristic	*Elements of the Characteristic*	*Information Requirements*
Terrain	Those aspects of terrain and geography that impact information content and flow.	• How does terrain (and weather conditions) canalize and compartmentalize information content and flow? • How does terrain (and weather conditions) impact information flow?
Civilian Information Infrastructure	Key information system links and nodes (information conducts) in the operating area.	• What are the key information systems (telephone, microwave, Internet, and so on)? • What information content is passed on each information system? • Who (friendly forces, enemy, civilians, other organizations) uses each information system? • Who manages and controls the information systems?
Media	Radio, TV, print, and Internet, to include audiences.	• What media sources are available (for adversary and friendly use) in the AO? • What information content is reported by each media source? • Who is each media's audience? • What is the context or bias of the media outlets?
Civilian Population	• Demographics, such as distribution, language, religion, ethnicity, and education. • Cultural factors, such as societal structures, ideologies, perceptions, and beliefs.	• How does the populace communicate? • What information content does the populace need or want? • What are the populace's biases? • What is the populace's social organization? • What are the populace's cultural characteristics?
Third-Party Organizations	Interagency, nongovernmental organizations, private volunteer organizations, and international organizations that can be competing influences in the information environment.	• Who are the interagency, nongovernmental organizations, private volunteer organizations, and international organizations in the AO? • What are their purpose, goals, and objectives? • What information do these organizations project?

Figure 5-1. Visualization of the information environment

5-11. Planners analyze each of the previously identified significant characteristics using the three-dimensional model to determine specific impacts on operations in the information environment (that is, Step 2 of IPOE). To accomplish this task, each characteristic is considered within the framework of the three following dimensions:

- *Physical.* Units focus on what information systems in the operational area collect, process, and disseminate information. Identification should include the tangible aspects of each significant characteristic, such as technical information systems and networks (for example, radio towers, fiber-optic networks, and telephone networks) and nontechnical (human) information network nodes and links (such as persons with influence, key leaders, and face-to-face communications networks). Additionally, analysis should show where those information systems and networks are located in the physical environment.
- *Cognitive.* Units focus on the values, beliefs, and perceptions of key individuals and organizations in the operational area that make decisions, as well as how those decisions are formulated. This analysis should show how this human mental programming affects the value of specific information to those key individuals and organizations in the operational environment.
- *Information.* Units focus on how information flows and the content of that information. Flow describes the exchange of information in terms of conduits, form, and speed. Content includes the major subjects or topics circulating in the AO.

THE COMBINED INFORMATION OVERLAY

5-12. Analysis of the information environment should result in a CIO. The CIO (Figure 5-2, page 5-6) is not a static document; it is intended to be a working product that is continually refined as new information becomes available. Building a CIO begins with a map of the operational area (ideally the same map used by the intelligence and operations staffs). The information environment's significant characteristics are combined and plotted on the map to show aggregate effects in relation to the terrain of the operational area. This should result in the identification of subinformation environments.

5-13. Subenvironments are areas in which the information environment's significant characteristics and effects notably differ from adjacent areas. Because the composition of the information environment is not uniform, there will be distinct subinformation environments in the operating area. Physical features and cognitive aspects of the information environment determine subinformation environments. Leaders must consider that subinformation environments may transect international borders and unit boundaries. For example, subinformation environments may be based on the significant characteristics of ethnicity, media presence, and population density. One subenvironment may have a single ethnic group with widespread access to media and information, whereas another subinformation environment may have an entirely different populace group with limited or no access to outside media. The subenvironments can be further analyzed to determine their composition and character. Ideally, analysis will identify those parts of the operational area that favor either the friendly or adversary forces' operations.

5-14. After subenvironments are identified, key information nodes are selected within each subinformation environment. Information nodes are places, persons, or infrastructure that shape information content and flow by creating or transmitting information. Identifying key nodes is important because these areas may be the most-effective means for inserting messages into the local populace or adversary networks. The nodes critically affect information content and flow. Each subinformation environment will likely have one or more key information nodes. An information node can be human (for example, key communicators or leaders), technological (for example, cellular telephone towers, media outlets, and religious or meeting centers), or both. Nodes critical to both are key terrain in that they critically affect information within the operational environment and provide an advantage to either adversary or friendly forces. For example, a well-known mosque with an influential imam is a possible candidate for a key node because it creates or perpetuates information content affecting military operations.

5-15. The CIO is a guide, not a rigid template. It typically depicts mission-significant aspects of the information environment, subinformation environments, key information nodes, and information flow in the operating area. The information included in the graphic should be presented in a concise manner. Whatever final form the CIO takes, it must present an operationally-relevant overview of the information environment. Every CIO will be unique because every information environment is different.

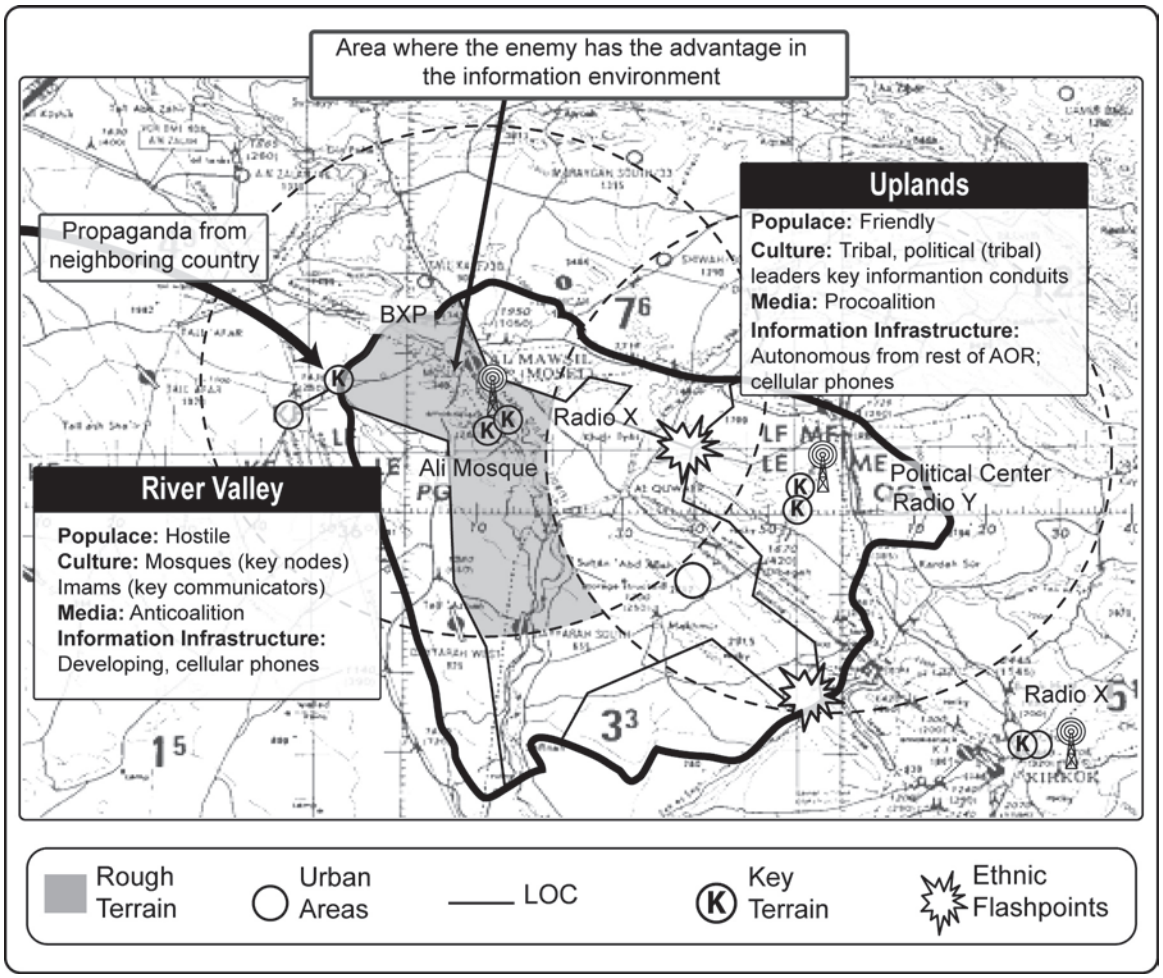


Figure 5-2. Example combined information overlay

ADVERSARY OPERATIONS IN THE INFORMATION ENVIRONMENT

5-16. Information and the information environment are not benign and often favor one side over another. Opposing forces use the information environment just as they use the physical environments of air, land, and sea to place their enemy at a disadvantage and to achieve their objectives. Understanding this, IO planners must identify how the adversary views and uses the information environment.

5-17. The adversary does not use the information environment in the same way or have the same constraints and means as U.S. forces. To avoid mirror-imaging the friendly concept of IO upon the adversary and to prevent mismatching U.S. capabilities and vulnerabilities, adversary operations in the information environment can be viewed in terms of activities to collect, protect, and project information. These three functions are universal to any armed force's ability to use information as combat power regardless

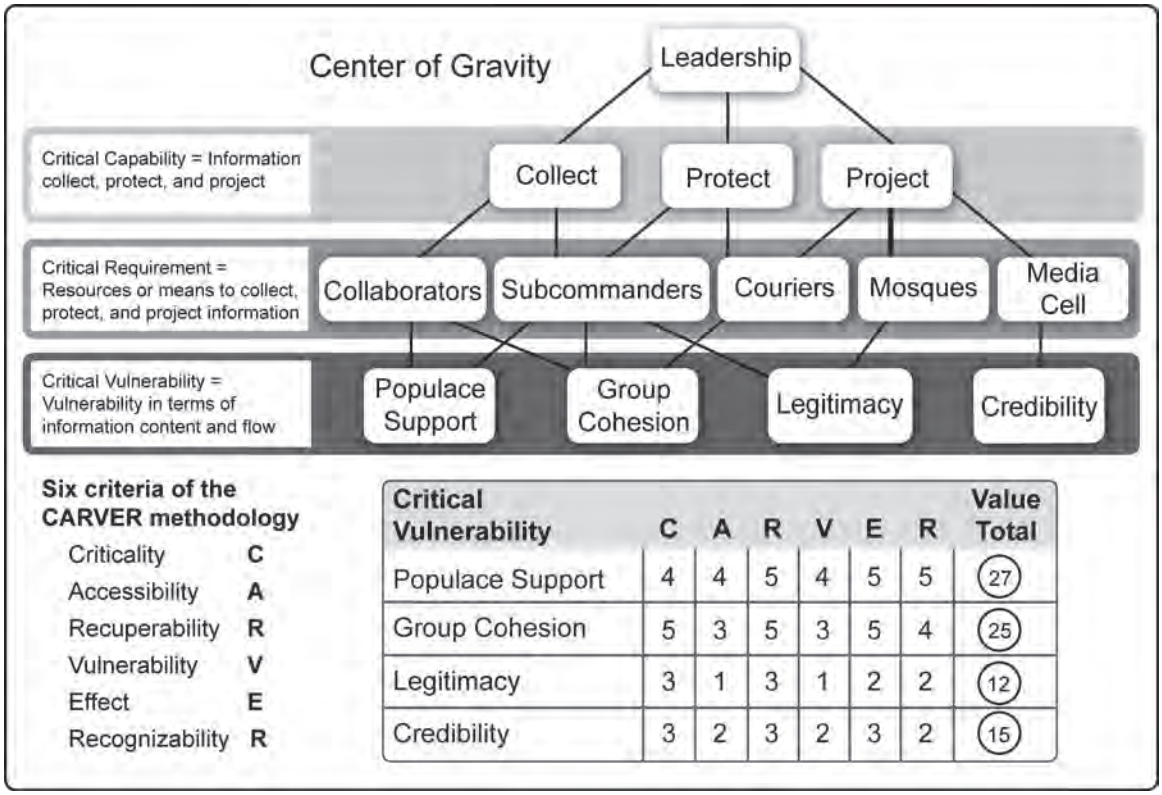
of its organization, capabilities, and mission. As such, they form the basis of the adversary's capabilities (and vulnerabilities) in the information environment. Collect, protect, and project are defined as:

- *Collect.* To plan and execute operations, the adversary must collect accurate and timely information.
- *Protect.* To be successful, the adversary must protect its critical information from collection and maintain its means of communication.
- *Project.* To further its goals and objectives, the adversary must project the information into the information environment to influence the perceptions of its target audiences.

5-18. Depending on the adversary, the means used can be as simple as direct human observation and open sources (collect); couriers and intimidation (protect); and night letters, other printed materials, and graffiti (project). Ideally, analysis of how the adversary operates in the information environment is based on modeling, or templating.

TEMPLATING USING CENTER-OF-GRAVITY ANALYSIS

5-19. Once a clear understanding of the environment is established, IO planners should analyze adversary capabilities, requirements, and vulnerabilities in the information environment (Figure 5-3). The purpose of performing a COG analysis is to determine and evaluate the adversary's critical vulnerabilities for exploitation. Because this tool is used to evaluate the adversary, the appropriate time to perform this analysis is during Step 3 (evaluate the threat) of IPOE. The results of the COG analysis are later used during COA development to exploit identified vulnerabilities.



Critical Vulnerability	C	A	R	V	E	R	Value Total
Populace Support	4	4	5	4	5	5	27
Group Cohesion	5	3	5	3	5	4	25
Legitimacy	3	1	3	1	2	2	12
Credibility	3	2	3	2	3	2	15

Figure 5-3. Example center-of-gravity analysis and the use of the CARVER process to rank and plot critical vulnerabilities in the information environment

5-20. The COG analysis of the adversary should be conducted by the J-2/G-2/S-2. If not, IO planners and operational detachments in the field can use a COG analysis to analyze the adversary in the information environment by—

- *Identifying potential threat COGs.* Visualize the threat as a system of functional components. Based upon how the threat organizes, fights, makes decisions, and its physical and psychological strengths and weaknesses, select the threat's primary source of moral or physical strength, power, and resistance. Depending on the level (strategic, operational, and tactical), COGs may be tangible entities or intangible concepts. To test the validity of the COG, the question that needs to be asked is: "Will the destruction, neutralization, or substantial weakening of the COG result in changing the threat's COA or denying its objectives?" When possible, the J-2/G-2/S-2 identifies the COG. If these assets are unavailable, then an independent information environment may need to identify the COG. Typically this is the adversary's information position, which is a way of describing the quality of information an organization possesses and its ability to use that information.
- *Identifying critical capabilities.* Each COG is analyzed to determine what primary abilities (functions) the threat possesses in the context of the operational area and friendly mission that can prevent friendly forces from accomplishing the mission. Critical capabilities are not tangible objects; rather, they are threat functions. To test the validity of a critical capability, the questions that need to be asked are: "Is the identified critical capability a primary ability in context with the given missions of both threat and friendly forces? Is the identified critical capability directly related to the COG?" A critical capability is a means that is a crucial enabler for a COG to function and, as such, is essential to the accomplishment of the adversary's specified or assumed objectives.

Note. The adversary's critical capabilities are the functions in the information environment—collect, protect, and project.

- *Identifying critical requirements for each critical capability.* Each critical capability is analyzed to determine what conditions, resources, or means enable threat functions or mission. To test validity of a critical requirement, the questions that need to be asked are: "Will exploitation of the critical vulnerability disable the associated critical requirement? Does the friendly force have the resources to affect the identified critical vulnerability?"

Note. Critical requirements usually are tangible elements such as communications means, nodes, or key communicators.

- *Identifying critical vulnerabilities for each critical requirement.* Each critical capability is analyzed to determine which critical requirements (or components thereof) are vulnerable to neutralization, interdiction, or attack. As the hierarchy of critical requirements and critical vulnerabilities are developed, interrelationships and overlapping between the factors are sought to identify critical requirements and critical vulnerabilities that support more than one critical capability. When selecting critical vulnerabilities, a critical-vulnerability analysis is conducted to pair critical vulnerabilities against friendly capabilities.

Note. Critical vulnerabilities may be tangible structures or equipment, or intangible perception, populace belief, or susceptibility.

- *Prioritizing critical vulnerabilities.* The CARVER is a special operations forces methodology to prioritize targets. The methodology can be used to rank-order critical vulnerabilities, thereby prioritizing the targeting process. The six criteria are applied against the critical vulnerability to determine impact on the threat organization as follows:
  - *Criticality* is the estimate of the critical vulnerability importance to the enemy. Vulnerability will significantly influence the enemy's ability to conduct or support operations.

- *Accessibility* is the determination of whether the critical vulnerability is accessible to the friendly force in time and place.
- *Recuperability* is the evaluation of how much effort, time, and resources the enemy must expend if the critical vulnerability is successfully affected.
- *Vulnerability* is the determination of whether the friendly force has the means or capability to affect the critical vulnerability.
- *Effect* is the determination of the extent of the effect achieved if the critical vulnerability is successfully exploited.
- *Recognizability* is the determination if the critical vulnerability, once selected for exploitation, can be identified during the operation by the friendly force, and can be assessed for the impact of the exploitation.

5-21. The result of the analysis should determine the adversary's vulnerabilities that can be attacked by friendly-force IO capabilities. Figure 5-3, page 5-7, provides a visual depiction of the relationship between critical vulnerabilities.

5-22. In testing the validity of the COG analysis, leaders should apply the following questions:

- Will destruction, neutralization, or substantial weakening of the COG result in changing the threat's COA or denying its objective?
- Does the friendly force have the resources and capabilities to accomplish destruction or neutralization of the threat COG? If the answer is no, than the threat's identified critical factors must be reviewed for other critical vulnerabilities, or planners must reassess how to attack the previously identified critical vulnerabilities with additional resources.

ADVERSARY ACTIVITIES IN THE INFORMATION ENVIRONMENT

5-23. As part of determining the adversary's COA (Step 4 of IPOE), IO planners should determine how the threat employs its assets to operate in the information environment and achieve information superiority over U.S. forces. To be valid, this analysis should be developed in concert with, and integrated into, the intelligence staff's analysis.

5-24. To graphically depict an adversary's COA in the information environment, planners start with the CIO and then add why (likely information objectives and actions), where (location of primary information assets and means), when (a forecast of when the adversary will employ its assets), and how (the employment of capabilities) the adversary will seek information superiority. The result is a concept of the operation that describes how the adversary will operate in the information environment. In turn, this product can be used during mission planning.

CONSIDERATIONS

5-25. Intelligence that may be considered less-than-credible or insignificant to a traditional intelligence analyst can be key to an IO planner. Some examples include the following:

- *Perceptions.* Planners use the target audience's existing perceptions to their advantage. Knowledge and understanding of existing perceptions of the population, insurgent groups, and HN government and forces can provide IO opportunities to exploit to achieve desired effects or counter the adversary's exploitation. Gaps in understanding perceptions can be answered using MIS teams, CA teams, and during the conduct of key-leader engagements. Examples of perceptions to exploit or counter include—
  - An insurgent group that believes a mole exists within their organization (exploit).
  - The populace believes that insurgents are forcing U.S. forces out of bases (counter).
- *Rumors.* Planners use rumors as a method to achieve an effect. IO planners look for various fissures in organizations to exploit and shape perceptions. Examples are—
  - Mistrust or jealousy among individuals.
  - Greed or desire for power.

- *Sensitive-site exploitation.* Soldiers conducting sensitive-site exploitation, should observe the location and mentally record information that may not be of immediate tactical value but can be used by IO planners to better understand the information environment. Questions that Soldiers should ask include—
  - Is there a TV? What channel is it on?
  - Is there a radio? What station is it on?
  - Are there periodicals? If so, what type are they? What language?
  - Are there music compact discs? What type of music?
  - How much food is in the house? Is it more than necessary to support the family?

Page 3011 of 3957

Appendix A

Planning Aids

This appendix provides multiple planning aids for Soldiers conducting IO missions. It outlines the duties and responsibilities of the IOWG and provides Soldiers with numerous mission analysis tools.

INFORMATION OPERATIONS WORKING GROUP

A-1. The IOWG brings together representatives of those staff elements concerned with the information operation. It is the most important meeting held by the assistant chief of staff, information operations (G-7)/information operations staff officer (S-7). The unit SOP should address the following for the working group:

- *Purpose.* The purpose of the IOWG is to synchronize the contributions of all staff elements to the work of the IO section.
- *Frequency.* The frequency of IOWGs depends on the situation and echelon. The working group may gather daily, weekly, or monthly, depending on the situation, echelon, and time available. Corps and division HQ may have daily (combat operations) or weekly (stability operations) IOWGs. Battalion and brigade HQ normally have fewer working groups than higher echelons.
- *Composition (chair and attendees).* The G-7/S-7 determines participation in the IOWG. It is a mix of staff-element representatives and subject-matter experts.
- *Inputs and outputs.* Attendees must know what information, products, and formats they are required to produce and use.
- *Agenda.* The formality of the IOWG also varies by echelon. For purposes of organization and focus, even the simplest IOWG should have an agenda.

COMPOSITION

A-2. The composition of the IOWG is tailored to the agenda. Representatives from every staff section need not attend each and every IOWG. Participants are selected because they either represent a critical element or capability, or have expertise that is critical to the IO. Core participants are staff members and subject-matter experts who regularly attend the IOWG due to their role in IO. Core participants include the following:

- IO personnel.
- MIS representatives.
- EW representatives.
- OPSEC representatives.
- COCAM representatives.
- CA representatives.
- PA representatives.
- MILDEC representatives.
- Representatives from the J-2/G-2/S-2.
- Representatives from the J-3/G-3/S-3, effects cell.
- Special technical operation planners.
- Fire support officer.
- Others, as required.

Page 3012 of 3957

A-3. There are other staff members who may not attend the IOWG on a regular basis, but whose role is no less important. They include the following:

- COMCAM officer in charge.
- G-6/S-6 representative.
- Cultural advisor.
- Chaplain.
- Political advisor.
- Subordinate-unit IO officers.
- Staff Judge Advocate representative.
- Liaison officers.

DUTIES AND RESPONSIBILITIES

A-4. Figure A-1 provides the duties and responsibilities of the IO working group members.

G-7/S-7	• Chair and facilitate working group. • Establish and enforce agenda. • Encourage active participation.
IO Capability Representatives	• Serve as subject-matter expert for their staff function or unit. • Provide input on capability status. • Provide input on current and future tasks and activities.
G-2/S-2 Representatives	• Provide intelligence relevant to IO. • Answer working group requests for information.
G-3/S-3 Representatives	• Provide input on current and future operations.
Subordinate Unit IO Representatives/Liaison Officers	• Serve as subject-matter expert for their unit. • Provide input on current and future missions, priorities, and tasks.
Recorder	• Record, write, and disseminate minutes of working group.
Other Participants	• Serve as subject-matter expert for their staff function or area of expertise. • Actively participate in the working group.

Figure A-1. Information operations working group duties and responsibilities

PREPARATION

A-5. Preparation is critical to a successful IOWG. A successful working group requires a collective effort from the IO section. For example, someone sets and prepares the agenda, another person notifies participants and ensures each is prepared to provide meaningful input to the working group, and another person prepares the IOWG presentation. Preparation tasks for the IWOG include the following:

- Set agenda.
- Notify participants:
  - Verify time and place of IOWG.
  - Identify additional participants.
- Review status of due-outs and contact those participants with due-outs.
- Coordinate with participants who have formal input.
- Publish a read-ahead packet:
  - If possible, provide IOWG materials to participants prior to the meeting.
  - Ensure participants provide input to IOWG presentation prior to the meeting.
- Assign a recorder to take minutes for the working group.

A-6. There are certain basics of meeting management that—if applied to the IOWG—can increase its effectiveness. Some basic suggestions include the following:

- Meet at established times and places.
- Keep meetings short—1 hour is a good rule of thumb.
- Have an agenda and follow it.
- Tailor working group membership to those people who are truly needed.
- Encourage participation by members; working groups are not one-way conversations.
- Complete detailed work and coordinate actions before the IOWG. Discuss actions and issues that are relevant to the working group.
- Identify and work critical issues. Identify and work side issues after the working group.
- Follow through on actions and due-outs. Record and track the results of the working group and publish minutes.
- Insist on timely delivery of due-outs and products.
- Invite subordinate and higher-command representatives.
- Give feedback to working-group members.

AGENDA

A-7. IOWG agendas vary by mission, situation, and echelon. A typical IOWG agenda includes the following:

- Roll call.
- Due-outs from previous IOWG.
- Intelligence update.
- Assessment update.
- Operations update.
- Discussion and issues.
- Review of due-outs.
- Conclusion.

A-8. Some IOWGs are organized along the lines of a targeting meeting, whereas others are similar to an operations meeting. Regardless of what agenda the IOWG takes, the purpose remains the same—to synchronize IO's contributing capabilities.

Due-Outs from Previous Working Group

A-9. Due-outs address unanswered questions or issues from the previous IOWG. Previous due-outs not answered during the IOWG should be carried over to the next IOWG for resolution. Typically, a due-out identifies the issue or question requiring resolution, and the person or element responsible for answering the due-out.

Intelligence Update

A-10. The purpose of the intelligence update is to answer current G-7 intelligence requirements. As such, it focuses on the information environment, the adversary's actions in the information environment, and the impact of those actions on friendly operations. Intelligence updates for IO should not be a regurgitation of other conventional intelligence updates. One way to structure the intelligence update is to capture significant events in the information environment and organize them by the G-7's intelligence requirements. Figure A-2, page A-4, provides a sample intelligence update format.

Assessment Update

A-11. The purpose of the assessment update is to assess the impact and effectiveness of current IO. Its focus is on analyzing and presenting information and intelligence from unit operations and intelligence reports, as well as input from the IOWG members. Figure A-3, page A-4, provides a sample of how the

assessment update can be depicted. Each operational area has a pie chart that represents the status of the current IO objectives (in this example there are five IO objectives).

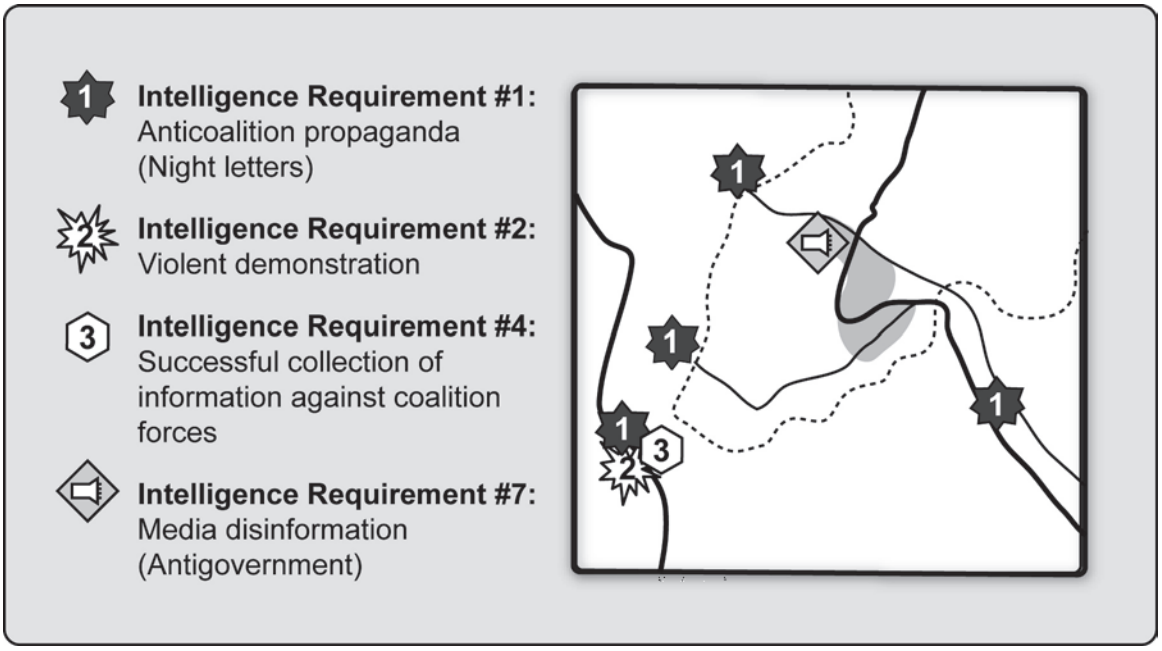


Figure A-2. Sample intelligence update format

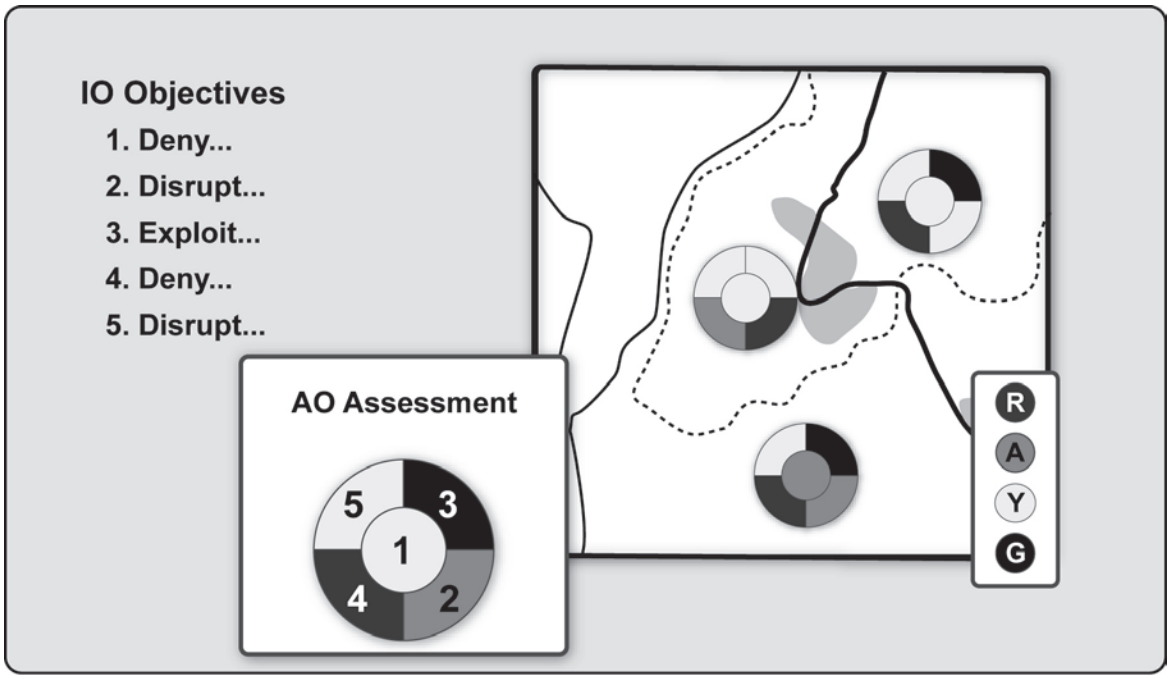


Figure A-3. Sample assessment update format

OPERATIONS UPDATE

A-12. The purpose of the operations update is to synchronize the IO objectives with element/capability tasks and targets for current and future (mid-range) IO. The focus is on gaining or maintaining information

superiority. One way to structure the operations update is to use graphics that show time, location, and purpose for key IO tasks for each major operation. Figure A-4 provides a sample format.

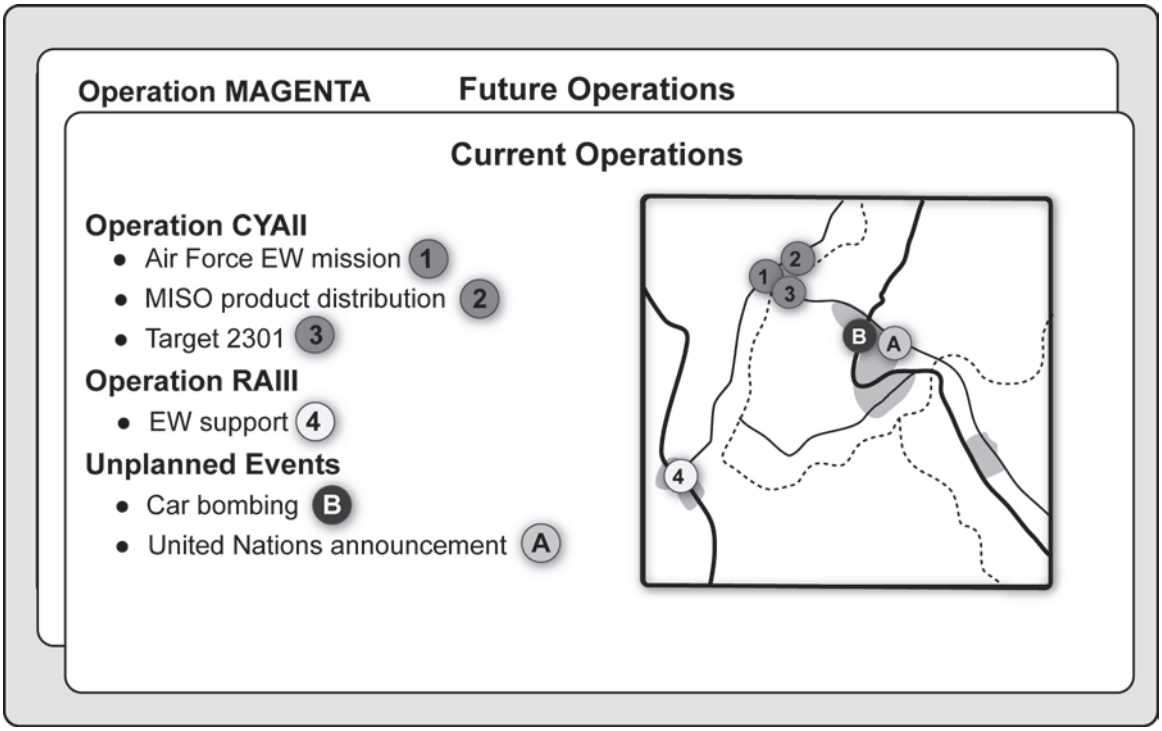


Figure A-4. Sample operations update format

Discussion and Issues

A-13. The purpose of the discussing issues or special topics is to support the G-7/S-7 decisionmaking and to synchronize the current and future activities of IO supporting capabilities. Discussion topics are selected by the G-7/S-7. Working-group participants have the opportunity (and responsibility) to discuss the topics from the perspective of their staff function or area of expertise. This discussion can be facilitated or focused by the use of an operations calendar (Figure A-5, page A-6) containing critical events and planned operations.

Review of Due-Outs

A-14. The purpose of reviewing due-outs is to ensure the working group participants understand and acknowledge their due-outs and responsibilities for the next meeting. Prior to final questions and comments, the G-7/S-7 reviews new due-outs identified during the working group as well as any open due-outs from the previous working groups. Each due-out should identify the issue or question requiring resolution, and the person or element responsible for answering the due-out.

Conclusion

A-15. The G-7/S-7 briefly discusses what the meeting accomplished and what working-group objectives were met. If necessary, side conversations, meetings, and other subworking groups are identified and scheduled.

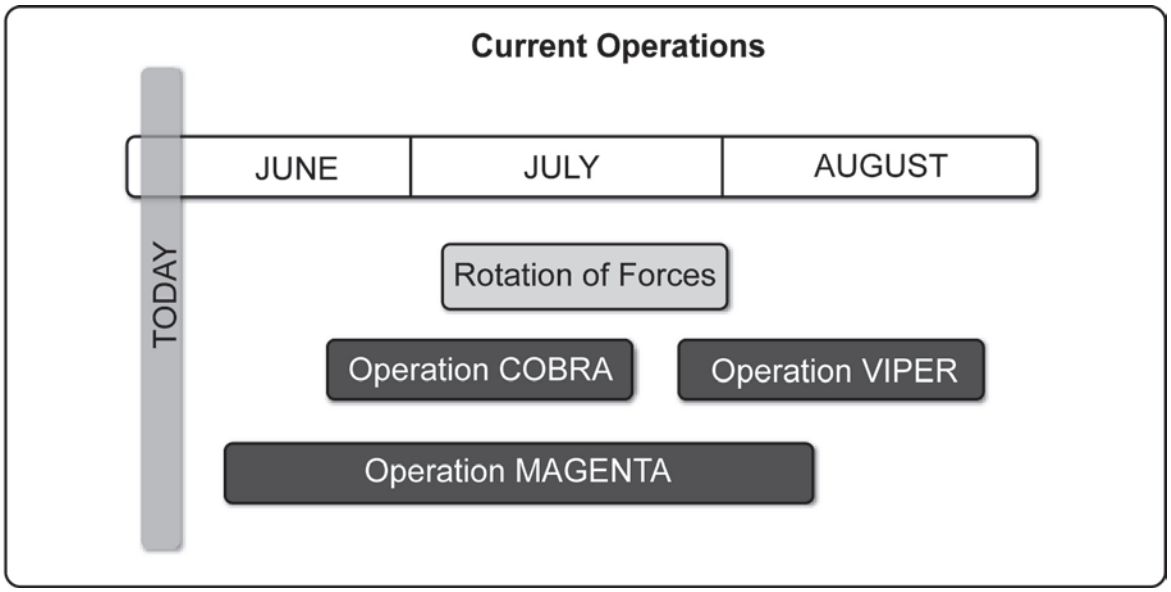


Figure A-5. Sample operations calendar

INFORMATION OPERATIONS PLANNING AIDS

A-16. Figure A-6 is an IO planning aid depicting the relationship between the military decisionmaking process and IO. Figure A-7, page A-7, depicts the relationship between IPOE and IO.

Military Decisionmaking Process Step	*Information Operations Focus*
Receipt of Mission	• Conduct initial assessment of information operation. • Determine IO planning requirements.
Mission Analysis	• Understand IO situation. • Analyze the higher HQ IO. • Define and analyze the information environment and threat. • Develop IO mission statement and objectives. • Seek commander's IO guidance.
COA Development	• Identify friendly IO capabilities and vulnerabilities. • Develop IO concept of support.
COA Analysis	• Visualize operations in the environment. • War-game IO concept of support against how the enemy will employ its information systems and assets.
COA Comparison	• Analyze and evaluate IO support to each COA.
COA Approval	• Finalize details of the information operation.
Orders Production	• Prepare IO annex and input to base operation order/operation plan.

Figure A-6. Information operations planning aid

A-17. The purpose of performing a COG analysis (Figure A-8, page A-7) is to determine and evaluate the adversary's critical vulnerabilities for exploitation. Because this tool is used to evaluate the adversary, the appropriate time to perform this analysis is during Step 3 (evaluate the threat) of IPOE.

A-18. In testing the validity of the COG analysis, leaders should apply the following questions:

- Will destruction, neutralization, or substantial weakening of the COG result in changing the threat's COA or denying its objective?
- Does the friendly force have the resources and capability to accomplish destruction or neutralization of the threat COG? If the answer is no, then the threat's identified critical factors must be reviewed for other critical vulnerabilities, or planners must reassess how to attack the previously identified critical vulnerabilities with additional resources.

Intelligence Preparation of the Operational Environment Steps	*Information Operations Focus*	*Analysis Product*
Define the operational environment.	Define the information environment.	Combined information overlay—significant characteristics of the information environment and effects on operations.
Describe the operational environment's effects.	Describe the information environment's effects.	
Evaluate the threat.	Evaluate the threats' information system.	• Threat COG analysis—critical vulnerabilities. • Threat templates—who makes decisions; what nodes, links, and systems the threat uses; how information assets are employed.
Determine threat COAs.	Determine threat actions in the information environment.	Information situation template—when, where, and why the threat will seek to gain information superiority.

Figure A-7. Relationship between intelligence preparation of the operational environment and information operations

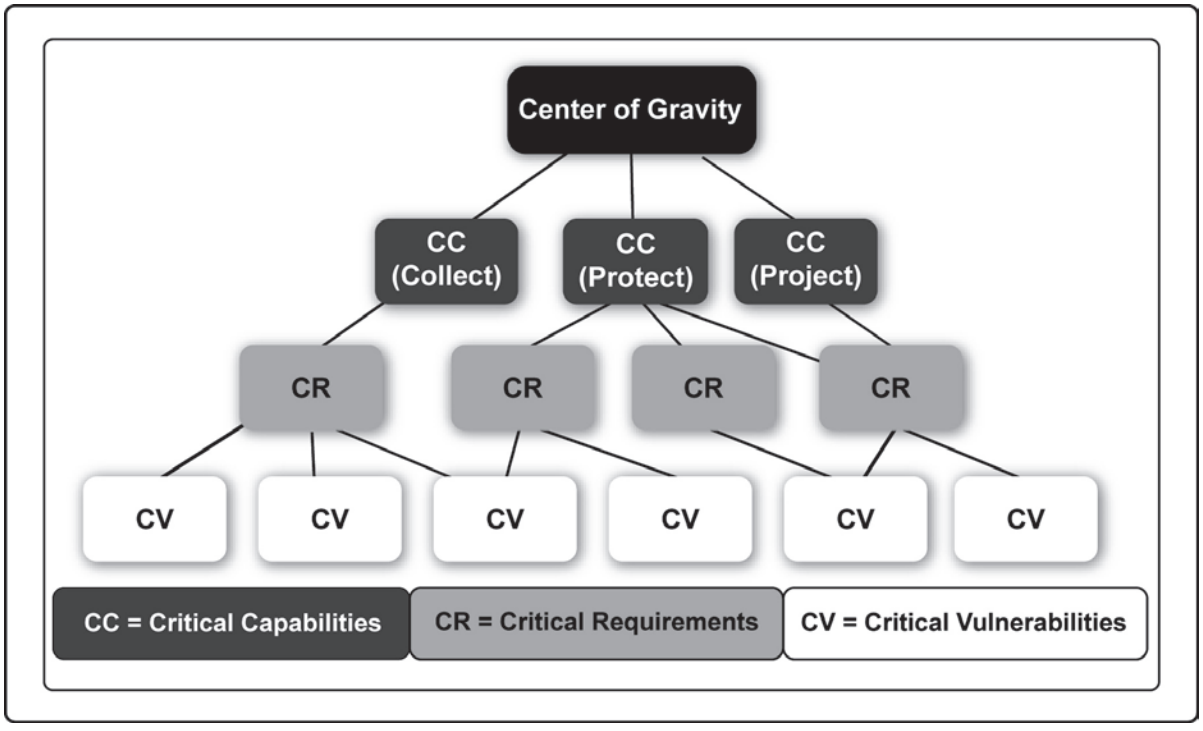


Figure A-8. Sample center-of-gravity analysis

A-19. Figure A-9, page A-9, is a sample combined information overlay. Figure A-10, page A-9, depicts a sample IO mission-to-task product chart. Figure A-11, page A-10, depicts a sample IO mission and tasks (tactical level). Figure A-12, page A-10, depicts a sample COA sketch.

A-20. In addition to doctrinal effects, IO have a number of nondoctrinal effects, to include the following:

- *Destroy.* This renders a target so damaged that it cannot function as intended nor be restored to a usable condition without being rebuilt.
- *Degrade.* This reduces the effectiveness or efficiency of adversary information systems, assets, or functions.
- *Disrupt.* This temporarily interrupts the flow of information.
- *Deceive.* This misleads or manipulates adversary understanding of friendly forces' activities, capabilities, vulnerabilities, and intentions.
- *Influence.* This affects an adversary or others perceptions, attitudes, and behavior to support friendly-force objectives.
- *Preserve (nondoctrinal).* This maintains the effectiveness or efficiency of friendly-force information systems, assets, or functions (related to doctrinal effect *protect*).
- *Deny.* This hinders or prevents an adversary and others from gaining access to, collecting, or using information concerning friendly forces.

A-21. Possible IO tasks include the following:

- Control.
- *Counter.*
- Counter-reconnaissance.
- Defeat.
- Delay.
- *Demonstrate.*
- Destroy.
- *Deter.*
- *Engage.*
- Fix.
- *Inform.*
- Interdict.
- Isolate.
- *Jam.*
- Neutralize.
- *Persuade.*
- *Prevent.*
- *Protect.*
- Secure.
- Suppress.

Note. Italicized tasks are proposed IO tactical tasks.

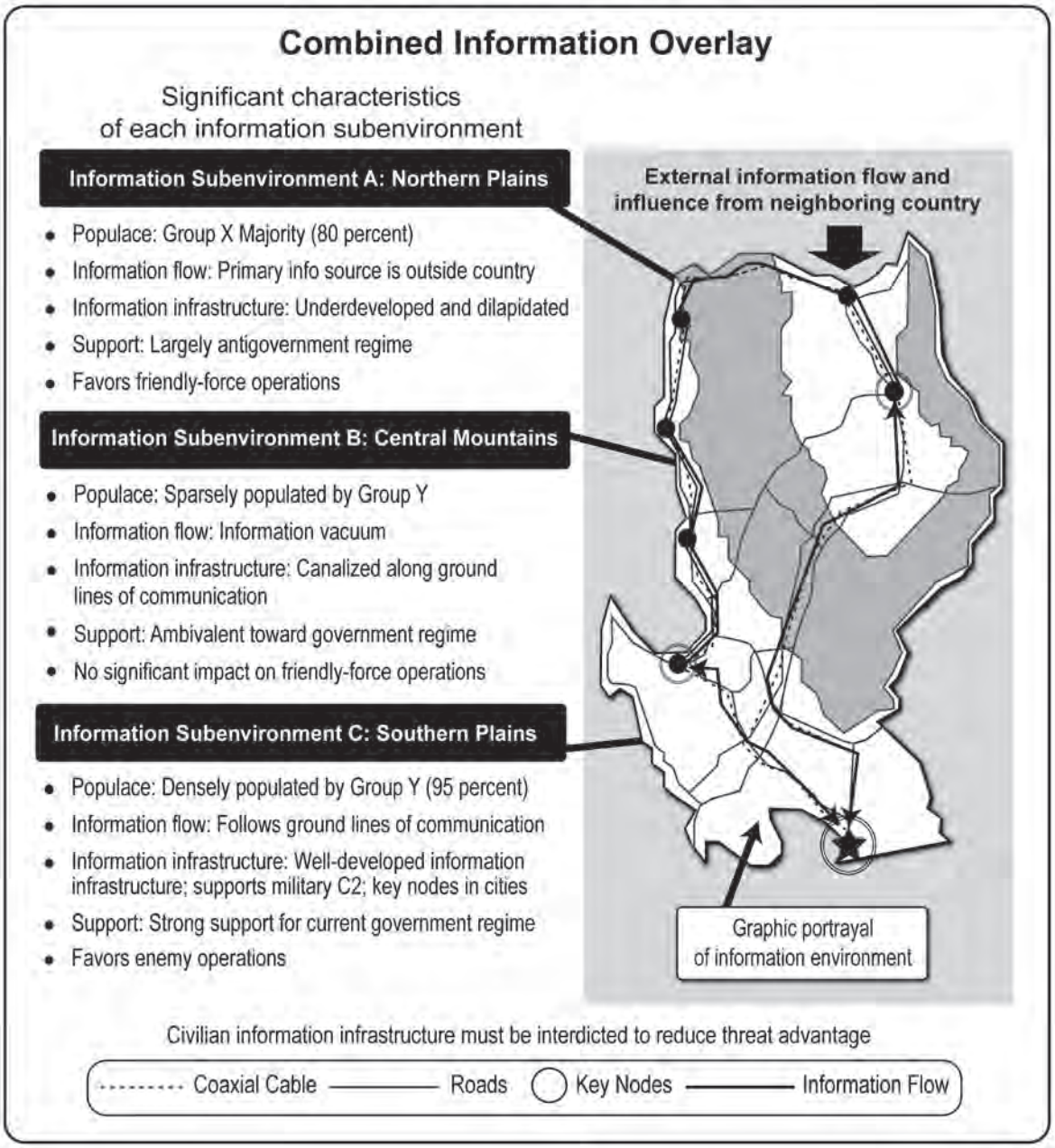


Figure A-9. Sample combined information overlay

Mission	*Tasks Products*
IO Mission Statement	How IO will support the command's mission (who, what, where, when, why).
IO Objectives (3 to 5 Objectives per Phase)	What IO will do to affect the information environment (effect, object of the effect [target], purpose of the effect).
Tasks to IO Elements	What actions the elements will perform to execute the information operations (task, purpose).
Tasks to Units	Task, purpose.
IO Concept of Support	How the information operation will be conducted (commander's intent for IO, information superiority for the operation, general plan for IO, priority).

Figure A-10. Mission-to-task products

IO Mission: On order, the friendly force disrupts the enemy ground and air defense forces' C2, influences civilian populace perceptions, and protects Corps' critical information in the AO to facilitate destruction of 1st Operational Strategic Command forces.

IO Objectives:

- Disrupt the enemy force's air defense C2 to prevent coordinated engagement of the friendly force's deep attacks.
- Disrupt operational reserve command posts and communication networks to delay employment of reinforcing or counterattack forces.
- Influence civilian populace in occupied areas to minimize interference with the friendly force's operations.
- Deny detection and identification of the friendly force's main and tactical command posts to prevent targeting by the enemy force's artillery fires.

Figure A-11. Sample information operations mission and tasks (tactical level)

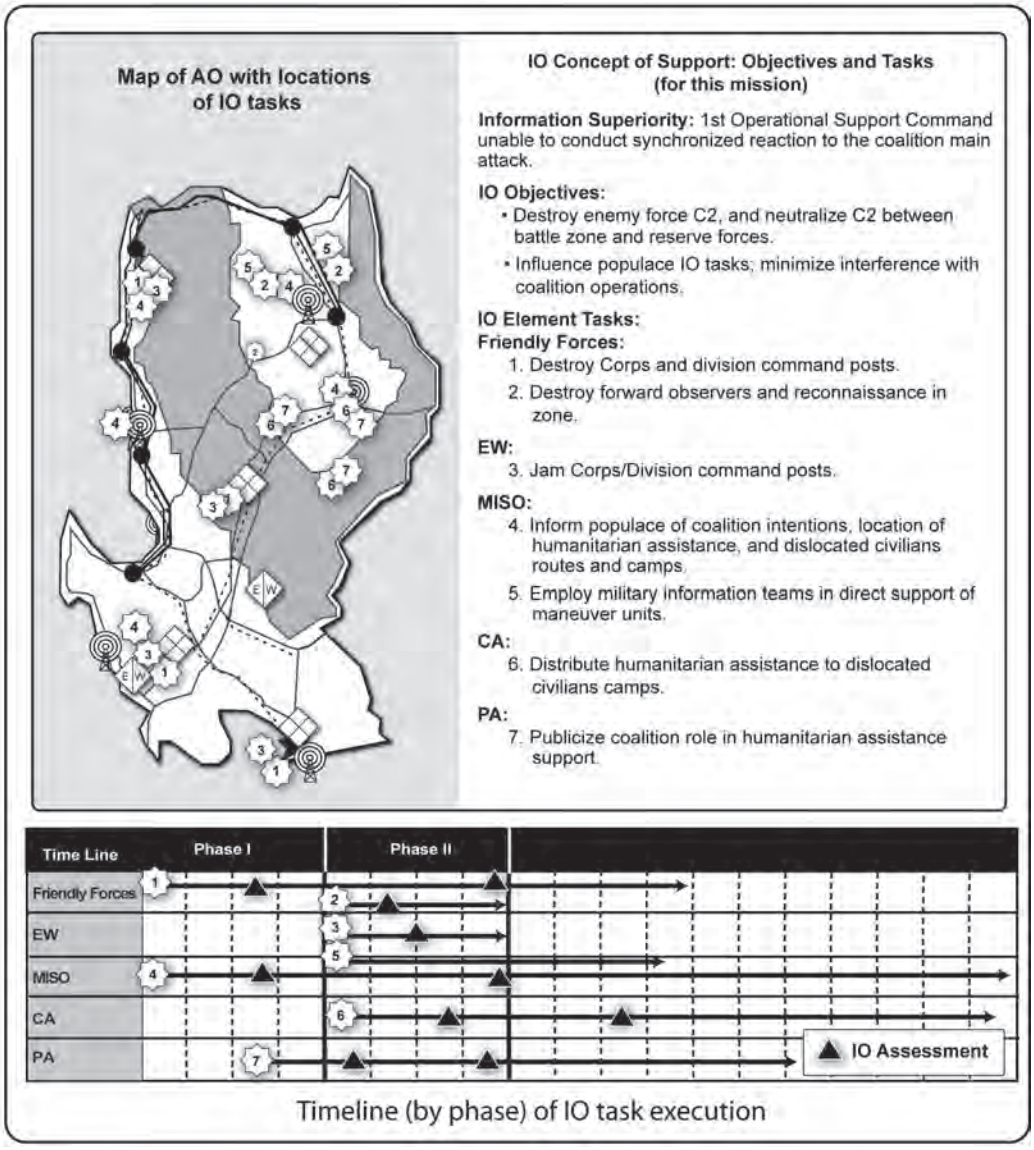


Figure A-12. Sample course-of-action sketch

MISSION ANALYSIS AND INFORMATION OPERATIONS

A-22. As part of the planning process, the IO staff must conduct its own mission analysis. Figure A-13 depicts the relationship between IO and mission analysis.

Military Decisionmaking Process Step	*Information Operations Focus*
Analyze Higher HQ Order	Analyze the higher HQ IO.
Perform IPOE	Define information environment and determine threat COAs.
1. Determine Tasks	Determine what the IO must do.
2. Review Available Assets	Determine organic and support IO capabilities.
3. Determine Constraints	Determine constraints on information content and flow.
4. Identify Facts and Assumptions	Identify facts and assumptions relevant to information content, flow, and use.
5. Perform Risk Assessment	Input hazards resulting from IO tasks.
6. Determine CCIR and EEFI	Determine EEFI.
Determine Intelligence, Surveillance, and Reconnaissance Plan	Input information requirements for IO.
Update Timeline	Input lead time for IO tasks.
Write Restated Mission	Write IO mission statement (if used).
7. Deliver Mission-Analysis Briefing	Input to mission-analysis briefing.
Approve Restated Mission	Approve IO mission statement (if used).
Develop Commander's Intent	Input to commander's intent.
Issue Commander's Guidance	Issue guidance for IO.
Issue Warning Order	Input for IO.
Review Facts and Assumptions	Address changes to IO planning factors.

Figure A-13. Mission analysis and information operations

A-23. Figure A-14, page A-12, provides a sample mission-analysis work sheet. The mission-analysis work sheet—

- Provides a tool to conduct mission analysis.
- Focuses on the minimum information needed for a plan.
- Follows the sequence of the mission-analysis briefing format, not the steps of mission analysis.

A-24. Identify specified and implied tasks to IO; not tasks to the capabilities. Tasks to the capabilities may be a constraint because they allocate resources away from the IO. Specified tasks are tasks specifically assigned to a unit by its higher HQ. Implied tasks are tasks that must be performed to accomplish a specified task or the mission, but are not stated in the higher HQ order.

A-25. IO tasks ignore staff coordination, administrative, and SOP tasks (for example, conducting a weekly IOWG, or submitting daily reports). Leaders organize identified specified and implied tasks to improve clarity. Tasks may be divided into two categories—

- Tasks to shape the information environment and to engage enemy forces.
- Tasks associated with information flow and information content.

A-26. Essential tasks are specified or implied tasks that must be executed to accomplish the mission. Leaders select three to five essential tasks, which are approved by the commander during the mission-analysis briefing.

1. **Facts:** Situation remains that the enemy will continue to use improvised explosive devices, small-unit attacks, and ambushes to attempt to gain strength for its cause. Friendly forces will continue to find and engage the enemy to eliminate improvised explosive devices. Current strength remains at 90 percent. Troops in the area of operations remain on the offensive and material readiness remains at 90 percent.
2. **Assumptions:** Attacks will continue to increase as the weather continues to improve, allowing for more insurgents and better leadership. This has been the pattern over the last several years and by all indications will continue.
3. **Tasks:** a. Specified: Detachments within the area of operations will continue to hunt for suspected insurgents and find, fix, capture, or eliminate as situation dictates. Additionally, detachments will continue to provide support to coalition forces and provide humanitarian support to the host nation. b. Implied: Continue offensive operations against insurgents. Continue to provide operational support to coalition forces and provide humanitarian support and security for the host nation. c. Essential: Provide for security and protect essential elements of friendly information. Provide training support to host-nation and coalition forces and conduct offensive operations to deter and eliminate insurgent activities in concert with collation partners.
4. **Constraints:** Close air support is authorized in rural areas. The use of close air support in urban areas must be approved by regional commander. Cultural support team will interrogate women and children only and detachments will provide security, as applicable.
5. **Available Assets:** All organic detachment equipment will be used, to include combat controllers, interpreters, Civil Affairs teams, Military Information Support teams, provincial reconstruction teams, and coalition support. Current rules of engagement remain in effect. Avoid using themes that will denigrate host-nation forces, such as cultural and religious themes. All releases to the media must first be approved by the public affairs office.
6. **Risk Assessment:** Improvised explosive devices will remain a constant threat. Weather conditions will hamper aviation and air support.
7. **CCIR:** In order to maintain the offensive, the commander needs to know current situational status and personnel status for both U.S. and coalition forces. a. PIR: Commander needs a clear and concise understanding of the enemy strengths and weaknesses; the disposition of forces and key leaders. b. FFIR: Commanders need a clear and concise understanding of coalition and friendly forces within the area of operations—specifically, which units are available to support detachments if needed, to include other ongoing operations within the detachment area of operations.
8. **EEFI:** Protection of intelligence requirements. Mission of higher and friendly forces within the area of operations, infiltration and exfiltration routes, unit strength, and communications must be protected.

Figure A-14. Example of a mission-analysis work sheet

Review Available Assets

A-27. Leaders examine available assets to determine IO capabilities and limitations, considering both organic and supporting assets based on current task-organization, support relationships, and status of units. Assets are compared to specified, implied, and essential tasks to determine if there are enough assets to accomplish all tasks. It may be useful to translate assets into IO capabilities (effects and targets). Figure A-15, page A-13, provides a sample matrix to help in this comparison.

Organization	*Asset*	*Means*	*Supported Essential Task*	*Effect*	*Target*
Organic Assets					
Tactical Psychological Operations Company	1 x Product Development Detachment 9 x Tactical Psychological Operations Teams	Face-to-face Loudspeaker Handbills Posters Radio Television	N/A	Influence Inform Deceive	Local populace
Military Intelligence Company	3 x Prophet	Electronic attack	N/A	Disrupt	Enemy communication
Civil Affairs Battalion	12 x Tactical Support Teams	Face-to-face Humanitarian assistance Medical assistance Reconstruction projects	N/A	Influence Inform Co-opt	Local civilian leaders Local populace
Supporting Assets					
CFACC	EA6B EC130	Electronic attack Electronic support	Disrupt Degrade Destroy Inform Influence		Division-level communications Corps-level communications

Figure A-15. Example of an information operations asset/capability matrix

DETERMINE CONSTRAINTS

A-28. Constraints are restrictions on the use and employment of IO. The two types of constraints are prohibited actions (cannot do) and directed actions (must do; that is, resources and assets are required to do something). Constraints affect the use of IO capabilities and may be found in base orders, annexes, and appendixes. Constraints may be organized by affect on information content and flow (Figure 3-4, page 3-6).

FACTS AND ASSUMPTIONS

A-29. Facts and assumptions establish an understanding of the situation. Facts are known data concerning the situation. Assumptions are accepted as true in absence of facts. Leaders focus on facts and assumptions that concern assigned tasks. Figure A-16, page A-14 provides a sample fact and assumption analysis. Facts and assumptions may be organized as follows:

- Information environment (content and flow).
- Adversary capabilities and vulnerabilities in the information environment.
- Friendly capabilities and vulnerabilities in the information environment.

Information Environment	• Local populace is illiterate. (Fact) • Radio primary means to reach populace. (Fact) • Populace is pro-United States. (Fact) • Local leaders can control populace behavior. (Assumption)
Adversary Forces	• SIGINT is limited to short-range very high frequency radio. (Fact) • Use satellite and cell phones for C2. (Fact) • Will direct adversary information against U.S. forces. (Assumption)
Friendly Forces	• Friendly forces can jam the enemy's C2. (Fact) • Friendly forces can use local radio stations. (Assumption)

Figure A-16. Example of a fact and assumption analysis

RISK ASSESSMENT

A-30. Leaders identify and assess risks in the information environment arising from the essential tasks for IO. Risk assessment has five steps:

- Identify hazards (accomplished during mission analysis).
- Assess hazards (accomplished during mission analysis).
- Develop controls.
- Determine residual risk.
- Implement controls.

A-31. IO planners identify two kinds of hazards (risks). Tactical risk is concerned with hazards that exist because of the presence of the enemy or adversary. Accidental risk includes risks to friendly forces, to civilians, and the operation's impact on the environment.

INPUT TO COMMANDER'S CRITICAL INFORMATION REQUIREMENT

A-32. The CCIR identifies the information needed for direct execution of the mission. There are two types of CCIRs—PIRs and FFIRs:

- PIRs are information the commander must know about the enemy. For IO, PIRs focus on conditions in the information environment and threat actions to affect the information environment.
- FFIRs are information the commander must know about the friendly force. For IO, FFIRs focus on the friendly force's capability to shape information content and flow.

ESSENTIAL ELEMENTS OF INFORMATION

A-33. EEFI is information that must be protected from the adversary's intelligence system. Sources of information for developing EEFI are commander's guidance, facts, assumptions, and essential-task lists, and the intelligence estimate (information about adversary intelligence capabilities and requirements). EEFIs are written as statements, not questions; otherwise, EEFI may be confused with PIRs. Figure A-17, page A-15, provides an example.

PIR	• What information systems is the adversary using for C2? • What means is the enemy using to disseminate propaganda? • Is adversary information turning popular opinion against operations?
FFIR	• Media coverage of alleged friendly force's misconduct. • Civilian casualties caused by friendly-force operations.
EEFI	• Friendly force's means of intelligence collection. • Tribal leaders who are assisting friendly forces.

Figure A-17. Example of a commander's critical information requirement and essential elements of information for information operations

MISSION-ANALYSIS BRIEFING

A-34. The IO portion of the briefing is included either in the G-3 and G-2 planners' presentations or, when appropriate, developed as separate slides. IO input typically includes the following:

- *Mission.* Commander's intent for IO of HQ two levels up and own commander's IO guidance.
- *IPOE.* CIO and enemy COAs in the information environment.
- *Facts and assumptions.* Critical facts and assumptions for IO.
- *Tasks.* Specified, implied, and essential tasks for IO.
- *Constraints.* Restrictions on the use and employment of IO.
- *Forces available.* Organic and supporting IO-capable assets and their capabilities and limitations.
- *Risk assessment.* Risks in the information environment.
- *CCIR.* Input to PIR, FFIR, and EEFI.
- *Timeline.* Input to the time allocation plan for accomplishment of IO essential tasks.
- *Restated mission.* IO mission statement (if used).

INFORMATION ENVIRONMENT CONSTRUCT

A-35. Figure A-18 depicts the different dimensions of the information environment and their key characters.

Information Environment Dimensions	*Key Characteristics*
Cognitive • Individual and collective consciousness • Where decision are made	• Beliefs • Values • Perceptions • Awareness • Decisionmaking
Information • Intersection of physical and cognitive dimension • Where information is created and exists	• Information content • Information flow • Information functions—collect, project, protect
Physical • The physical world—land, sea, air, and space • Where information systems and networks reside	• Technological information systems, Internet, media • Human—societal organization, military formations, third-party organizations

Figure A-18. Information environment

DEFINE INFORMATION ENVIRONMENT

A-36. Leaders define the information environment by examining the AO to identify the following significant characteristics of the cognitive, information and physical dimensions:

- *Terrain.* Canalization and compartmentalization.
- *Civilian information infrastructure.* Key links and nodes.
- *Media.* Radio, TV, print, and Internet, including audiences.
- *Civilian population:*
  - Demographics, such as distribution, language, religion, ethnicity, and education.
  - Cultural factors, such as societal structures, ideologies, perceptions, and beliefs.
- *Third-party organizations.* Nongovernmental organizations, private organizations, criminal organizations.

A-37. The information environment variances by level of war are depicted in Figure A-19.

Tactical	Physical	• Terrain and weather. • Local information systems. • Face-to-face contact.
	Information	• Line-of-sight flow. • Content addresses immediate needs.
	Cognitive	• Immediate perceptions and behavior.
Operational	Physical	• Regional information systems.
	Information	• Over-the-horizon flow. • Content addresses higher-level issues and concepts.
	Cognitive	• Near-term group perceptions and behavior.
Strategic	Physical	• Mass, long-distance information systems.
	Information	• Global flow. • Content addresses abstract ideas, ideologies, and philosophies.
	Cognitive	• Long-term perceptions and beliefs.

Figure A-19. Information environment variances by level of war

DESCRIBE THE INFORMATION ENVIRONMENT'S EFFECTS

A-38. Leaders analyze each significant information environment characteristic in detail and plot the data in a template (such as the sample provided in Figure A-20, page A-17).

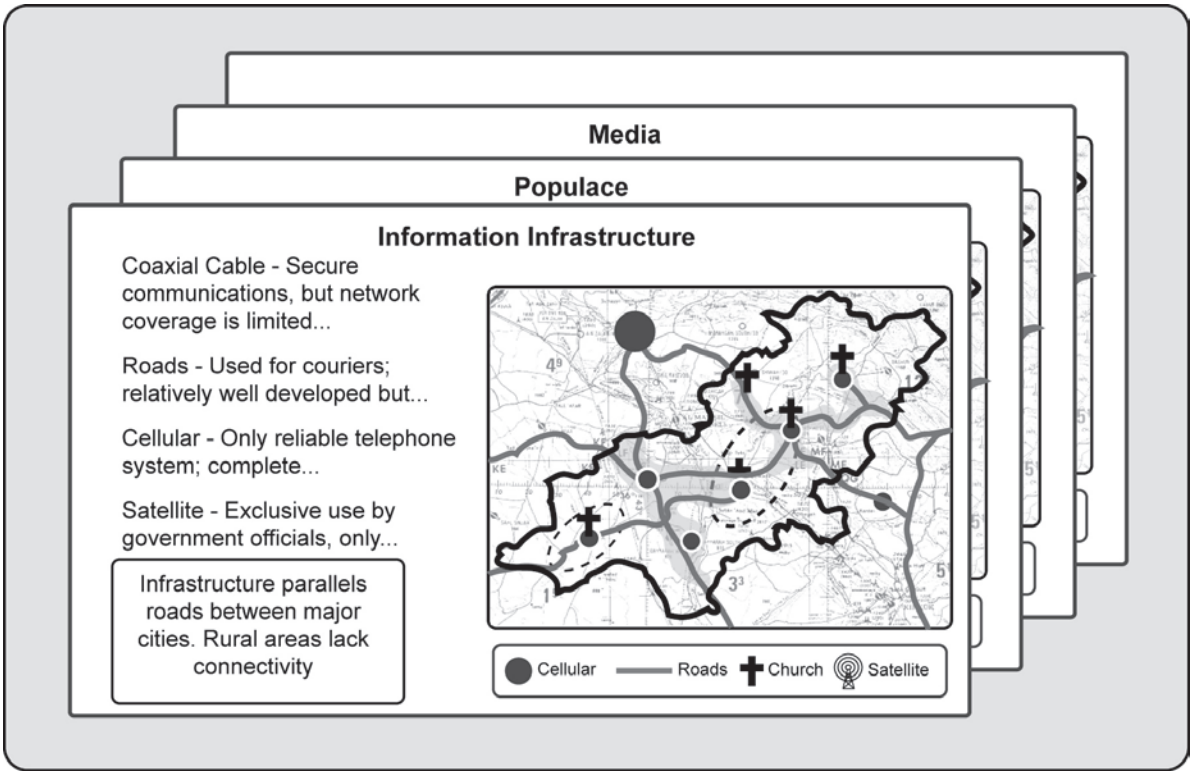


Figure A-20. Sample information environment effects matrix

Describe Subinformation Environment and Key Nodes

A-39. By identifying and acting on key nodes, a military force can affect the information environment. Subinformation environments are areas in which the information environment's characteristics and effects are notably different from those of adjacent areas. Subinformation environments—

- Are determined by physical features and cognitive aspects of the information environment.
- Are formed by interactions of physical and cognitive dimensions.
- Determine an advantage to the friendly or adversary force.

A-40. Information nodes are key terrain in the information environment. Information nodes are places, persons, or infrastructures that shape information content and flow by creating or transmitting information. Information nodes—

- Exist in each subinformation environment.
- Can be human, technological, or both.
- Are located at the center of information content and flow.
- Critically affect information flow and content.
- Provide an advantage to one side or the other.

Combined Information Overlay

A-41. The CIO is a graphic depiction of where and how the information environment's effects will impact military operations. Figure A-21, page A-18, provides a template for a CIO. Figure A-22, page A-19, provides a sample CIO. The CIO—

- Depicts subinformation environments and key nodes.
- Describes information flow in the operating area.
- Includes a "so what" analysis.

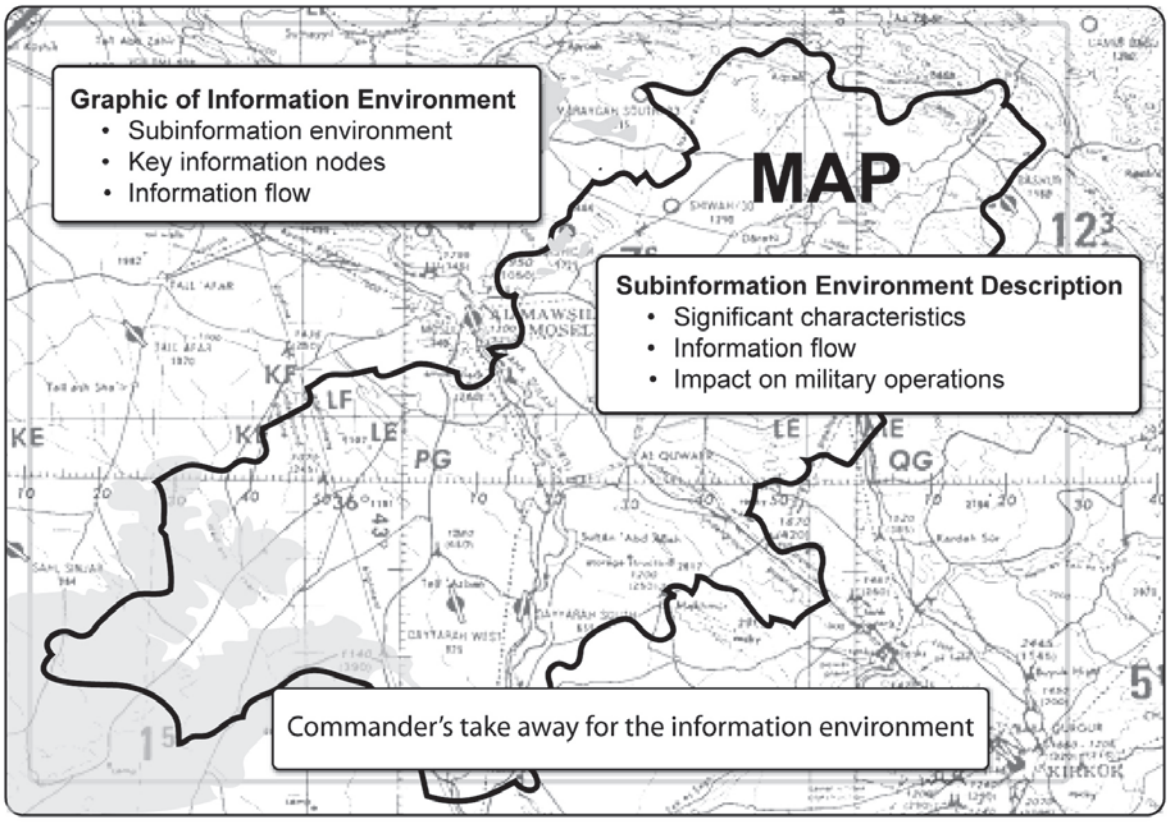


Figure A-21. Combined information operations overlay template

EVALUATE THE THREAT—CENTERS OF GRAVITY

A-42. The purpose of performing a threat COG analysis is to determine and evaluate the enemy's (and others') critical vulnerabilities for exploitation. Because this tool is used to evaluate the threat, the appropriate time to perform this analysis is during step 3 (evaluate the threat) of IPOE. The results of COG analysis are later used during COA development to exploit identified vulnerabilities. Chapter 5, Templating Using Center-of-Gravity Analysis, page 5-7, provides additional information.

A-43. The COG analysis of the threat should be conducted by the G-2. The IO staff will provide input to the COG analysis and use it to determine what aspects of the threat IO should engage. Figure A-23, page A-20, provides a graphical depiction of where the COG analysis falls into the military decisionmaking process.

EVALUATE THE THREAT—TEMPLATING

A-44. More formal modeling produces templates that portray the normal or doctrinal (historical) composition and organization of the adversary's information system and its assets. The result should identify adversary capabilities and vulnerabilities under ideal conditions in the information environment. Templates will vary widely by operation—the examples provided are illustrative only.

Decisionmaking Template

A-45. The decisionmaking template identifies who makes decisions. Its purpose is to identify key leaders, organizational structures, linkages and interrelationships, key decisionmakers, and decisionmaking characteristics. Figure A-24, page A-20, provides a sample decisionmaking template.

Information Infrastructure Template

A-46. The information infrastructure template identifies what assets and means the adversary uses to collect, protect, and project information. The template identifies critical adversary information system nodes, links, and systems (to include those assets capable of impacting the information environment). Figure A-25, page A-21, provides a sample information infrastructure template.

Information Tactics Template

A-47. The information tactics template identifies how the adversary will collect, protect, and project information. It identifies adversary tactics, past use of information, and available assets. Figure A-26, page A-21, provides a sample information tactics template.

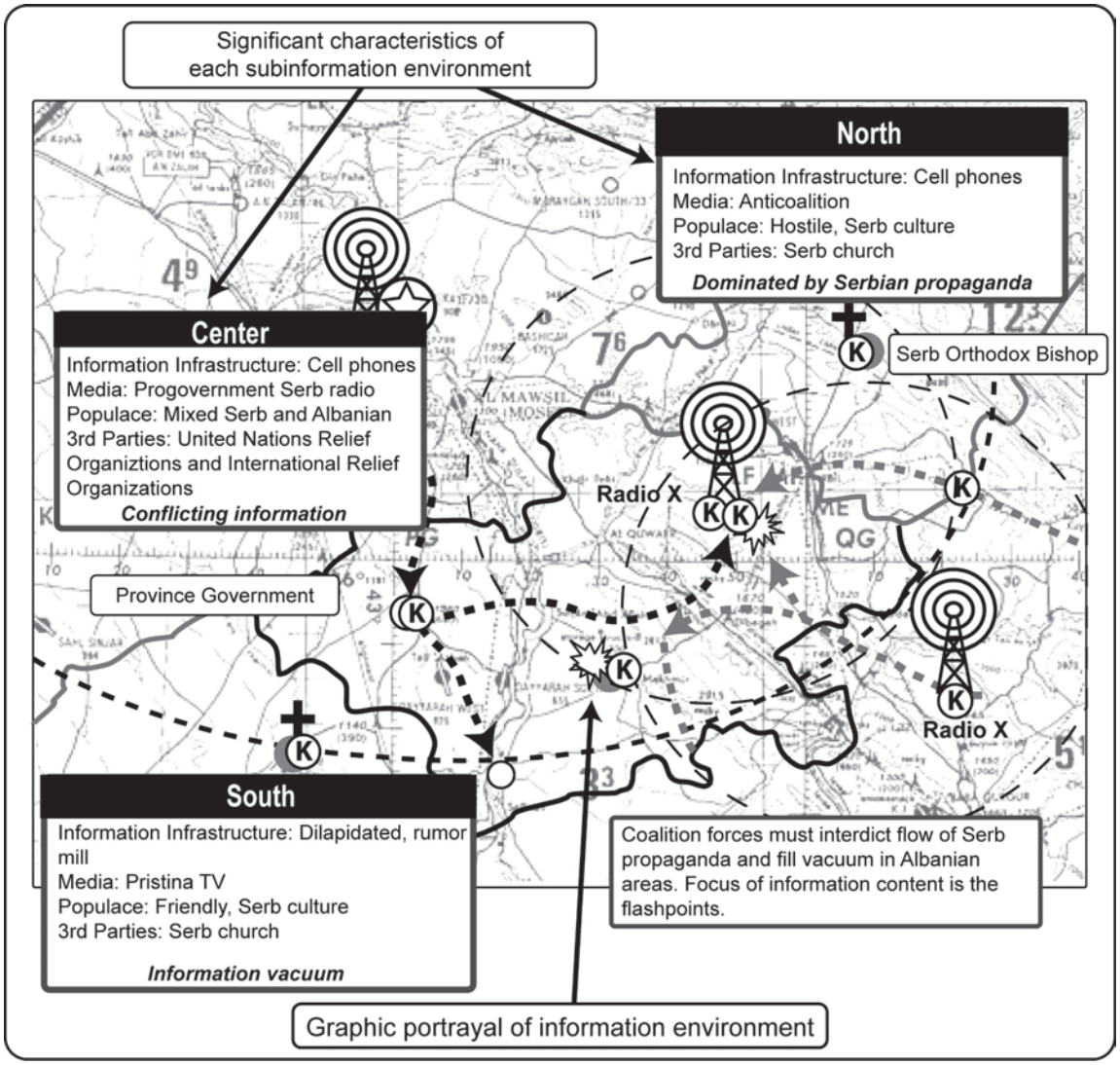


Figure A-22. Example of a combined information operation

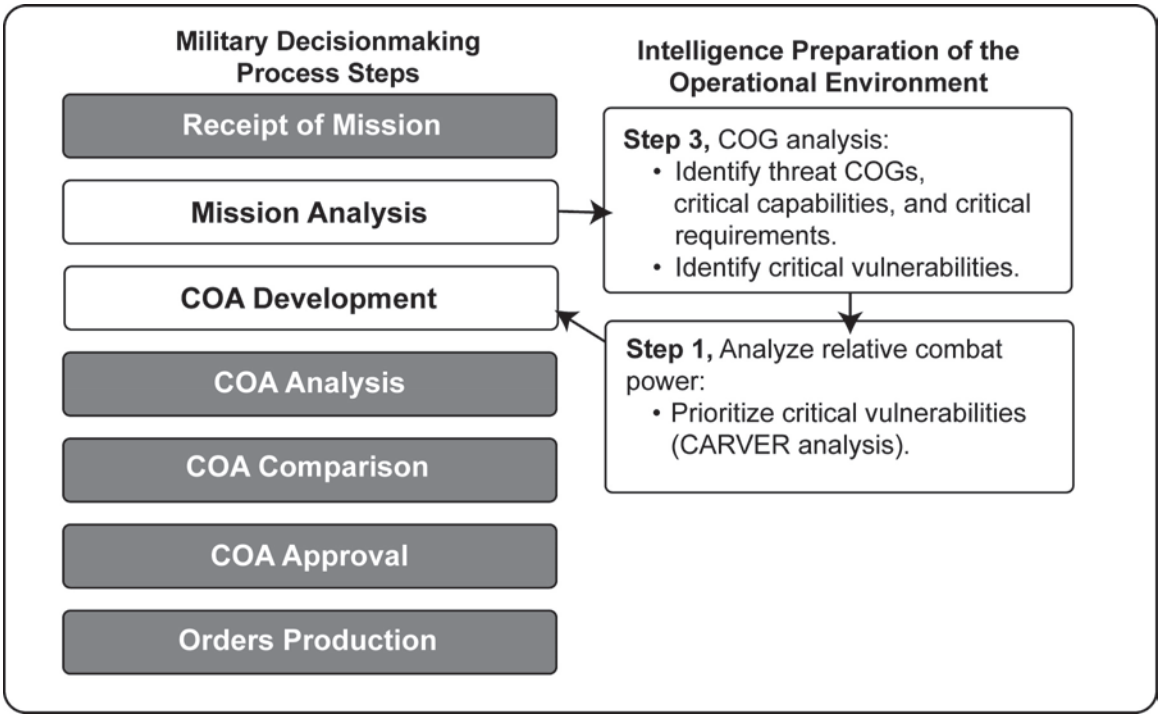


Figure A-23. Relationship between center-of-gravity analysis and the planning process

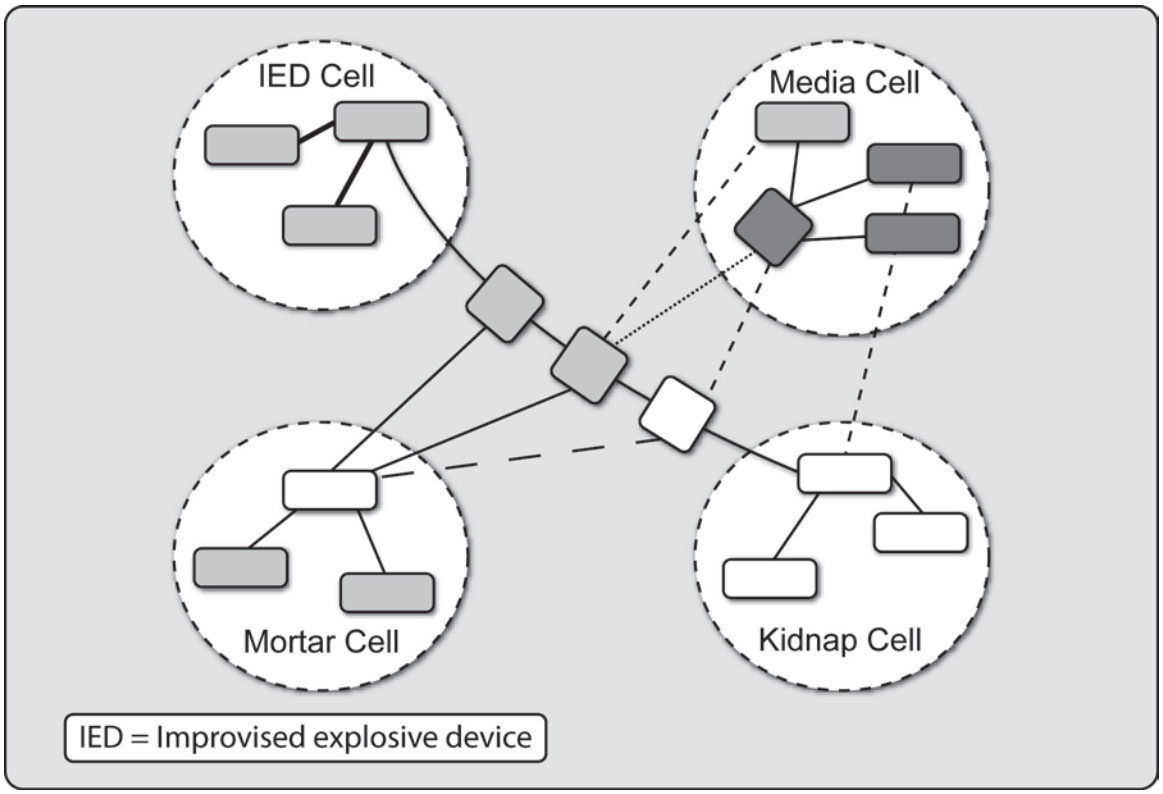


Figure A-24. Decisionmaking template

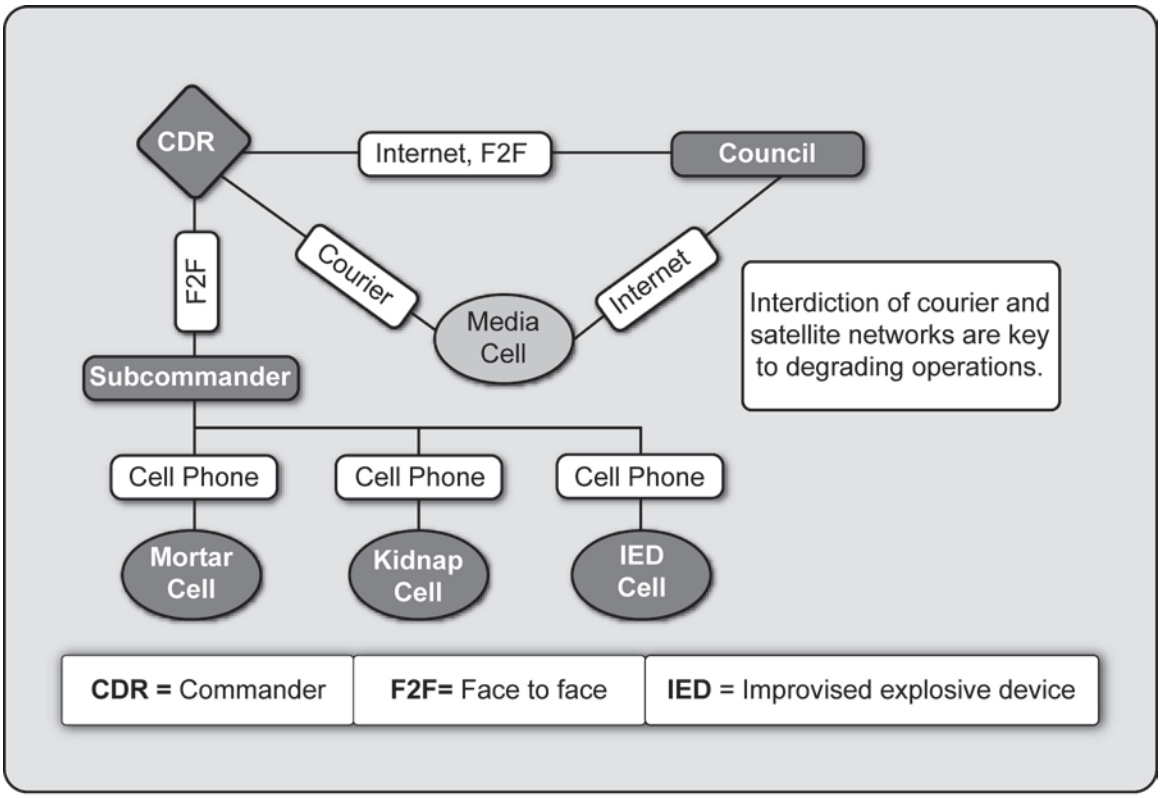


Figure A-25. Information infrastructure template

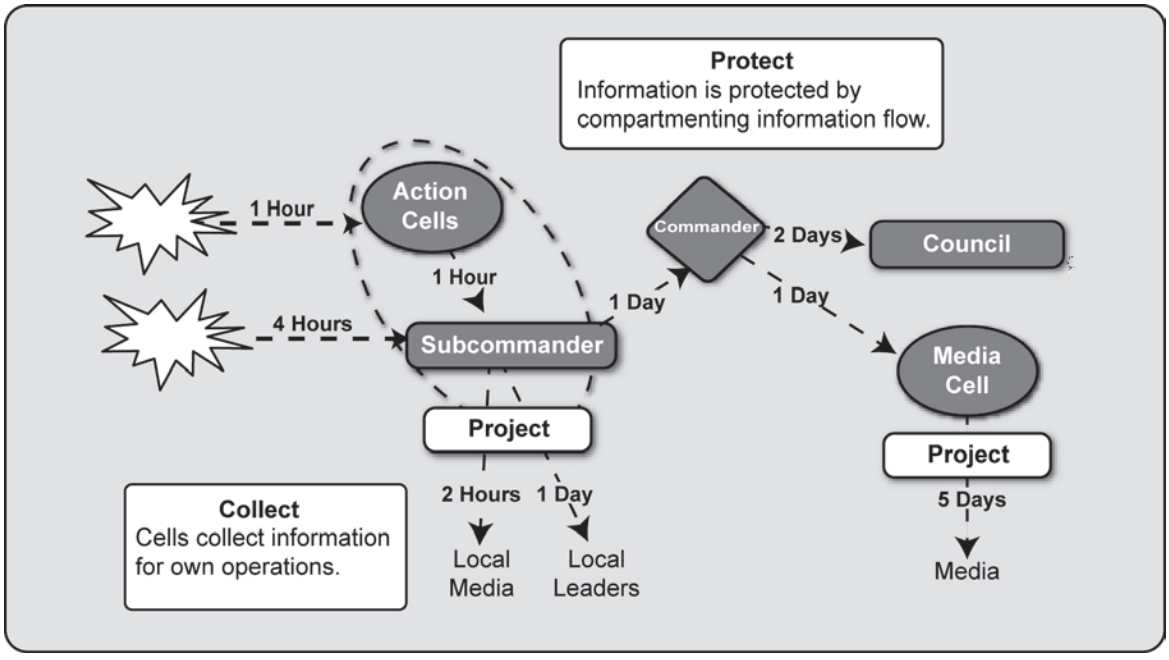


Figure A-26. Information tactics template

DETERMINE THREAT ACTIVITIES IN THE INFORMATION ENVIRONMENT

A-48. The information situation template identifies where, when, and why the adversary will seek information superiority. The result is a concept of operations that describes how the adversary will operate in the information environment. Figure A-27 provides a sample information situation template.

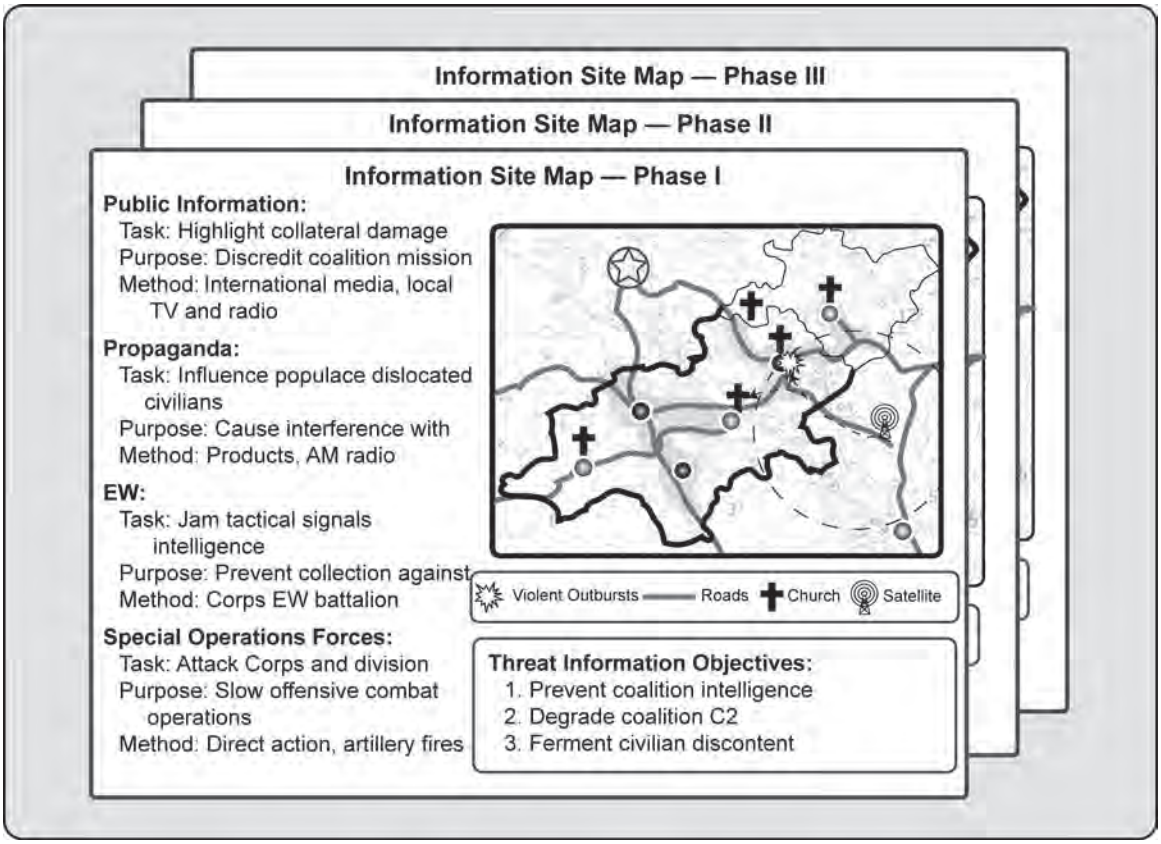


Figure A-27. Information situation template

STAFF ESTIMATE FOR INFORMATION OPERATIONS

A-49. The staff estimate is an assessment of the situation and an analysis of the COAs the commander is considering. The estimate includes an evaluation of how factors in a staff section's functional area influence each COA, and the conclusions and recommendations for each COA. Staff estimates are normally text documents, but may be formatted as maps, graphics, or charts. The estimates are as comprehensive as possible, yet not overly time-consuming to develop. They are developed as part of the planning process, and updated as the operation progresses.

A-50. The staff estimate for IO is an estimate tailored to the specific needs of the IO staff. It assesses the situation in the information environment and analyzes the best way to achieve information superiority. Leaders focus on the information environment and the use of information by enemy and friendly forces. When possible, graphics are added to illustrate the less-tangible aspects of IO.

A-51. The written estimate is a six-paragraph document. The first two paragraphs are necessary for all plans. The other paragraphs can be truncated when time is short. Figure A-28, page A-23, depicts a format for a written IO estimate.

1. **Mission.** Define information superiority for the mission (Step 1).
2. **Situation and considerations.**
   a. Characteristics of the information environment (Step 2).
   b. Enemy forces (Step 3).
   c. Friendly forces (Step 4).
   d. Assumptions (Step 5).
3. **COAs.** List options for achieving information superiority.
4. **Analysis.** Estimate likelihood of accomplishing IO objectives given available time and capabilities.
5. **Comparison.** Compare COAs using evaluation criteria.
6. **Recommendations and conclusions.**
7. **Recommended COA based on which is most supportable by IO.**

Figure A-28. Example of an information operations estimate format

MISSION

A-52. The IO mission describes the operational advantage that IO achieves in support to the unit's mission.

Characteristics of the Information Environment

A-53. The characteristics paragraph describes the significant characteristics of the information environment in terms of the physical, information, and cognitive dimensions. The following characteristics should be considered:

- Terrain.
- Civilian information infrastructure.
- Media.
- Civilian population.
- Third-party organizations.

A-54. The character of each subinformation environment in the AO is reviewed to determine whether it favors friendly or adversary forces. Leaders identify information nodes in each subinformation environment (that is, places, persons, or infrastructure that shape information content and flow by creating or transmitting information).

Enemy Forces

A-55. The enemy forces paragraph describes how, when, where, and why the enemy force operates in the information environment. It identifies enemy capabilities and vulnerabilities in the information environment in terms of information—collection, protection, projection.

Friendly Forces

A-56. The friendly forces paragraph describes friendly-force capabilities to operate in the information environment. It identifies friendly vulnerabilities to enemy and third-party actions in the information environment.

Assumptions

A-57. The assumptions paragraph lists the assumptions essential for planning, execution, and assessment of the information operation. It is organized by—

- Information environment (information content and flow).
- Adversary capabilities and vulnerabilities in the information environment.
- Friendly capabilities and vulnerabilities in the information environment.

GRAPHIC INFORMATION OPERATIONS ESTIMATE

A-58. A graphic IO estimate (Figure A-29) contains the same basic information as a written estimate. It includes—

- Information superiority for the mission.
- Characteristics of the information environment (subinformation environment nodes).
- Enemy vulnerabilities and capabilities in the information environment.
- Friendly-force capabilities and vulnerabilities in the information environment.

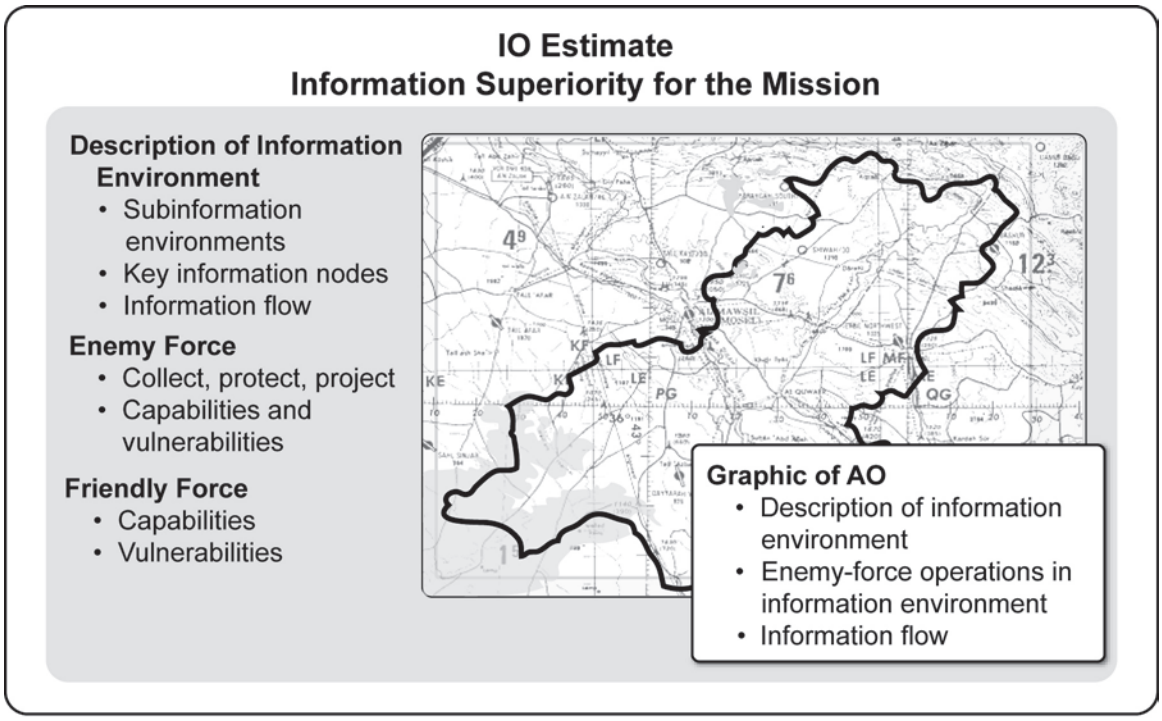


Figure A-29. Graphic information operations estimate

INFORMATION OPERATIONS ANNEX

A-59. Plans and orders are as detailed as time permits. Depending on the command and mission, these documents can be a series of overlays with written comments or they can be voluminous documents of hundreds of pages. Whatever the format, an order must be clear, concise, timely, and useful to the implementing commands and units. The IO annex describes the information operation as a whole and how IO forces will gain information superiority in support of the scheme of maneuver. This approach places less emphasis on individual IO assets and capabilities and more on the aggregate IO effects needed to achieve information superiority. The IO staff must be careful to not let the requirement to develop and explain the IO element contribution to the operation overwhelm the primary purposes of the IO annex, which are to—

- Provide operational details on the information operation.
- Focus element and unit tasks on achieving specific effects in the information environment.
- Provide the information needed to assess the information operation.

A-60. There are two basic formats for an annex:

- *Five-paragraph IO annex.* The five-paragraph annex (Figure 3-12, pages 3-16 and 3-17) is used when time is available and/or when directed by the G-3 or unit SOP.
- *Matrix IO annex.* The matrix annex (Figure 3-13, page 3-17) is used when time is available or when directed by the G-3 or unit SOP.

A-61. Figure A-30 provides an example of an execution matrix.

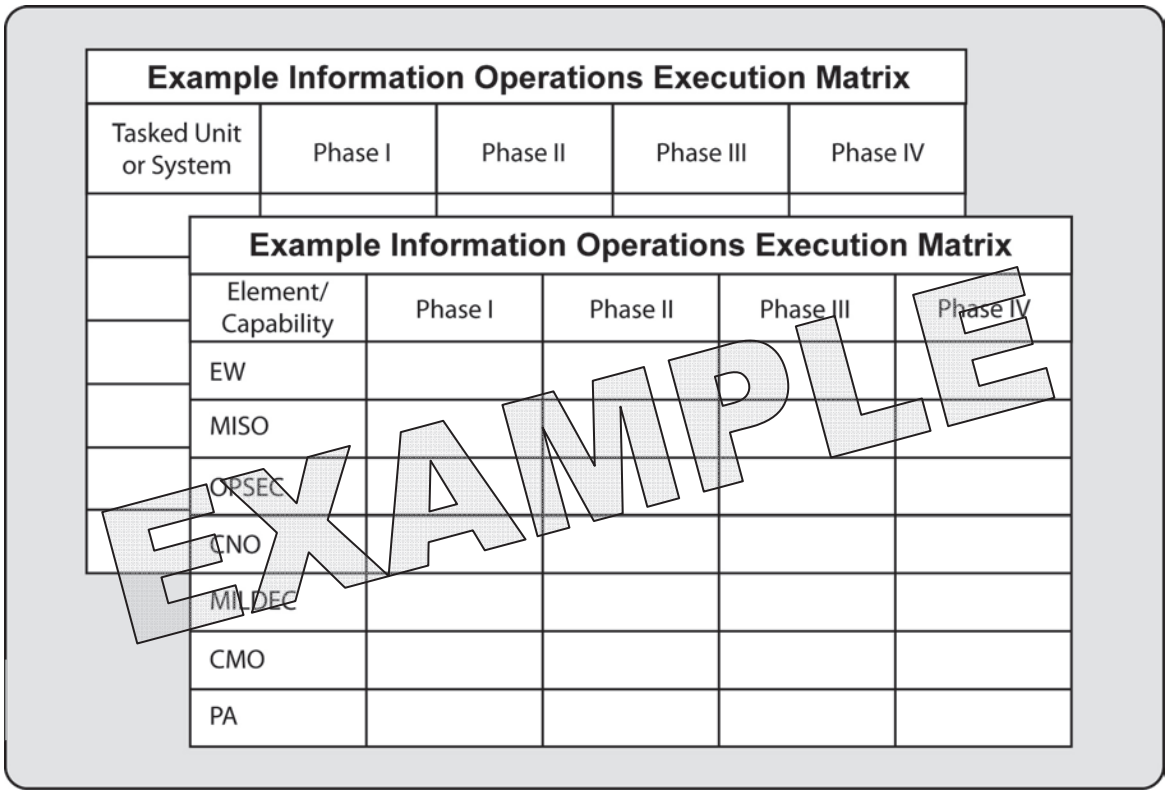


Figure A-30. Example of an execution matrix

INFORMATION OPERATIONS CONCEPT OF SUPPORT

A-62. The IO concept of support is a word picture that explains execution of the information operation from beginning to end and how the capabilities will be employed to gain information superiority. This requires defining information superiority for the operation. A well-written concept is concise and understandable. Although there is no doctrinally prescribed formula for an IO concept of support, planners should consider including the following:

- *Commander's intent for IO.* Explain what the commander wants IO to do to the enemy or the information environment.
- *Information superiority.* Explain specifically what information superiority is within the context of the operational situation and the mission. Include the specific time and location information superiority will be achieved.
- *General scheme for IO.* Use doctrinal concepts and terms to explain how the IO objectives will be achieved, who will perform IO (that is, the tasked units), and the sequencing of key tasks. Relate the key tasks to the achievement of information superiority.
- *Priority of support.* Designate which subordinate unit or element has the priority of IO assets and capabilities.
- *Restrictions on the employment of IO.* List prohibited and directed actions that affect the employment of IO.

This page intentionally left blank.

Appendix B

Tactical Deception Aid

Tactical MILDEC is deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. The purpose of tactical deception is to mislead or confuse the enemy decisionmaker by distorting, concealing, or falsifying indicators of friendly intentions, capabilities, or dispositions. Figure B-1 provides an overview of the deception planning process. Figure B-2, page B-2, provides a deception estimate format.

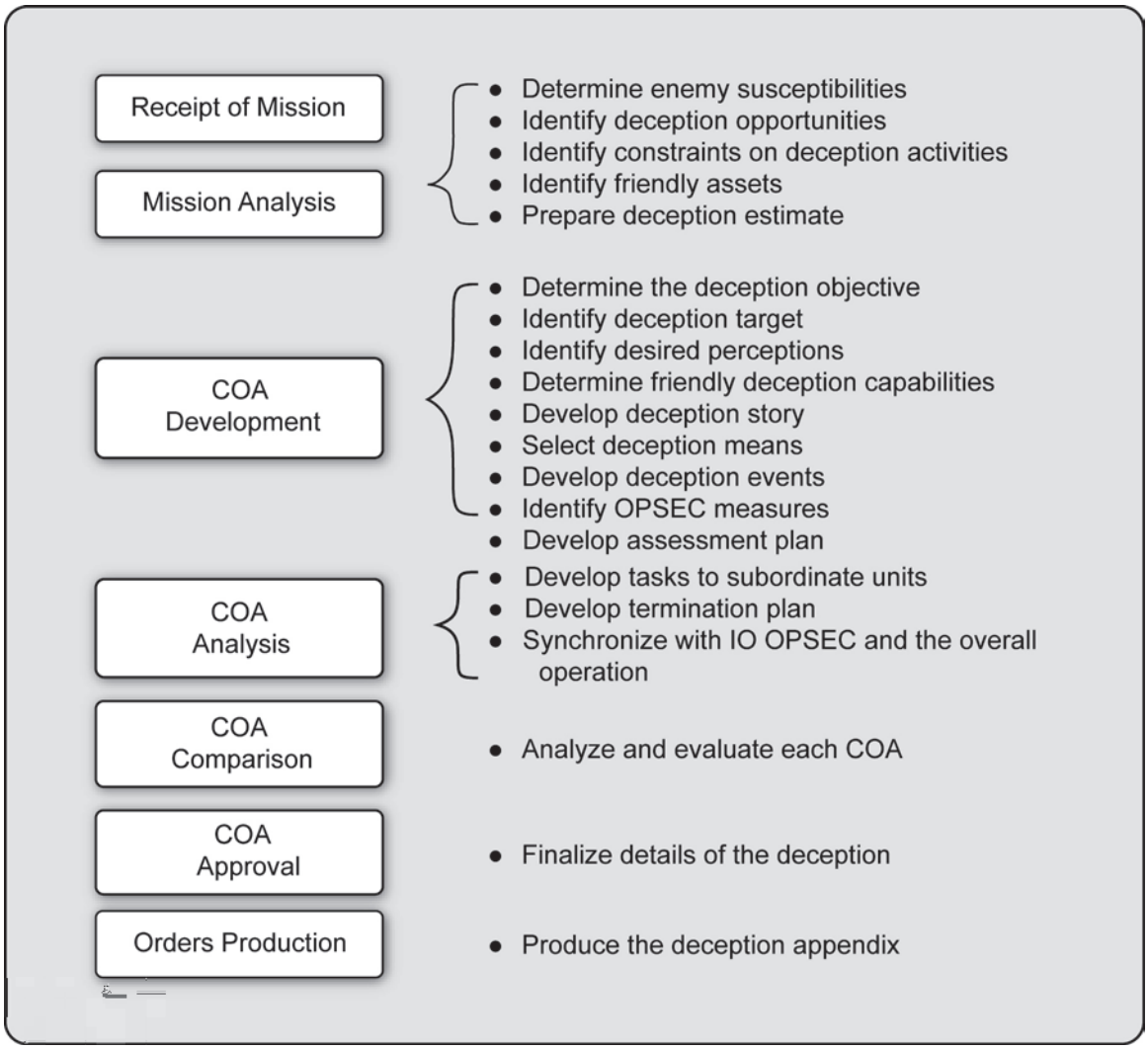


Figure B-1. Deception planning process overview

Page 3038 of 3957

Mission	• Restated mission of the command. • Deception objective. Identify the purpose of the deception.
Situation and COA	• Summarize the situation in terms of characteristics of the AO, enemy situation, friendly situation, assumptions. • Identify friendly deception COA.
Analysis of Deception COAs	• For each deception COA, list the target-vulnerability analysis, desired perceptions, deception story, means, events, risk analysis, and probability-of-success assessment.
Comparison of Deception COAs	• Compare each deception COA in terms of costs and benefits, operational risks, comparative strengths, weaknesses, and probabilities of success.
Recommendation	• Recommend a deception COA.

Figure B-2. Deception estimate format

DESIRED PERCEPTIONS

B-1. Desired perceptions are those thoughts the target audience must process to believe the planned deception story. The formation of the target audience's perceptions is largely based on the means and events used to portray the deception story.

MEANS

B-2. Considerations for selecting deception means include the following:

- What collection systems or mechanisms does the target audience use?
- How much credibility does the target audience place on information from each conduit?
- What kind of information can be conveyed through each of the means?
- When is each means available to transmit information?
- What filters affect information as it moves through the means?
- How long will it take the information to reach the target audience?

EVENTS

B-3. The deception story is portrayed to the target audience through deception events conducted by friendly forces. These are pieces of a puzzle that the target audience assembles over time. The puzzle itself is the deception story, the pieces are the deceptive events seen by the target audience via the means. Events must be observed and accepted as reality by the target audience. The two types of deception events include—

- Those necessary for the formation of desired perceptions (required events).
- The supporting events that complement or reinforce the desired perceptions.

ASSESSMENT PLAN

B-4. The two primary forms of feedback in deception operations are—

- *Indicator feedback.* This feedback is information that indicates whether and how the deception story is reaching the deception target audience. This feedback is useful for the timing and sequencing of executions. (It answers the question: "Is the target audience receiving the deception story as planned?")
- *Perception feedback.* This feedback is information that shows whether the target audience is forming the desired perceptions and is acting (or is likely to act) in accordance with the deception objective. (It answers the question: "Is the target audience acting in accordance with the deception objective?")

B-5. At the tactical level, the pace of operations and limited number of collection assets may reduce the practicality and utility of feedback. For this reason, at the lowest levels of command, tactical deception operations must not depend on feedback for successful execution.

DECEPTION TECHNIQUES

B-6. Tactical deceptions often contain one or more of the following techniques:

- *Feint.* A feint is a limited operation to deceive the enemy of the location or time of the decisive operation. Forces seek direct fire contact with the enemy but avoid decisive engagement. Feints usually occur before or during the main operation. Multiple feints may be needed to portray the deception story. The objective of a feint is to cause the enemy to misemploy forces.
- *Demonstration.* Demonstrations are shows of force to deceive the enemy as to the location or time of the decisive operation. They are similar to feints, except no contact is made with the enemy. The objective is to delude the enemy into an unfavorable COA. Demonstrations are useful when time and distance factors make the lack of contact realistic.
- *Ruse.* A ruse is a deliberate exposure of false information to enemy collection means.
- *Display.* A static display of an activity, force, or equipment is intended to deceive enemy observation. Displays project the appearance of objects that do not exist or appear to be something else. Observables include the use of heat, smoke, electronic emissions, false tracks, and fake command posts.

DECEPTION TACTICS

B-7. The two types of deception tactics are ambiguity-increasing deception and ambiguity-reducing deception. The following paragraphs discussed these tactics.

AMBIGUITY-INCREASING DECEPTION

B-8. Ambiguity-increasing deception increases decisionmaker uncertainty about key information needed to make decisions. It can be used to delay a specific decision or reduce the quality of a decision. Ambiguity-increasing deception—

- Presents conflicting elements of information.
- Overloads enemy intelligence-collection and analytical capabilities.
- Confuses enemy expectations about friendly-force size, activity, location, unit, time, equipment, intent, or mission.

AMBIGUITY-DECREASING DECEPTION

B-9. Ambiguity-decreasing deception provides the decisionmaker with the illusion of reduced uncertainty and risk. It can be used to elicit specific behavior that can be exploited by friendly forces and to provide cover for friendly actions. Ambiguity-decreasing deception—

- Reinforces the enemy's preconceived beliefs.
- Draws enemy attention from one set of activities to another.
- Creates the illusion of strength where weakness exists.
- Creates the illusion of weakness where strength exists.
- Accustoms the enemy to particular patterns of activity that are exploitable later.

MILITARY INFORMATION SUPPORT OPERATIONS IN SUPPORT OF DECEPTION OPERATIONS

B-10. At the tactical level, MISO are a primary deception capability. MIS units may conduct tactical deception by using sonic deception (that is, loudspeakers) for protection and in support of direct action missions. MIS forces may also develop, modify, and disseminate print and audiovisual products to support a deception operation.

DECEPTION IN SUPPORT OF COMBAT OPERATIONS

B-11. In support of combat operations, deception can preserve friendly forces and equipment from destruction, gain time, or minimize an enemy's advantage. A deception is most effective if the friendly force has more COAs available than the enemy has forces to cover in strength. The purpose of deception in combat operations is to create an operational advantage through surprise (that is, specific time, place, method, and scope of an attack). Possible objectives include the following:

- Delay or prevent the enemy's action or counteraction.
- Cause the enemy to misdirect assets.
- Cause the enemy to employ forces in ways that makes them vulnerable to the friendly COA.
- Cause the enemy to reveal strengths, dispositions, and intentions.
- Cause the enemy to waste combat power with inappropriate or delayed actions.

DECEPTION IN SUPPORT OF STABILITY OPERATIONS

B-12. Deception is appropriate during stability and support operations when transparency of operations is a likely requirement. Deception may serve to protect U.S. Soldiers, mask operational intentions, and deter adversary factions. The purpose of deception during such operations is to degrade adversary attempts to disrupt peace. Possible objectives include the following:

- Cause hostile forces to not attack friendly forces (protection).
- Deter factional violence.

B-13. Political objectives may override military considerations, to include the use of deception. Participation of multinational forces also may restrict the utility and use of deception.

DECEPTION IN SUPPORT OF OPERATIONS SECURITY

B-14. Deception in support of OPSEC increases the likely detection of indicators that the enemy can observe to derive an incorrect conclusion. OPSEC hides real indicators, whereas deception shows fake indicators. Observables are presented to distract enemy intelligence collection away from (or provide cover for) real friendly operations and activities.

DECEPTION IN SUPPORT OF COUNTERINSURGENCY

B-15. During counterinsurgency missions, in-depth human-factors analysis of deception target audiences may not be possible. In lieu of a human-factors analysis of the target audiences, planners can use profiles of cell leaders or security organizers. Counterdeception is important, as insurgent and guerrilla warfare theory emphasizes the use of deception to accomplish goals.

Appendix C

Tactical Operations Security Aid

OPSEC is a universal IO capability. It should be included in all plans, operations, and activities. The OPSEC process is a framework to systematically identify, analyze, and protect information. The goal of OPSEC, in conjunction with unit security programs, is to achieve essential secrecy. The OPSEC process should be integrated into the military decisionmaking process. It uses the steps indicated in Figure C-1, but does not have to follow them in a particular sequence.

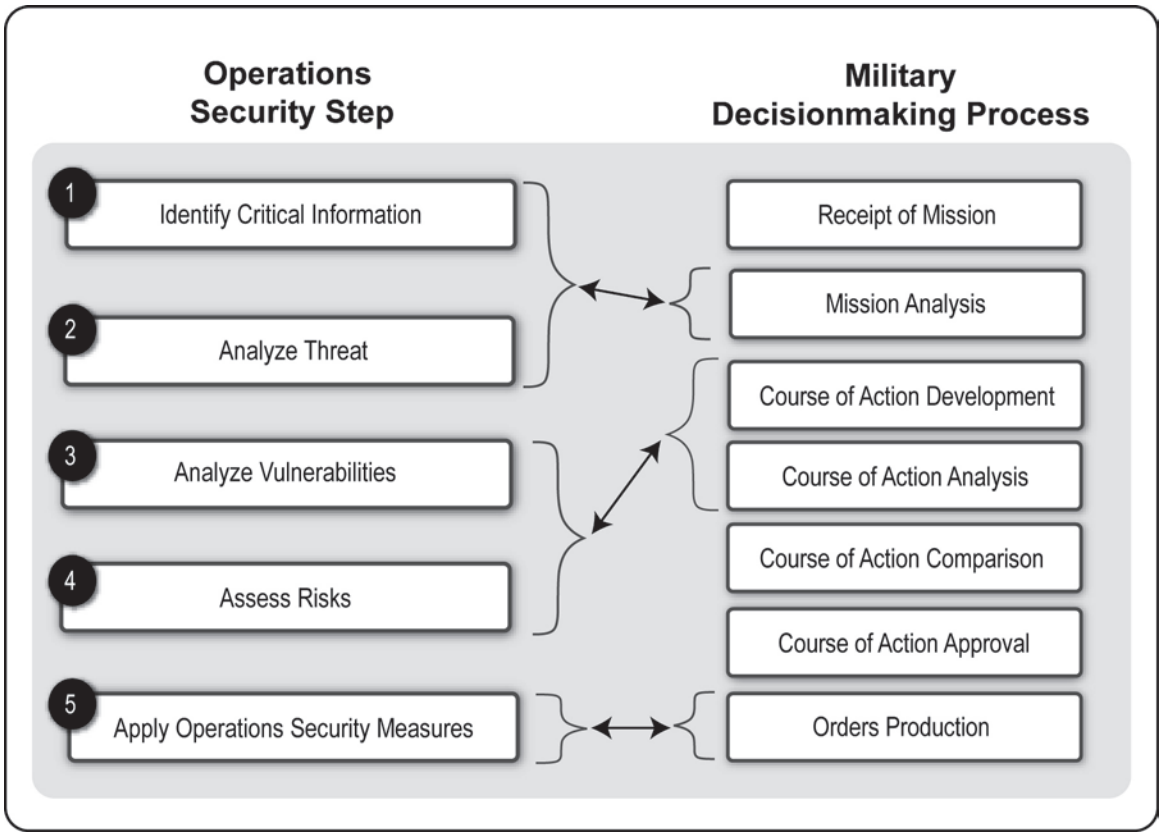


Figure C-1. Operations security and the planning process

IDENTIFY CRITICAL INFORMATION

C-1. Planners determine what information must be protected (that is, a list of EEFI). Sources of EEFI include the—

- Higher HQ plans and operation orders.
- Commander's guidance.
- Current unit EEFI.

Page 3042 of 3957

C-2. EEFI focus on friendly-force intentions (time and place of units and operations), capabilities, and vulnerabilities (strength, technologies, and tactics). EEFI are different for every operation. Leaders must avoid the "cookie-cutter" approach and should continually develop new EEFI or refine old EEFI. The OPSEC working group can be used to take advantage of subject-matter experts (for example, aviation and communications). Leaders identify the length of time each EEFI must be protected (not all information needs protection for the duration of the operation). EEFI are prioritized and kept to a manageable number (perhaps five).

ANALYZE THE THREAT

C-3. The threat to EEFI is the sum of enemy information needs and enemy collection capabilities. A CI template (Figure C-2) is a useful tool to depict enemy collection capabilities. It shows when and where the EEFI are vulnerable to enemy collection.

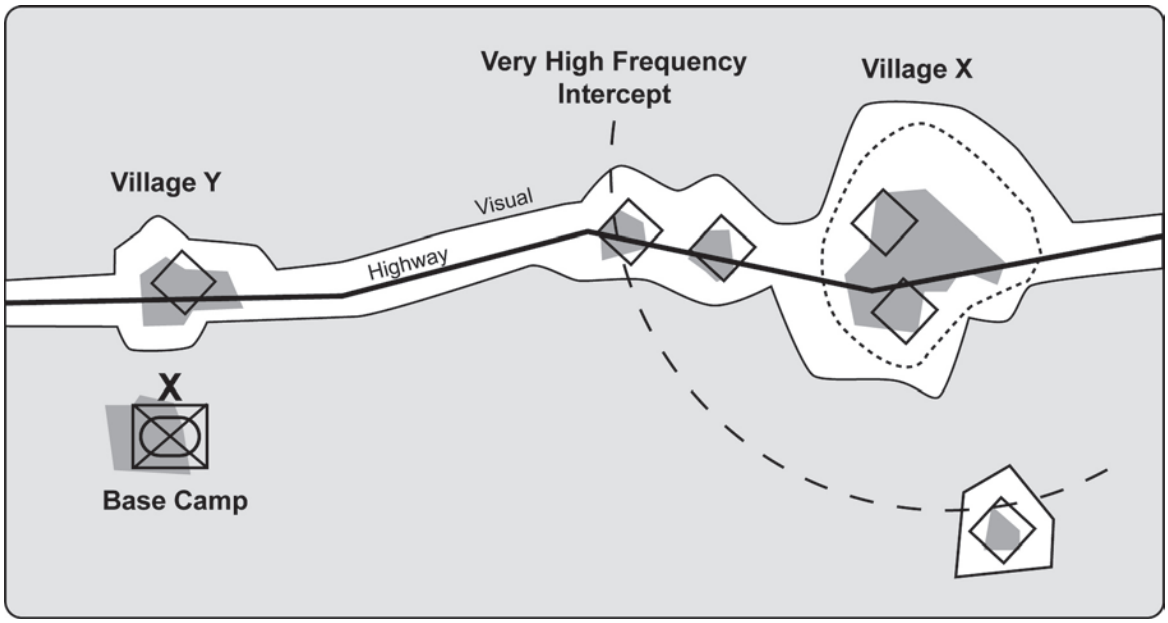


Figure C-2. Example of a counterintelligence template

ANALYZE VULNERABILITIES

C-4. Leaders identify each EEFI's vulnerability to enemy intelligence collection (that is, OPSEC vulnerability). The OPSEC vulnerability is a result of the OPSEC indicator and enemy collection capabilities. OPSEC vulnerabilities are detectable indicators of EEFI. OPSEC indicators become OPSEC vulnerabilities if they can be observed, analyzed, and acted upon by the enemy. To determine OPSEC vulnerabilities, leaders—

- *Identify OPSEC indicators.* Leaders determine what detectable actions and OSINT can be interpreted or pieced together by the enemy to derive EEFI.
- *Compare OPSEC indicators to enemy collection capabilities.* Leaders determine which indicators can be observed, analyzed, and acted upon by the enemy.

ASSESS RISK

C-5. Leaders develop measures to protect OPSEC vulnerabilities by conducting risk assessments for each vulnerability and then selecting one or more OPSEC measure for each vulnerability. There are three types of OPSEC measures:

- *Action controls.* The controls change unit procedures, activities, and actions (for example, randomized routine activities, avoiding repetitive TTP).

- *Countermeasures.* These measures disrupt enemy information-gathering and targeting (for example jamming [EW], physical attack, and camouflage and concealment).
- *Counteranalysis.* This action deceives the enemy by providing false indicators (for example, decoys and deception in support of OPSEC).

C-6. Once leaders decide which OPSEC measures to implement, they must check that OPSEC measures do not create new vulnerabilities. Leaders must balance OPSEC measures with operational effectiveness.

APPLY OPERATION SECURITY MEASURES

C-7. Leaders apply OPSEC tasks to units and staff as follows:

- Rewrite approved OPSEC measures as tasks.
- Assign responsibility and coordinate OPSEC tasks with units and staff.
- Coordinate OPSEC measures with MILDEC, PA, and COMCAM to prevent compromise of EEFI.
- Integrate OPSEC tasks with IO.
- Include OPSEC tasks in the operation order/operation plan.
- Adjust OPSEC measures based on adversary reaction to the implemented OPSEC measures.
- Monitor execution.
- Evaluate effectiveness.
- Adjust measures and tasks.
- Coordinate monitoring of OPSEC measures through the G-2 and CI.

This page intentionally left blank.

Appendix D

Media Assessment Aid

Media analysis is a quick and useful technique for evaluating the impact of media coverage on military operations.

IDENTIFY MEDIA SOURCES

D-1. Planners identify media outlets that are critical to mission accomplishment by analyzing the flow of media reporting in the AO and area of interest, selecting those media outlets that have local, regional, or international influence. Media outlets that are overtly biased toward the adversary should not be used. A good sampling of media outlets includes the following:

- *Local media in the AO.* These outlets influence local public opinion.
- *Regional media in countries adjacent to the AO.* These outlets can influence public and political opinion in the AO and area of interest. For example, in Afghanistan it is important to monitor the Pakistani press.
- *International media are the larger media outlets associated with countries outside the AO.* Typically these outlets impact U.S. domestic, coalition partner, and worldwide public and political opinion (for example, in Canada, the Canadian Broadcasting Corporation; in the United Kingdom, the British Broadcasting Corporation; in Germany, *Der Spiegel;* and in the United States, the Cable News Network, *The Washington Post*, *Los Angeles Times*, and *The New York Times*).

Note. Home (domestic) media is a primary consideration for the PA staff, but it is not a consideration for military IO.

D-2. The media analysis presented in this aid is a tool that staffs can use to understand and assess the impact of media reporting on friendly and enemy activities in the AO. This type of media analysis helps the staff—

- Maintain situational awareness on media reporting.
- Evaluate the impact of media reporting on the mission.
- Identify adversary information.
- Provide data for assessment.

D-3. Other staff elements may also conduct media analysis to support their functional area:

- The PAO conducts a media content analysis to assess news coverage.
- The intelligence staff may collect and analyze media reporting as part of OSINT.
- MIS forces prepare extensive media assessments and analyses of commercial and government media within their AO, as they seek to leverage more indigenous and credible local media outlets to use for dissemination.

D-4. The IO staff must be prepared to analyze the media, to monitor changes in the information environment, and to counter adversary misinformation and propaganda.

Page 3046 of 3957

DATA COLLECTION

D-5. Planners systematically monitor media coverage of the command, its mission, and the AO from the sources identified above. Useful sources of media reports and stories include the following:

- *PAO media operations center*. This center provides translations of foreign press coverage in addition to monitoring major English-language media outlets.
- *OSINT media-monitoring sources (contracted by the Department of Defense).*
- *United States Government open-source center.*
- *Internet.*

D-6. Data collection must be continuous and consistent—usually on a daily basis. Several factors can affect collection of data reports. Items that need to be considered include the following:

- English-language media sources are readily available and may skew the collection effort away from local media.
- Translation of local and regional media may cause a lag time of a day or more.
- A database should be created, populated, and maintained to establish a baseline upon which comparisons can be made (for example, media reporting for one month versus another month).

D-7. Other than the PAO's media content analysis, there is no established doctrinal method for analyzing the media. The media analysis process identified in Figure D-1 has been field-tested. It can be modified to fit command and staff needs.

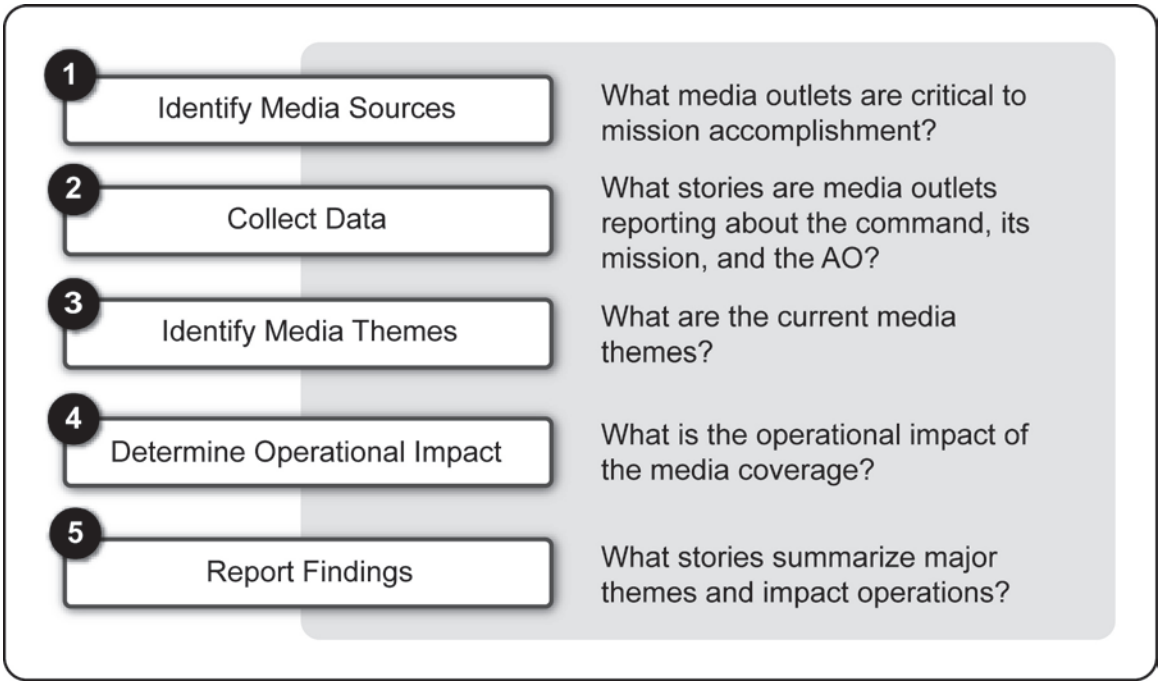


Figure D-1. Media analysis process

IDENTIFY MEDIA THEMES

D-8. Planners analyze and plot the media coverage collected above to identify current media themes (Figure D-2). Planners should do this by—

- Picking out primary themes in media reports and stories.
- Categorizing themes into groups that either support (positive), run counter to the command's objectives (negative), or are neutral to either enemy or friendly forces.
- Identifying ad hoc themes of interest to the command.
- Pairing media sources and themes to the command's objectives or lines of operation.

Objective	*Theme (+/–)*	*Source*
Maintain international support for mission	(+) United Kingdom supports troop expansion	British Broadcasting Corporation News and Cable News Network
	(–) U.S. missile strikes kill civilians	British Broadcasting Corporation News and Associated Press
Objective	*Theme (+/-)*	*Objective*
Reduce popular support for insurgents	(+) Tribal elders turn in Taliban to Afghan police	Local Armed Forces radio and TV
	(–) Taliban propaganda about U.S. missile strikes	*Dawn* (Pakistani newspaper)

Figure D-2. Media theme assessment diagram

DETERMINE OPERATIONAL IMPACT

D-9. Planners analyze the themes identified above to determine the impact on friendly and enemy operations. Media sources and themes are categorized by echelon (that is, local, regional, and international). For each theme, planners answer the following questions:

- Who is the originating source of the theme:
  - Enemy or hostile forces?
  - Friendly forces?
  - Third-party organization?
  - Embedded media?
- Who is the target audience?
- What is the circulation of theme (most critical for local media)?
- What are the second- and third-order effects?
- Is the event affected by extended media coverage?

D-10. Themes are prioritized within each category based on degree of impact. Planners determine which negative themes pose potential problems for ongoing and future operations and determine which positive themes provide an opportunity for exploitation.

REPORT FINDINGS

D-11. There is no standard method on how to report media findings. The key is to portray media coverage in an easily understood format that can be quickly scanned to see what themes are important. Planners should use color coding to clearly display the impact of each theme: green is positive, red is negative, and blue is neutral. Symbols (for example, +/–, letters, or numbers) should be added so the analysis can be understood if printed in black and white. Planners must resist the temptation to fill the

boxes with headlines rather than themes. Media themes that reflect enemy propaganda should be added, along with an assessment of operational impacts. Planners display a trend analysis to put the current media reporting into a broader context. Figure D-3 provides one technique of reporting findings.

CONSEQUENCE MANAGEMENT

D-12. Military operations can trigger either positive or negative coverage by the media. This coverage may be a situation that must be mitigated to prevent or reduce the impact on the unit mission, or exploited as an opportunity to further the command's objectives. Such a situation is called “media bounce.”

D-13. Media bounce refers to the staying power of a story over time. The bounce is usually short, particularly if another newsworthy event occurs. Monitoring media bounce avoids reacting to an event that loses media’s attention and may renew negative reporting, thereby aggravating the situation. A consequence-management tracker (Figures D-4 and D-5, page D-5) is a simple decisionmaking aid that tracks subsequent media reporting of an event (bounce) to determine whether subsequent command action is required.

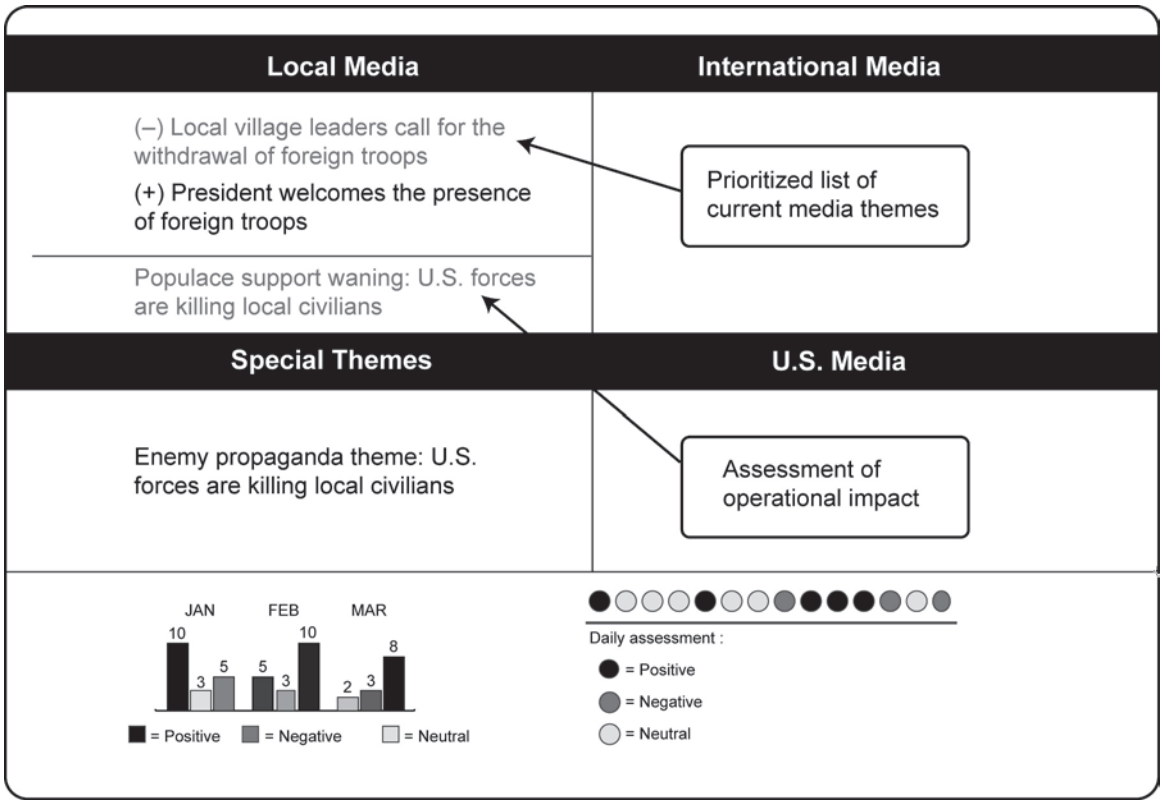


Figure D-3. Sample media report

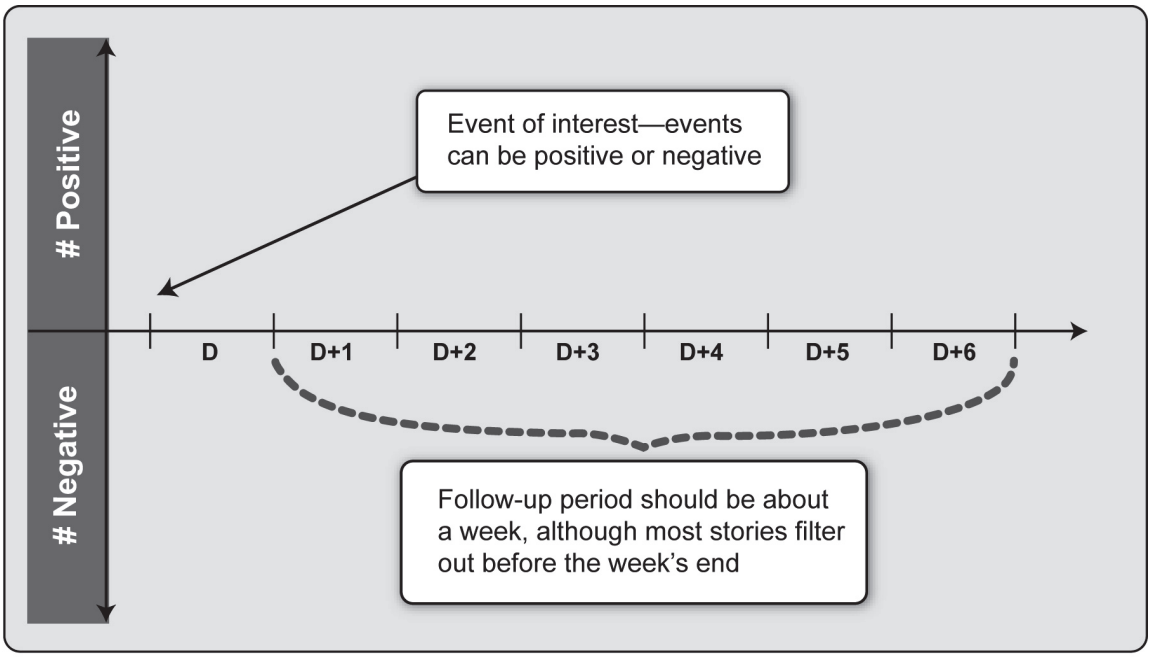


Figure D-4. Consequence-management tracker format

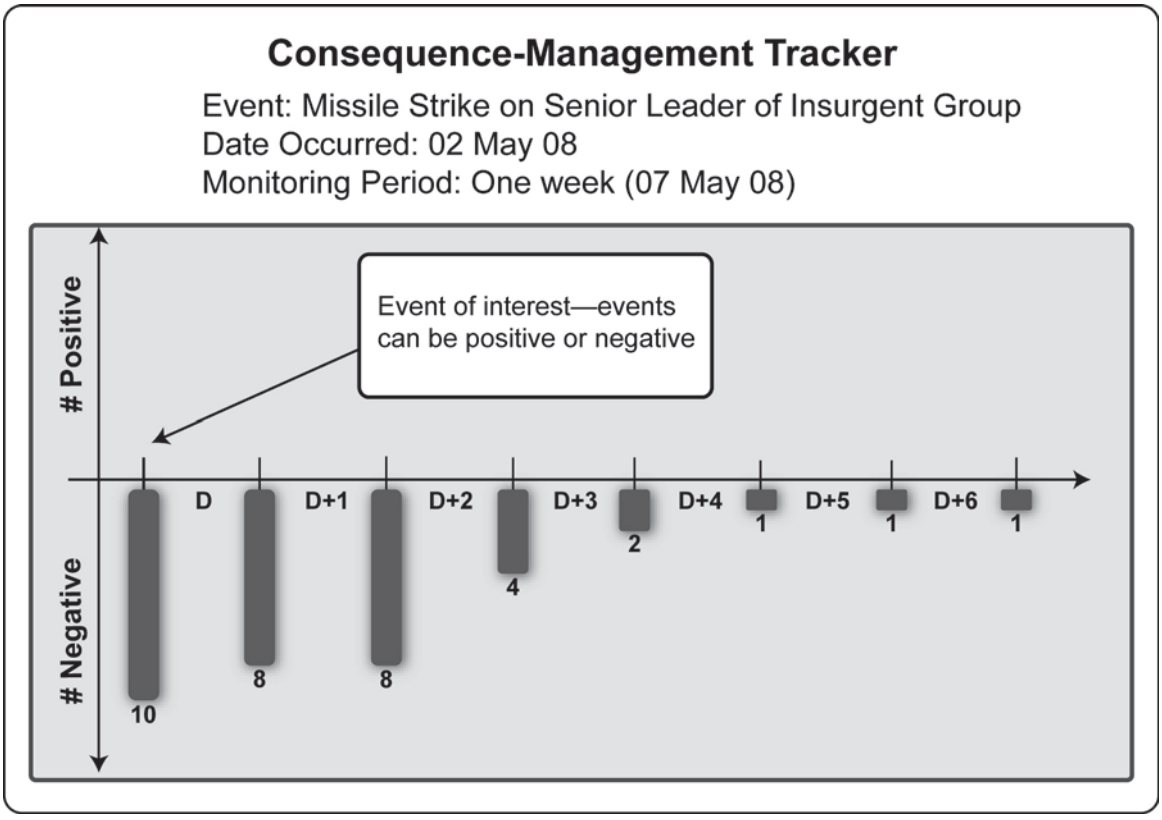


Figure D-5. Example of a consequence-management tracker

This page intentionally left blank.

Appendix E

Conducting Face-to-Face Meetings

This appendix provides a guide for tactical face-to-face engagements by troops at the detachment, company, battalion, and group level when meeting target audiences.

Leaders must always remember they are representing their unit, the command, and, for all intents and purposes, the United States and its allies. Regardless of rank or position, actions taken when in contact with the populace can shape the battlefield to defeat an enemy seeking local sanctuary to conduct attacks on the forces and allies of the United States.

PREPARING FOR A FACE-TO-FACE MEETING

E-1. Leaders can take a number of steps to prepare for face-to-face meetings. These steps include:

- *Research.* Leaders should learn everything they can about the target audience, to include proper name and title, approximate age, family members, ethnicity, language spoken, and the target-audience's relationship to other leaders, friendly forces, third-party organizations, and the adversary. Reliance on intelligence and MISO capabilities provides a strong foundation of information to leaders prior to a face-to-face meeting.
- *Check previous contacts.* Leaders should determine who has had contact with the target audience; when the meeting took place; what was discussed; what promises were made; whether the target audience was deemed truthful, manipulative, or trustworthy; and the groups or individuals to which the target audience is tied. With attached or assigned MIS forces managing the key-leader engagement program, this information should be catalogued and ready for access to guide future contacts.
- *Keep records.* Leaders should take notes during the conversation (either personally or via an aide) referring back to them at the end to capture the essence of the conversation. Notes should be shared with other interested persons, particularly MIS planners.
- *Coordinate.* Face-to-face meetings are coordinated to prevent other friendly forces from sending mixed messages to the target audience.
- *Set a time limit.* Leaders determine how long the meeting should be, staying as close to the timeline as possible while exploiting any available opportunities.
- *Consider perceptions.* Many factors affect target-audience perceptions (for example, uniforms, long versus short guns, large versus small convoys, aircraft in the area, type and size of escort, civilians present, and the number of people attending the meeting).
- *Plan for problems.* Leaders establish code words to maintain control of information flow and security. Typical situations where code words may be used include the desire to end the conversation, a noted potential for violence or increased threat, and other possible emergencies.
- *Rehearse.* Leaders practice the discussion with another person through the translator. Comments should be solicited from anyone having experience with the target audience.
- *Plan the rest of the operation.* Leaders should plan face-to-face meetings with the same intensity and focus as they would plan combat operations. Special items of note include—
  - Translator integration.
  - Movement (ingress and egress).
  - Security (both sides know of planned meetings, so units must anticipate compromise).
  - Contingency and emergency situations and covert danger signals.

Page 3052 of 3957

CONDUCTING A FACE-TO-FACE MEETING

E-2. When conducting face-to-face meetings, leaders should—

- *Bring past notes or previous reports for reference.* This demonstrates interest as well as directs the conversation into favorable areas.
- *Perform introductions.* Leaders introduce everyone in their party and record the names and positions of everyone outside their party who is attending. Collecting information is a key goal of each meeting.
- *Take photographs.* After asking (and receiving) permission, leaders should take photographs of the target audience.
- *Be sincere.* Leaders may wish to apologize in advance for any cultural mistakes made, reassuring the target audience that no offense is intended. Leaders may ask the target audience to point out errors as a learning tool. As the face-to-face meeting ends, the leader may wish to ask what cultural mistakes were made and thank the target audience for helping the leader to learn the local culture.
- *Avoid restricted topics.* Leaders should not discuss sensitive issues such as religion or other societal practices.
- *Compare notes.* Immediately after the meeting, the attendees should discuss what was observed to ensure an accurate understanding of what occurred.
- *Avoid false assumptions.* Leaders should never assume the target audience does not understand English.

CHANCE ENCOUNTERS AND CONTACTS

E-3. A chance encounter or contact with the target audience occurs most often during patrols at the squad, platoon, and company levels. The leader of the unit should conduct the face-to-face meeting based upon a preplanned battle drill. Items to consider during chance encounters include the following:

- *Maintain security.* The leader of the patrol should preserve security of the communicator and the target audience.
- *Maintain schedule.* The leader of the patrol should limit the length of the face-to-face meeting by establishing a code word for when it is time to end the meeting.
- *Identify the local leader.* The leader of the patrol should ask who is in charge and talk to him only. The patrol should not distribute anything to the populace without the local leader's permission.
- *Be fair and firm.* The leader of the patrol should stay in charge and be respectful, not rude.
- *Be selective.* The leader of the patrol should select a maximum of one or two people to talk with.
- *Take notes.* The patrol should get names of all people contacted, approximate ages, hometown, business or activity, subjects covered, demeanor towards friendly forces, and any particular concerns of the target audience. This information should be shared with the intelligence and MISO capabilities at the first opportunity after the contact.
- *Be prudent.* The patrol should not make promises that cannot be kept.
- *Establish rapport.* The leader of the patrol should offer the target audience refreshments (such as a bottle of water) and move to a comfortable location. Sit, if possible.
- *Focus.* The patrol should stay on message by knowing what messages the command is focusing on in specific AOs and during specific time periods.
- *Reinforce the message.* The patrol should use any applicable/available printed products (handbills, pamphlets, or posters) to reinforce the verbal message and request a formal follow-up engagement, if deemed necessary, based on the issues discussed.
- *Report.* The patrol should report all contacts with local leaders up the chain of command to ensure that an accurate picture of the situation is developed.

Page 3053 of 3957

Appendix F

How to Use Translators

The following information is specifically applicable to category I (local hire, uncleared) translators. However, some aspects of the information are applicable to category II (cleared for SECRET) and category III (cleared for TOP SECRET) translators.

Leaders must remember that the translator is their voice and their representative to the community. The translator will be seen as a representative of the command, of the Army, and of the United States. As such, leaders must monitor and keep all aspects of their behavior professional and ethical regardless of their nationality or ethnicity.

GENERAL GUIDELINES

F-1. Leaders should insist translators—

- Speak in first person.
- Remain nearby when the leader is speaking.
- Carry a notepad and take notes, as needed.
- Project clearly and mirror the vocal stress and overall tone of the leader.

F-2. Good leaders know their translators. The lives of Soldiers may be in the translator's hands, so it is critical to know the translator's strengths and weaknesses. Translators should be treated as part of the unit. The better the translator is integrated into the unit, the better the translator's performance.

F-3. Translators should be used for translation duties only. Using them for other activities may violate their contract. An example of misemployment is using a translator to run errands in town. However, sending the translator to town to coordinate a meeting for U.S. officials is allowed.

F-4. The translator is the leader's voice and, as such, may be subject to physical harm because of the messages delivered. Translators should be offered physical protection. If the translator is allowed to carry a weapon, the unit must ensure that he can handle it in a safe manner. Range familiarization/qualification (as well as knowledge of movement techniques and chemical, biological, radiological, and nuclear equipment) is highly recommended.

F-5. Translators should be allowed rest periods to collect their thoughts and catch their breath. Meal meetings are especially challenging for a translator. Leaders should ensure the translator is allowed to eat during or after the meeting.

F-6. Translators should be dressed like the troops they are supporting so they can be readily identified as a friendly in a combat situation to preclude fratricide. Uniform accessories (such as wet weather gear, body armor, and glint tape) that are common on Soldiers' uniforms should be made available to the translator.

REHEARSING WITH A TRANSLATOR

F-7. Leaders must check the translator to verify their abilities. To ensure accuracy and security, periodically record your translator, both with and without his knowledge, for quality checks by higher HQ. If operational details are briefed to the translator during the mission rehearsal, units may consider having the translator remain on the base camp until execution. Also ensure the translator does not have a cellular telephone or other communication device.

Page 3054 of 3957

F-8. Leaders must rehearse conversations, particularly when dealing with complex, new, or sensitive issues. A rehearsal will help define words the translator may not know and ensure the translator understands the overall message to be conveyed. Leaders provide feedback to the translator and make corrections as needed. Leaders must keep in mind that if the translator performs poorly, it affects the target audience's perception of the unit.

WORKING WITH A TRANSLATOR

F-9. Leaders must always maintain eye contact with the person they are speaking with and not the translator. The target audience should be observed for gestures, posture, and body language.

F-10. Leaders using translators should speak in short clips and not recite long paragraphs. The goal is to make the target audience feel like they are conversing and not being lectured. One to two sentences at a time is a good rule. Acronyms, slang, and idioms should be avoided.

F-11. For simple ideas or routine information, some leaders feel confident that the translator is capable of delivering the intended message. This technique works best if the leader introduces the topic and then expresses confidence in the translator's ability to speak on the leader's behalf. Conversations should be ended with closing comments and an opportunity for questions.

BATTLE DRILLS AND STANDING OPERATING PROCEDURES

F-12. There are some situations when a leader may want to establish battle drills or SOPs that address information the translator will convey to the local populace. Some possible situations and the type of information that the translators should be prepared to provide are—

- *Vehicle checkpoints.* Common concerns include questions about where the vehicle occupants are going or if they are armed, and instructions on where vehicle occupants should stand or what they should do during the search.
- *Cordon and search.* Common concerns include an explanation of what military forces are doing when they question residents about any weapons or suspicious activities.
- *Detention of a person.* Common concerns include an explanation telling why the person was detained, how the detention process works, how the detainee's family can reach the detainee, and how friendly forces humanely treat detainees.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army Doctrine Publication
AO	area of operations
C2	command and control
CA	Civil Affairs
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CCIR	commander's critical information requirement
CI	counterintelligence
CIO	combined information overlay
CJSOTF-AP	combined joint special operations task force—Arabian Peninsula
CMO	civil-military operations
CMOC	civil-military operations center
CNA	computer network attack
CND	computer network defense
CNO	computer network operations
COA	course of action
COG	center of gravity
COMCAM	combat camera
DA	Department of the Army
DSPD	defense support to public diplomacy
EA	electronic attack
EEFI	essential elements of friendly information
EIOT	essential information operations task
EMS	electromagnetic spectrum
EW	electronic warfare
FFIR	friendly-force information requirement
FID	foreign internal defense
FM	field manual
G-2	assistant chief of staff, intelligence staff section
G-3	assistant chief of staff, operations staff section
G-5	assistant chief of staff, plans staff section
G-6	assistant chief of staff, command, control, communications, and computer systems staff section
G-7	assistant chief of staff, information operations
HN	host nation
HQ	headquarters
HUMINT	human intelligence

Page 3056 of 3957

IA	information assurance
IO	information operations
IOWG	information operations working group
IPOE	intelligence preparation of the operational environment
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
J-5	plans directorate of a joint staff
J-6	command, control, communications, and computer systems directorate of a joint staff
JCCC	joint combat camera center
JP	joint publication
JSOTF	joint special operations task force
MASINT	measurement and signature intelligence
MILDEC	military deception
MIS	Military Information Support
MISO	Military Information Support operations
MNF	multinational force-Iraq
MOE	measure of effectiveness
MOP	measure of performance
OPSEC	operations security
OSINT	open-source intelligence
PA	public affairs
PAO	public affairs officer
PIR	priority intelligence requirement
S-2	intelligence staff officer
S-3	operations staff officer
S-6	command, control, communications, and computer systems staff officer
S-7	information operations staff officer
SF	Special Forces
SFG(A)	Special Forces group (Airborne)
SFODA	Special Forces operational detachment A
SFODB	Special Forces operational detachment B
SIGINT	signals intelligence
SOP	standing operating procedures
SOTF	special operations task force
TC	training circular
TTP	tactics, techniques, and procedures
TV	television
U.S.	United States
USAJFKSWCS	United States Army John F. Kennedy Special Warfare Center and School
USD(P)	Under Secretary of Defense for Policy

USG United States Government

SECTION II – TERMS

information environment

The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02)

information operations

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries and potential adversaries while protecting our own. Also called **IO**. (JP 1-02)

information superiority

The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02)

This page intentionally left blank.

References

SOURCES USED

These are the sources quoted or paraphrased in this publication.

ARMY PUBLICATIONS

ADP 3-0, *Unified Land Operations,* 10 October 2011.

ADP 5-0, *The Operations Process,* 17 May 2012.

FM 3-05.301, *Psychological Operations Process, Tactics, Techniques, and Procedures,* 30 August 2007.

FM 3-13, *Inform and Influence Activities,* 25 January 2013.

FM 3-53, *Military Information Support Operations,* 4 January 2013.

ARMY FORMS

DA Forms are available on the Army Publishing Directorate web site (www.apd.army.mil).

DA Form 2028 *(Recommended Changes to Publications and Blank Forms).*

JOINT PUBLICATIONS

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 8 November 2010.

JP 3-13, *Information Operations,* 13 February 2006.

This page intentionally left blank.

Index

C

chance encounters and contacts, 2-20

civil-military operations (CMO), 1-2, 2-1, 2-19, 2-30, 2-32, 2-39 and 2-40, 3-1, 3-7, 3-13 and 3-14, 3-18 and 3-19, 4-7

combat camera (COMCAM), 1-2, 1-5, 2-1, 2-17 through 2-19, 2-30 and 2-31, 2-39 and 2-40, 3-1 and 3-2, 3-5 and 3-6, 3-18, 4-7, A-2, C-3,

combined information overlay (CIO), 3-2, 5-3, 5-5 and 5-6, 5-9, A-15, A-17

command information message, 2-20

commander's critical information requirement (CCIR), 3-6, 4-1, A-11 and A-12, A-14 and A-15

computer network attack, 2-16 and 2-17, 2-33, 2-35, 2-38,

computer network defense (CND), 2-16, 2-32 through 2-38

computer network exploitation, 2-16 and 2-17

computer network operations (CNO), vi, 1-2, 1-5, 2-1, 2-16 and 2-17, 3-1, 3-5, 3-13, 3-18

concept of support statements and sketches, 3-9

consequence management, 2-31, 4-3

constraints on information operations, 3-5

countering adversary IO, 2-28

counterintelligence (CI), 1-2, 2-2, 2-4 and 2-5, 2-32 through 2-38, 3-13, C-2 and C-3

crisis-action team, 4-7

critical events, 4-4, A-5

critical information, iv, 2-2 through 2-5, 2-8, 2-19, 3-2, 3-6, 3-8, 3-12, 5-7, A-10, A-15,

criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER), iv, 5-7, 5-8

D

deception in support of OPSEC, 2-4, 2-6, C-3

defense support to public diplomacy (DSPD), 1-2, 2-31, 2-39 and 2-40

demining operations, 2-13

E

effects against the adversary, 3-10

effects for information operations, 3-11

effects to protect friendly forces, 3-10

effects to shape the environment, 3-11

electromagnetic spectrum (EMS), 2-1, 2-15 and 2-16

electronic attack (EA), 2-15 and 2-16, 2-32 through 2-37, 3-5 and 3-6, 3-12, 3-17

electronic warfare (EW), vi, 1-2, 1-5, 2-1, 2-4, 2-15 and 2-16, 2-32 through 2-38, 3-5, 3-12 through 3-14, 3-17 through 3-19, 4-2, 4-7, A-1, C-3

essential elements of friendly information (EEFI), 2-3 through 2-5, 2-19, 2-32, 2-35, 2-39, 3-2, 3-6 and 3-7, 4-4 and 4-5, A-11 and A-12, A-14 and A-15, C-1 through C-3

essential information operations task (EIOT), 3-12

essential tasks for information operations, 3-2

EW planner, 1-5

F

face-to-face meeting, 2-12, 2-20, 2-22, E-1 and E-2

force protection officer, 2-5

foreign internal defense (FID), 1-5, 2-18, 2-31, 3-10, 3-19

friendly-force information requirement (FFIR), A-12, A-15

G

graphic information operations estimate, 3-4

H

humanitarian assistance, 1-4, 2-13, 2-30

I

information assurance (IA), 1-2, 2-16, 2-32 through, 2-38, 3-13

information messages, 2-20

information operations (IO) capabilities, 2-32 through 2-38, 3-13

information operations (IO) objectives, 2-17, 3-3, 3-10 through 3-13, 4-1 and 4-2, 4-5, 4-8, A-4, A-23, A-25

information operations working group (IOWG), 4-6 and 4-7, A-1 through A-3, A-11,

information superiority, vi, 1-1 and 1-2, 1-4 and 1-5, 2-1, 2-5, 2-16, 3-1 and 3-2, 3-7 through 3-10, 3-12 through 3-14, 3-16, 4-4 and 4-5, 5-9, A-5, A-7, A-9, A-22 through A-25,

intelligence preparation of the operational environment (IPOE), 3-2, 3-6, 3-8, 5-1 through 5-3, 5-5, 5-7, 5-9, A-6, A-11, A-15, A-18

intelligence support to IO, 5-3

IO annex, 3-16, A-6, A-24

IO concept of support sketch, 3-14, 3-17

IO intelligence summary, 4-8

IO planner, 1-5, 2-16, 3-1, 3-7, 3-10, 3-19, 4-6, 5-9

IO situation report, 4-8

J

joint special operations task force (JSOTF), 1-5, 2-3, 2-7, 2-12, 2-16, 2-18, 2-28, 2-30, 3-6, 3-19, 4-6, 4-8

K

key-leader engagements, 1-5, 2-1, 2-20, 2-23 and 2-24, 2-30, 4-4, 4-7, 5-9

Page 3062 of 3957

M

measure of effectiveness (MOE), 3-11, 4-2 and 4-3, 4-6

measure of performance (MOP), 4-5

message development, 2-22

military deception (MILDEC), vi, 1-2, 1-5, 2-1 and 2-2, 2-5 through 2-7, 2-9 through 2-11, 2-14, 2-19, 2-32 through 2-38, 3-1, 3-5, 3-13 and 3-14, 3-17 and 3-18, 4-7, A-1, B-1, C-3

Military Information Support operations (MISO), vi, 1-2, 1-5, 2-1, 2-11 through 2-15, 2-18 through 2-21, 2-24, 2-28, 2-30 through 2-39, 3-1, 3-5 and 3-6, 3-13 and 3-14, 3-17 and 3-18, 4-2 through 4-4, 4-6, B-3, E-1 and E-2

MISO programs, 2-11

MISO series, 2-12 through 2-15

mission analysis, iv, 2-12, 3-7, A-11

mission, enemy, terrain and weather, troops and support available-time available, and civil considerations, 1-5

N

noncombatant evacuation operations, 2-13

O

open-source intelligence (OSINT), 2-3, 3-8 and 3-9, 4-3, 5-2, C-2, D-1 and D-2

operation plan, 2-4, 2-28, A-6, C-3

operational-level OPSEC, 2-2

operations security (OPSEC), vi, 1-2, 1-5, 2-1 through 2-6, 2-8, 2-10, 2-12, 2-19, 2-32 through 2-39, 3-6 and 3-7, 3-13 and 3-14, 3-17 and 3-18, 4-7, A-1, B-4, C-1 through C-3

orders production, 3-15, A-6

P

peacekeeping, 1-4

physical attack, 1-2

physical security, 1-2, 2-32, through 2-38

priority intelligence requirement (PIR), 3-7, 5-3, A-12, A-15

propaganda, 2-1, 2-13, 2-26 through 2-29, 2-31, 2-33, 2-39, 3-6, 3-12, 3-18, 4-7, A-15, D-1, D-3 and D-4

public affairs (PA), 1-2, 1-5, 2-1, 2-12, 2-14, 2-18 through 2-21, 2-27 and 2-28, 2-30 through 2-32, 2-39 and 2-40, 3-1, 3-6 and 3-7, 3-13 and 3-14, 3-18, 4-2, 4-4, 4-7, A-1, C-3, D-1

public affairs officer (PAO), 1-5, 2-14, 2-19 and 2-20, 3-1 and 3-2, 3-5, 4-3, 4-6, D-1 and D-2

public information messages, 2-20

R

rewards programs, 1-5

S

Special Forces operational detachment A (SFODA), 2-8, 2-12 and 2-13, 2-16, 2-20, 2-27, 2-32, 3-1 and 3-2, 3-19

Special Forces operational detachment B (SFODB), 2-13, 2-16

special operations task force (SOTF), 1-5, 2-7, 2-12 and 2-13, 2-16, 2-27, 2-30, 3-19, 4-6, 4-8

staff estimate for IO, 3-2, A-22

T

tactical-level OPSEC, 2-2

target audiences, 2-11 through 2-14, 2-20, 2-28 and 2-29, 5-7, B-4, E-1

targeting process, 2-12, 2-20, 5-8

tasks against the adversary, 3-12

tasks to defend friendly forces, 3-13

tasks to shape the environment, 3-13

theme, iv, 2-12, 2-14, 2-21, 2-32, 2-36, D-3

W

working group, 2-3, 2-5, 2-28, 4-2 and 4-3, 4-6, A-1 through A-3, A-5, C-2

working with translators, 2-26

TC 18-06
22 March 2013

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
1307001

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: Not to be distributed; electronic media only.

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SUBVERSIVE INFLUENCE: VULNERABILITIES OF THE UNITED STATES AND ITS ELECTIONS TO RUSSIAN INTERFERENCE CAMPAIGNS

by

Daniel H. McMasters

December 2020

Co-Advisors: Mikhail Tsypkin
Carolyn C. Halladay

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
SUBVERSIVE INFLUENCE: VULNERABILITIES OF THE UNITED STATES AND ITS ELECTIONS TO RUSSIAN INTERFERENCE CAMPAIGNS

5. FUNDING NUMBERS

6. AUTHOR(S) Daniel H. McMasters

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The United States and its allies have been subjected to clandestine interference campaigns led by the Russian government for nearly a century. The targets and mechanisms of subversive Kremlin influence have varied over the decades, but themes such as seeking to tamper with electoral processes have seen refinement and renewed vigor in the 21st century. From the inception of the Soviet Union to the era of Vladimir Putin, this thesis investigates the targets and mechanisms of subversive Russian influence—with particular focus on election meddling—to identify the greatest U.S. vulnerabilities to such interference campaigns. We determined that the Kremlin possesses a wide variety of well-honed tools such as disinformation, cyberattacks, and forgeries that allow it to apply stress to democratic systems and exploit rival nations' internal divisions, and that it has had success in deploying such tools in a number of Western democratic elections since 2014. We find that significant damage to the credibility of elections and the U.S. government is a viable vulnerability for Russian interference campaigns, and that mounting defensive measures against and mitigation thereof must be a top priority for U.S. national and homeland security entities.

14. SUBJECT TERMS Russian interference, cyberattacks, election security, subversive influence	**15. NUMBER OF PAGES** 137
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Page 3068 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 3069 of 3957

Approved for public release. Distribution is unlimited.

SUBVERSIVE INFLUENCE: VULNERABILITIES OF THE UNITED STATES AND ITS ELECTIONS TO RUSSIAN INTERFERENCE CAMPAIGNS

Daniel H. McMasters
Program Analyst, Federal Emergency Management Agency
BA, University of Memphis, 2007

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2020**

Approved by: Mikhail Tsypkin
Co-Advisor

Carolyn C. Halladay
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

Page 3070 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 3071 of 3957

ABSTRACT

The United States and its allies have been subjected to clandestine interference campaigns led by the Russian government for nearly a century. The targets and mechanisms of subversive Kremlin influence have varied over the decades, but themes such as seeking to tamper with electoral processes have seen refinement and renewed vigor in the 21st century. From the inception of the Soviet Union to the era of Vladimir Putin, this thesis investigates the targets and mechanisms of subversive Russian influence—with particular focus on election meddling—to identify the greatest U.S. vulnerabilities to such interference campaigns. We determined that the Kremlin possesses a wide variety of well-honed tools such as disinformation, cyberattacks, and forgeries that allow it to apply stress to democratic systems and exploit rival nations' internal divisions, and that it has had success in deploying such tools in a number of Western democratic elections since 2014. We find that significant damage to the credibility of elections and the U.S. government is a viable vulnerability for Russian interference campaigns, and that mounting defensive measures against and mitigation thereof must be a top priority for U.S. national and homeland security entities.

Page 3072 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 3073 of 3957

TABLE OF CONTENTS

I. INTRODUCTION....1
A. RESEARCH QUESTION....2
B. LITERATURE REVIEW....3
1. Russia's Intent, Capability, and Mechanisms....3
2. 21st Century Vulnerabilities....7
C. RESEARCH DESIGN....12
D. OVERVIEW OF CHAPTERS....12

II. A CENTURY OF KREMLIN INTERFERENCE: DIRTY TRICKS PAST AND PRESENT....15
A. THE ORIGINAL THREAT....15
1. Media Manipulation....16
2. Secret Proxy Organizations....21
3. Forgeries and Rumors....23
4. Manipulating Multiple Sides, Instigating Groups against Each Other, and Inciting Violence....25
5. Diminishing Returns, Lasting Impacts....26
B. CONTEMPORARY ADAPTATIONS AND NEW THREATS....28
1. Media Manipulation....28
2. Proxy Organizations....38
3. New Threats and Force Multipliers: Cyberattacks....44
4. Relative Impunity....49

III. ELECTION INTERFERENCE....51
A. SOVIET MEDDLING IN U.S. ELECTIONS....51
B. MODERN MEDDLING IN U.S. ELECTIONS....54
1. State-Run Media....54
2. Social Media....57
3. Microtargeting....64
4. Hacking and Cyberattacks....65
C. OTHER MODERN RUSSIAN EFFORTS TO INFLUENCE FOREIGN ELECTIONS....68

IV. FALLOUT AND VULNERABILITIES....75

V. CONCLUSION....87

Page 3074 of 3957

LIST OF REFERENCES **89**

INITIAL DISTRIBUTION LIST **119**

LIST OF FIGURES

Figure 1. Back the Badge Facebook Advertisement 59

Figure 2. Stop A.I. (AKA Stop All Invaders) Facebook Advertisement 61

Figure 3. BM (AKA Black Matters) Facebook Advertisement 62

Page 3076 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CHDS	Center for Homeland Defense and Security
CHEKA	All-Russian Extraordinary Commission for Combating Counter Revolution, Profiteering and Corruption (translated from Russian)
CIA	Central Intelligence Agency
COVID-19	coronavirus disease 2019
CPUSA	Communist Party of the United States of America
DDoS	distributed denial of service
DHS	Department of Homeland Security
DNC	Democratic National Committee
DNI	Director of National Intelligence
DOJ	Department of Justice
EU	European Union
FBI	Federal Bureau of Investigation
FSB	Federal Security Service of the Russian Federation (translated from Russian)
G20	Group of Twenty
GRU	Foreign Intelligence Service of the Russian Federation (translated from Russian)
HIV/AIDS	human immunodeficiency virus/acquired immunodeficiency syndrome
IRA	Internet Research Agency
JDL	Jewish Defense League
KGB	Komitet Gosudarstvennoy Bezopasnosti or Committee for State Security (translated from Russian)
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
RT	Russia Today (formerly)
WPC	World Peace Council

Page 3078 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 3079 of 3957

EXECUTIVE SUMMARY

For roughly a century, the United States and its allies have endured coordinated efforts by the Soviet, and then Russian government to interfere in the West's domestic affairs. The frequency, intensity, tactics, and targets of these clandestine attacks have varied over the years, but the Kremlin's main goals of information manipulation, societal destabilization, reputational harm, and political influence have remained largely consistent. The efficacy of Russia's influence measures has also varied over the decades, but 21st-century advances in technology and decreased Western focus on Moscow as a major threat since the end of the Cold War have allowed these insidious tactics to proliferate in new and damaging ways. Left unchecked, Russian influence campaigns could cause severe harm to the integrity of future elections and the credibility of U.S. institutions.[1]

This thesis studies the history of Soviet and Russian meddling in the domestic affairs of the United States and its Western rivals to identify trends in their efforts and successes, and examines various recent interference campaigns as a means to understand the Kremlin's subversive attempts to influence foreign elections unduly. Studying the gradual buildup of capabilities beginning with the Soviet Union through Russian interference in the 2016 U.S. elections, commonalities and signals can be identified that highlight the greatest vulnerabilities faced by the United States and other Western democracies. Common themes this thesis identifies in both Soviet and modern Russian interference efforts include the use of media manipulation, proxy organizations, fabricated material, and instigation of specific, opposing groups to provoke division. Other recent Western elections and referenda allegedly affected by Russian influence, including France's presidential election the following year, further highlight Kremlin attack patterns. Commonalities found in this analysis include hack-and-leak incidents, plots involving election infrastructure, and attempts to manipulate voters through disinformation. What

[1] Charles E. Ziegler, "International Dimensions of Electoral Processes: Russia, the USA, and the 2016 Elections," *International Politics; Basingstoke* 55, no. 5 (September 1, 2018): 569–71, http://dx.doi.org.libproxy.nps.edu/10.1057/s41311-017-0113-1; Vasu Mohan and Alan Wall, "Foreign Electoral Interference: Past, Present, and Future," *Georgetown Journal of International Affairs; Washington* 20 (September 1, 2019): 116.

emerges from this study is a clear signal that credibility of elections and legitimacy of government leaders and institutions are imperiled by Kremlin meddling, without a comprehensive or practical remedy.

Investigative findings by bodies including the bipartisan Senate Intelligence Committee demonstrate unequivocally that Russia's preferred influence operation outcomes in the 2016 U.S. presidential election came to pass, potentially along with "victories" in other elections.[2] With nearly a century of experience in covert influence techniques and plenty of practice trying to interfere in Western elections, Russia has many skills and tools, such as disinformation and cyberattacks with which to continue meddling in the democratic affairs of its rivals. The Kremlin has also clearly signaled an intention to continue stressing rival nations' democratic systems with a variety of techniques and targets, potentially including rumors of corruption and election fraud, exploitation, and exacerbation of domestic civil tensions, and even promotion of secession movements and rebellion loom as possible threats. Challenges to the legitimacy of some future elections are plausible, bolstered by a variety of well-honed Kremlin tradecraft, such as production or dissemination of genuine, doctored, or fabricated material designed to lend credence to allegations.

This thesis chronicles and draws connections between Soviet and modern Russian interference techniques to highlight the Kremlin's capacity and intention to inflict damage, such as election-related chaos and the ruination of the credibility of U.S. government institutions, leaders, and electoral systems. The examples and conclusions presented in this thesis seek to underscore the need for intelligence communities, investigative bodies, and other national and homeland security entities to prioritize efforts to identify, thwart, and deter Russian interference campaigns going forward, particularly with regard to the integrity of the electoral process.

---

[2] *Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia's Use of Social Media with Additional Views*, Rep. 116-XX, Senate, 116th Cong., 1st sess., 2018, 4–8, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

ACKNOWLEDGMENTS

This thesis is dedicated to my late mother, whose constant encouragement and faith in me gave me the motivation to take on the challenge of applying for the Naval Postgraduate School/Center for Homeland Defense and Security (CHDS) program; to my late father, whose support helped me to persevere through obstacles and personal tragedy to make it through 18 months of coursework; to my sister, whose selfless and tireless service as my sounding board, proofreader, and shoulder to cry on as we coped was immense and invaluable; and to my wife and children, whose patience and inspiration as I struggled through this long thesis journey while grieving the loss of my parents will take a lifetime to repay. Mom, Dad, Melissa, Ira, Matviy, Anya—from the bottom of my heart, thank you! You were my motivation, and my rock.

Special thanks go out to all my CHDS professors, classmates, administrators, support personnel, editor Nancy Sharrock, and thesis advisors, Drs. Halladay and Tsypkin. All of them showed me kindness, patience, and encouragement when I needed it most; some, such as Dr. Bellavita, also provided carrots. Many thanks as well are in order to my colleagues and supervisors at the Transportation Security Administration, Federal Emergency Management Agency, and Cybersecurity and Infrastructure Security Agency who gave me the opportunity and support I needed to complete this project while dealing with profound losses, joyous family additions, stressful relocations, unprecedented disaster and pandemic response, and multiple career changes (especially Randy Cotten, who always encouraged me to apply for training but falsely claimed “I can’t help you get a master’s degree,” and Eric Rosner, who never let me forget that I had an extension deadline looming). Many times during the course of this academic journey, I feared I had taken on too much all at once, but friends, family, classmates, and faculty lifted me every step of the way to get me through it. I cannot possibly thank you all enough for your support and all I learned from you along the way. I will be forever grateful for the experience and opportunity, as well as your faith in me.

Page 3082 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

For roughly a century, the United States and its allies have endured coordinated efforts by the Soviet, and then Russian government to interfere in the West's domestic affairs. The frequency, intensity, tactics, and targets of these clandestine attacks have varied over the years, but the Kremlin's main goals of information manipulation, societal destabilization, reputational harm, and political influence have remained largely consistent. The efficacy of Russia's influence measures has also varied over the decades, but 21st-century advances in technology and decreased Western focus on Moscow as a major threat since the end of the Cold War have allowed these insidious tactics to proliferate in new and damaging ways. Left unchecked, Russian influence campaigns could cause severe harm to the integrity of future elections and the credibility of U.S. institutions.[1]

Current Russian President Vladimir Putin is widely regarded as seeking to expand his nation's global influence and regional dominance, as well as to suppress any potential threat to his authoritarian grip on power in Russia.[2] While Putin may not share his Soviet predecessors' worries about imminent nuclear war with the United States, he does appear to retain their bitter mistrust and hostility toward the nation, which he accuses of fomenting and financing unrest within Russia along with revolutions in neighboring states.[3] Just as the Soviet leadership before him did, Putin appears to see weakening the U.S. government and its global influence as a key component of Russia's security and external power goals.

---

[1] Charles E. Ziegler, "International Dimensions of Electoral Processes: Russia, the USA, and the 2016 Elections," *International Politics; Basingstoke* 55, no. 5 (September 1, 2018): 569–71, http://dx.doi.org.libproxy.nps.edu/10.1057/s41311-017-0113-1; Vasu Mohan and Alan Wall, "Foreign Electoral Interference: Past, Present, and Future," *Georgetown Journal of International Affairs; Washington* 20 (September 1, 2019): 116.

[2] Robert Person, "Balance of Threat: The Domestic Insecurity of Vladimir Putin," *Journal of Eurasian Studies* 8, no. 1 (January 1, 2017): 44–45, https://doi.org/10.1016/j.euras.2016.11.001; Kari Roberts, "Understanding Putin: The Politics of Identity and Geopolitics in Russian Foreign Policy Discourse," *International Journal: Canada's Journal of Global Policy Analysis* 72, no. 1 (March 1, 2017): 29–30, https://doi.org/10.1177/0020702017692609.

[3] Vladimir Putin, "Predsedatel Pravitelstva Rossiyskoy Federatsiy Vladimir Putin provel zasedaniye Koordinatsionnovo soveta Obshcherossiyskovo narodnovo fronta" [Prime Minister of the Russian Federation Vladimir Putin led the Coordination Council of the All-Russia People's Front], Pravitel'stvo Rossiyskoy Federatsii [Office of the Prime Minister of the Russian Federation news release], December 8, 2011, https://web.archive.org/web/20120607083034/http://premier.gov.ru/events/news/17330/.

Page 3084 of 3957

As such, he employs the Kremlin's military and intelligence apparatus to do so.[4] Putin appears to believe that his foes engage in similar tactics, likely leading him to see Russia's influence campaigns as necessary, justified, and urgent. He has accused the U.S. government of fomenting revolutions in Eastern Europe to disrupt Russia's regional hegemony, aggressively expanding the North Atlantic Treaty Organization (NATO) to Russia's borders as a direct military provocation, and even attempting to remove him from power by leading a clandestine revolt.[5] Combined with his apparent fear that Western-style democracy could eventually lead to the end of his authoritarian reign, Putin has ample motivation to take steps to undermine and weaken the United States and its democratic allies. As such, the U.S. government must be aware of and on guard against all of Russia's destabilization efforts.

The November 2020 U.S. elections provide a case in point.[6] These elections took place in an environment in which the prospect of Russian interference was of grave concern to some voters and dismissed as a hoax by others, following years of reports and investigations about alleged Kremlin-backed election infrastructure tampering, dissemination of misinformation, and even attempts to incite violence.[7]

A. RESEARCH QUESTION

What are the greatest U.S. vulnerabilities to Kremlin interference campaigns, particularly with regard to elections?

---

[4] Michael Isikoff and David Corn, *Russian Roulette: The Inside Story of Putin's War on America and The Election of Donald Trump*, 1st ed. (New York: Twelve, 2018, 49, 57–58; Malcolm W. Nance, *The Plot to Destroy Democracy: How Putin and His Spies Are Undermining America and Dismantling the West*, 1st ed. (New York: Hachette Books, 2018), loc. 3561–3571 of 5796, Kindle.

[5] Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC: Defense Intelligence Agency, 2017), 15–17, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf?ver=2017-06-28-144235-937; Richard Sakwa, "'New Cold War' or Twenty Years' Crisis? Russia and International Politics," *International Affairs* 84, no. 2 (March 1, 2008): 257–263, https://doi.org/10.1111/j.1468-2346.2008.00702.x.

[6] Richard Clarke, "Counterterrorism Expert Richard Clarke on Trump's Relations with Intelligence Agencies," NPR, February 17, 2017, http://www.npr.org/2017/02/17/515728608/counterterrorism-expert-richard-clarke-on-trumps-relations-with-intelligence-age.

[7] University of Chicago Harris School of Public Policy and Associated Press-NORC Center for Public Affairs Research, *Americans Split on Relationship with Russia* (Chicago, IL: University of Chicago Harris School of Public Policy, 2020), https://apnorc.org/wp-content/uploads/2020/10/topline_release1.pdf.

Page 3085 of 3957

B. LITERATURE REVIEW

This section focuses on Russia as a saboteur attacking the civil society of other nations from within through manipulation of such tools as cyber infrastructure and access to information. Because incidents, such as the 2016 U.S. presidential election interference, involve such relatively novel mechanisms as cybersecurity and the use of social media or alternative news sources, much of the available literature is very recently published.[8] A consensus apparently does not exist regarding which aspect or target of subversive Russian attacks is the most important or dangerous; as a result, the burgeoning array of recent sources lacks a cohesive narrative, theme, or focus.

1. Russia's Intent, Capability, and Mechanisms

An abundance of literature dutifully explains Vladimir Putin's belief that modern Russia deserves to be the center of the Slavic and Eurasian world and at least as strong a global power as the Soviet Union and Imperial Russia once were.[9] Many works credit Putin's adversarial attitude toward the West to a fear that expansion of the NATO military alliance is designed to weaken or threaten Russia's global prominence and its dominance of the Eastern European and Central Asian regions.[10] Among these writers, prominent Russian dissident Garry Kasparov and U.S. historian Walter Laqueur argue that the Russian president views his nation's success and security as a zero-sum game requiring the weakening of the United States and its allies, as well as a global acknowledgement that many states from the former Soviet territories must remain irrevocably within Russia's

[8] Amos C. Fox and Andrew J. Rossow, "Assessing Russian Hybrid Warfare: A Successful Tool for Limited War," *Small Wars Journal* 12, no. 1 (August 8, 2016).

[9] Peter Pomerantsev, "Yes, Russia Matters: Putin's Guerrilla Strategy," *World Affairs* 177, no. 3 (September 30, 2014): 21; Tassos E. Fakiolas and Efstathios T. Fakiolas, "Domestic Sources of Russia's Resurgence as a Global Great Power," *Journal of International and Area Studies* 16, no. 2 (December 1, 2009): 100–101.

[10] John J. Mearsheimer, "Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions that Provoked Putin," *Foreign Affairs*, September 30, 2014, 77–79; Douglas Mastriano, "Putin—The Masked Nemesis of the Strategy of Ambiguity," *Defense & Security Analysis* 33, no. 1 (January 20, 2017): 69–70, https://doi.org/10.1080/14751798.2016.1272175.

orbit.[11] According to Laqueur, "Russian government strategy is dominated by the American shadow and the conviction that what helps the United States must be bad for Russia."[12] By extension, the Kremlin strategy also presupposes that what hurts the United States is quite likely beneficial for Russia.

Many sources emphasize that Putin's prior career as a foreign counterintelligence operative with the KGB[13] guides his alleged heavy use of clandestine or obfuscated tactics of subversion.[14] For example, Malcolm Nance warns, "For [Putin] to succeed at the mission of damaging the United States, he will use all tools of the Russian statecraft such as forging alliances, but also blackmail, propaganda, and cyberwarfare."[15] Regrettably, Nance's books and a number of other publications on the subject veer out of objective analysis and into sharply partisan political rhetoric. For example, Nance indulges his apparent distaste for Donald Trump with colorful descriptions, such as "Worse than his mouth was his fingers when connected to Twitter. In 140 characters he managed to derail his candidacy with insulting, racy, or inappropriate comments," potentially alienating some readers and blurring his analysis with his editorializing.[16] With years-long federal investigations into whether Russian interference helped Trump defeat Hillary Clinton in a polarizing 2016 election (and outsized national media coverage thereof), an influx of partisan, biased, and emotion-infused works on the topic is not particularly surprising, but must be taken with a grain of salt. Without much difficulty, recent mainstream newspaper articles and mass market books arguing for and against many Russia-based allegations can easily be found. To separate signal from noise and preserve accuracy, this thesis relies on scholarly, peer-reviewed sources where available. Study of partisan, biased, and speculative works is

---

[11] Garry Kasparov and Mig Greengard, *Winter Is Coming: Why Vladimir Putin and the Enemies of the Free World Must Be Stopped*, 1st ed. (New York: PublicAffairs, 2015), 253; Walter Laqueur, *Putinism: Russia and Its Future with the West*, 1st ed. (New York: Thomas Dunne Books, 2015), 151.

[12] Laqueur, 151.

[13] Komitet Gosudarstvennoi Byezoapasnosti [the Soviet Union's Committee for State Security].

[14] Malcolm Nance, *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election* (New York: Skyhorse Publishing, 2016), 24–26; Nance, *The Plot to Destroy Democracy*, loc. 687–701.

[15] Nance, *The Plot to Hack America*, 36; Nance, *The Plot to Destroy Democracy*, loc. 687–701.

[16] Nance, *Plot to Hack America*, 13.

nevertheless insightful, as the existence of multiple popular public works espousing exaggerated dangers, misguided fears, or foolhardy dismissal of legitimate risks could work to Russia's advantage as it seeks to undermine, conceal, and obfuscate. One example is a nakedly partisan 2018 work entitled *Russia Hoax* penned by a longtime Fox News anchor, which devotes an entire chapter to downplaying or refuting risks and legal questions regarding a controversial meeting between Trump campaign representatives and Russian representatives offering "dirt" on Clinton.[17]

A study by Kevin McCauley shows how Soviet manipulation techniques have evolved into the current threat posed by Putin's Kremlin.[18] This work alleges that in addition to launching conspiracy theory-peddling media disinformation campaigns and employing online "troll armies" to disparage unfavorable information sources, Russia employs targeted destabilization campaigns in a number of NATO and European Union (EU) countries in a further effort to weaken or dismantle the alliances.[19] Citing reports from NATO and the governments of Estonia, Moldova, and the United States, McCauley asserts, "The Russian Federation is conducting sophisticated and large-scale disinformation campaigns to destabilize U.S. allies and interests" and explains, "Russia continues to employ influence methods formulated under the Soviets, as well as integrating new information age methods."[20] His conclusions support others warning that Russia uses "troll armies" and such other cyber tactics as social media.

In pursuit of destabilization, Russia has been accused of interfering with elections of friend and foe alike, including Ukraine, Moldova, Georgia, the United States, Great

---

[17] Gregg Jarrett, *Russia Hoax: The Illicit Scheme to Clear Hillary Clinton and Frame Donald Trump* (Northampton, MA: Broadside Books, 2018), 171–190.

[18] Kevin N. McCauley, *Russian Influence Campaigns against the West: From the Cold War to Putin* (North Charleston, SC: CreateSpace Independent Publishing Platform, 2016).

[19] "Russian troll armies" is a term used to describe networks of internet commentators, allegedly paid by the Kremlin and often posing as Westerners, who systematically post propagandistic comments on Western news articles and social media in support of Russia or against its foes.

[20] McCauley, *Russian Influence Campaigns*, loc. 8541–8697.

Britain (particularly regarding Brexit), and France.[21] Mikhail Myagkov, Peter Ordeshook, and Dimitry Shakin provide "evidence and eyewitness accounts that even Russian spin doctors and those who committed fraud cannot dispute" of fraudulent machinations employed to ensure favorable results in both Russian and Ukrainian elections within the 21st century.[22] The same author team reached similar conclusions through a separate analysis of the 2004 Orange Revolution in Kyiv.[23] Ominously, both the 2009 *Forensics of Election Fraud* and the 2008 *Election Fraud: Detecting and Deterring Electoral Manipulation* also devote pages to the study of the U.S. vulnerability to election fraud, with the latter detailing several mechanisms by which Americans' confidence in the legitimacy of the vote could be shaken. One warning stands out sharply, namely that "in the United States since the 2000 election there have been concerns raised regarding electoral irregularities—either intentional election fraud or unintentional problems in the election that result in an inaccurate (and thus sometimes in the eyes of the losing side, fraudulent) outcome."[24] In more detail, the authors assert:

> The ongoing debate about the security of electronic voting technologies reflects one aspect of this debate. Concerns have also been raised about fraud in absentee voting, early voting, precinct voting, and voting by military personnel and overseas civilians… that are all unrelated to the type of voting technologies used. Moreover, in the 2002 gubernatorial election

[21] Vladimir Socor, "Russia Orchestrates Gagauz Election in Moldova, Ponders the Next Steps," NGO Publication, *Jamestown Foundation* 12, no. 59 (March 15, 2015), https://jamestown.org/program/russia-orchestrates-gagauz-election-in-moldova-ponders-the-next-steps/; Luke Harding, "Barack Obama Urges Russia Not to Interfere in Neighbouring States," *The Guardian*, sec. World news, July 7, 2009, https://www.theguardian.com/world/2009/jul/07/obama-russia-first-trip; Nance, *The Plot to Hack America*, 62; Isobel Thompson, "Did Russia Hack the Brexit Vote?," *Vanity Fair*, April 12, 2017, http://www.vanityfair.com/news/2017/04/did-russia-hack-the-brexit-vote; "France Warns Russia against Interfering in Elections," Radio France Internationale, February 16, 2017, http://en.rfi.fr/france/20170216-france-warns-russia-against-interfering-elections.

[22] Mikhail G. Myagkov, Peter C. Ordeshook, and Dimitri Shakin, *The Forensics of Election Fraud: Russia and Ukraine* (Cambridge, New York: Cambridge University Press, 2009), 139.

[23] Mikhail Myagkov, Peter C. Ordeshook, and Dimitry Shakin, "Fraud or Fairytales: Russia and Ukraine's Electoral Experience," *Post-Soviet Affairs* 21, no. 2 (January 1, 2005): 91–131, https://doi.org/10.2747/1060-586X.21.2.91.

[24] R. Michael Alvarez, Thad E. Hall, and Susan D. Hyde, eds., *Election Fraud: Detecting and Deterring Electoral Manipulation* (Washington, DC: Brookings Institution Press, 2008), 71.

Page 3089 of 3957

> in New Hampshire, there were convictions related to jamming political party 'get-out-the-vote' telephone banks.[25]

Such factors point to a potentially serious security risk. Between Russia's experience, history, and motivation regarding election infrastructure tampering in foreign states, and existing latent susceptibility to shaken confidence in U.S. elections, the Kremlin has a sizable opening to exploit in its destabilization efforts, and may already be attempting to make use of it.

2. 21st Century Vulnerabilities

Covert interference can take many different forms, and democratic elections can be subverted in a variety of ways from voter suppression and election infrastructure tampering to subversive attempts to influence potential voters. Works related to Russian attacks and emerging vulnerabilities regarding elections have proliferated in recent years, though some topics have garnered considerably more attention than others have. Methods of interference Russia has been accused of using to disrupt Western states' electoral processes successfully include the following:

- hacking as a form of espionage or sabotage
- the leaking of stolen information
- propagating false news and propaganda distribution and promotion
- deployment of online troll armies
- the financing of fringe candidates
- release of *kompromat* (compromising material) to damage a government leader or political candidate
- provocation and support of secession-minded dissidents

[25] Alvarez, Hall, and Hyde, 71.

Page 3090 of 3957

Of these tools, one with an abundance of recently produced literature is the topic of hacking. Cybersecurity sources from 2014 and earlier seem to focus on the threat to infrastructure, military, and intelligence rather than the use of stolen information to tip the balance in elections and undermine a particular candidate, party, or entity, but even on this topic, a consensus is also lacking. Marc Goodman presents dire warnings of drone and pacemaker hacking, as well as a large-scale power grid shutdown, in *Future Crimes*; likewise, Ted Koppel's *Lights Out* points out that Russia has already penetrated the United States' power grid network.[26] Both of these volumes argue that the U.S. government is not adequately equipped to deal with the large-scale disaster that a sustained cyberattack on the grid could cause, whether due to legislative inaction or practical limitations. Koppel's caution is particularly dire. He warns:

> The American public are not the only ones unwilling to contemplate, much less cope with, the eventuality of a debilitating cyberattack against our power grid. The government agencies and civic organizations charged with enabling the nation to recover from catastrophe are also woefully unprepared.[27]

Such lack of readiness could be due to any or all of the same failures (imagination, policy, capabilities, and management) identified in the 9/11 Commission Report regarding the federal government's inability to stop the novel terrorist attacks of September 11, 2001; indeed, each of these are alleged to some degree in Goodman and Koppel's works.[28] Though books, reports, and studies critical of U.S. government inaction and lack of preparedness against state-sponsored hacking threats are increasingly prevalent, works analyzing existing shortfalls and capabilities are less abundant but beginning to emerge. In March 2020, a congressionally sponsored group called the U.S. Cyberspace Solarium

---

[26] Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, First Anchor Books Edition (New York: Anchor Books, 2016), 43, 338–341; Ted Koppel, *Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath*, 1st ed. (New York: Crown Publishers, 2015), 71–72.

[27] Koppel, *Lights Out*, 92.

[28] Thomas H. Kean and Lee Hamilton and U.S. National Commission on Terrorist Attacks upon the United States, *9/11 Commission Report: The Official Report of the 9/11 Commission and Related Publications* (Washington, DC: Government Printing Office, 2004), http://www.gpoaccess.gov/911/index.html.

Commission released a report detailing risks, outlining challenges, and recommending a strategy of "layered cyber deterrence" U.S. government agencies could adopt to mitigate its cyber-based vulnerabilities.[29] The report contained more than 80 recommendations for U.S. government entities on the topics of structural reform, cultivation of enforcement tools, and promotion of resilience and collaboration with the private sector, though it remains unclear how many will be adopted. A consortium of U.S. government agencies attempted to conduct a 2020 exercise of a large-scale state-sponsored cyberattack with kinetic effects and produce an interagency after-action report, but the COVID-19 pandemic scuttled these plans.[30]

Works covering the spread of false information—"fake news"—have become abundant since the 2016 U.S. presidential election, to include information deliberately spread by suspected Russian actors. A 2017 paper from Stanford University states:

> Recent evidence shows that: 1) 62 percent of U.S. adults get news on social media; 2) the most popular fake news stories were more widely shared on Facebook than the most popular mainstream news stories; 3) many people who see fake news stories report that they believe them; and 4) the most discussed fake news stories tended to favor Donald Trump over Hillary Clinton.[31]

A key challenge to such recent studies is the fact that the fake-news environment continually changes in the era of social media; as awareness of fake-news campaigns and the associated risks grow, governments and media entities adapt to contain them, while purveyors rapidly adapt to the restrictions and entrepreneurs capitalize on dissent. For example, social media platforms Facebook, Twitter, Reddit and YouTube each took a number of escalating measures between 2017 and 2020 in reaction to novel fake-news tactics, but still drew criticism in the process and sometimes had to roll back certain actions

---

[29] Cyberspace Solarium Commission, *Report* (Arlington, VA: Cyberspace Solarium Commission, 2020), https://www.solarium.gov/report.

[30] "National Level Exercise 2020," *Federal Emergency Management Agency* (blog), July 23, 2020, https://www.fema.gov/emergency-managers/planning-exercises/nle/2020.

[31] Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (February 16, 2017): 212, https://doi.org/10.1257/jep.31.2.211.

in response to the backlash.[32] At the same time, such rival platforms as Gab and Parler have emerged specifically as an alternative for social media users frustrated by the restrictions of the industry's titans.[33] As a result, many recent works studying the environment of fake news and social media have become quickly outdated, and exist mainly as an incomplete snapshot in time inside a rapidly changing ecosystem. As a case in point, two 2020 studies on Facebook's internal efforts to combat fake news, while insightful and not without merit, each focused on measures the company modified, improved, or replaced just months later in response to newer threat information and public feedback regarding its policies.[34]

Books, think-tank reports, and a number of government hearings and reports highlight Russia's role in disinformation campaigns, including fake news and

[32] An example of measures rolled back due to criticism include Twitter's October 2020 decision to rescind its ban on the sharing of a controversial article about U.S. presidential candidate Joe Biden and his son. The veracity of the article's assertions had been heavily questioned and some U.S. lawmakers had warned of a high probability that its genesis had been a Russian disinformation campaign, though the official reason for Twitter's ban (and the blocking of Trump administration and congressional accounts that attempted to share it) was that the article contained private personal information and material allegedly gleaned from a hack. The reversal came after withering criticism and accusations of politically motivated censorship from President Trump and lawmakers from his party. The official reason given by Twitter was that the article had received so much attention that the information therein was no longer technically "private," and it did not publicly explain whether its stance on the allegations that it came from hacked material had changed. Paul Mena, "Cleaning up Social Media: The Effect of Warning Labels on Likelihood of Sharing False News on Facebook," *Policy & Internet* 12, no. 2 (June 1, 2020): 166, https://doi.org/10.1002/poi3.214; Petros Iosifidis and Nicholas Nicoli, "The Battle to End Fake News: A Qualitative Content Analysis of Facebook Announcements on How It Combats Disinformation," *International Communication Gazette* 82, no. 1 (February 1, 2020): 74, https://doi.org/10.1177/1748048519880729; Catherine Sanz and Catherine Thorbecke, "What Social Media Giants Are Doing to Counter Misinformation This Election," ABC News, October 18, 2020, https://abcnews.go.com/Technology/social-media-giants-counter-misinformation-election/story?id=73563997; Kevin Roose, "Facebook and Twitter Dodge a 2016 Repeat, and Ignite a 2020 Firestorm," *New York Times*, sec. Technology, October 15, 2020, https://www.nytimes.com/2020/10/15/technology/facebook-twitter-nypost-hunter-biden.htm; Kate Conger and Mike Isaac, "In Reversal, Twitter Is No Longer Blocking New York Post Article," *New York Times*, sec. Technology, October 16, 2020, https://www.nytimes.com/2020/10/16/technology/twitter-new-york-post.html.

[33] Craig Timberg and Isaac Stanley-Becker, "QAnon Learns to Survive—And Even Thrive—After Silicon Valley's Crackdown," *Washington Post*, October 28, 2020, https://www.washingtonpost.com/technology/2020/10/28/qanon-crackdown-election/.

[34] Mena, "Cleaning Up Social Media"; Iosifidis and Nicoli, "The Battle to End Fake News"; Conger and Isaac, "In Reversal, Twitter Is No Longer Blocking New York Post Article."

Page 3093 of 3957

propaganda.[35] The House of Representatives Committee on Armed Services 2015 hearing *Countering Adversarial Propaganda* and the Committee on Foreign Affairs' hearing *Confronting Russia's Weaponization of Information* from later that year provide a glimpse into the U.S. acknowledgement of Russia's campaign to harm the West through targeted information.[36] In the former, a member of the U.S. government's Broadcasting Board of Governors testified:

> With Russia, much of the propaganda that surfaces is aimed at destabilizing the West, undermining the trust and credibility of journalism, of government, of NATO, of EU, and all those things…the Russian propaganda aimed at the non-Russian audiences aimed at undermining NATO, EU, government, media…is a very scary destabilizing influence if it is actually having the impact—and it is a seeping impact—onto the audience.[37]

The latter went much further, beginning with a stark warning from Russian propaganda expert Peter Pomeranstev, who explained that while Russia knew it was no match for NATO in physical combat:

> what if the Kremlin could bypass NATO militarily, make war without ever, officially at least, firing a shot? What if it could use the very openness of democracy's open markets, open culture and, very importantly, open information against us? So over the 21st century, Russian military theorists developed a theory of what they called information psychological or hybrid war—a mix of media, economic and cultural warfare with a dab of covert military action.[38]

Witnesses at the hearing also explained how such a strategy was enacted through a wide array of tools to include what Pomerantsev described as "bankrolling and lending political support to both far right and far left parties" to create instability in Western nations,

---

[35] Marcel van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (Lanham: Rowman & Littlefield, 2016).

[36] *House Committee on Armed Services, Countering Adversarial Propaganda: Charting an Effective Course in the Contested Information Environment: Hearing before the Subcommittee on Emerging Threats and Capabilities*, House of Representatives, Hrg. 59, serial 97-493, 114th Cong., 1st sess., 2015; *House Committee on Foreign Affairs, Confronting Russia's Weaponization of Information: Hearing before the Committee on Foreign Affairs*, House of Representatives, serial 114-37, 114th Cong., 1st sess., 2015.

[37] H.R., *House Committee on Armed Services, Countering Adversarial Propaganda*, 15.

[38] H.R., *House Committee on Foreign Affairs, Confronting Russia's Weaponization of Information*, 5–6.

weakening U.S. influence and NATO power, and working to "sow divisions, demoralize and disorganize—to weaponize information." Such reports illustrate that while the U.S. government may not have had remedies for Russian destabilization efforts in the mid-2010s, it was not necessarily unaware of the threat thereof.

C. RESEARCH DESIGN

This thesis studies the history of Soviet and Russian meddling in the domestic affairs of the United States and its Western rivals to identify trends in their efforts and successes. My analysis requires a study of the known threats, adversarial tactics, and vulnerabilities and the Kremlin's apparent goals, to identify possible unmet needs for U.S. security and intelligence entities to use in countering Russian interference.

This thesis studies various recent interference campaigns as a means to understand the Kremlin's subversive attempts to influence foreign elections unduly. After studying the gradual buildup of capabilities beginning with Soviet Union, I explore the case of established Russian interference in the 2016 U.S. elections and trace Russia's actions to identify commonalities or signals to ascertain better the greatest vulnerabilities Russia has an opportunity to exploit. Common themes I identified in both Soviet and modern Russian interference efforts include the use of media manipulation, proxy organizations, fabricated material, and instigation of specific, opposing groups to provoke division. I also compare the 2016 U.S. election case to other recent Western elections and referenda allegedly affected by Russian influence, including France's presidential election the following year. Commonalities found in this analysis include hack-and-leak incidents, plots involving election infrastructure, and attempts to manipulate voters through disinformation. What emerges from this study is a clear signal that the credibility of elections and legitimacy of government leaders and institutions are imperiled by Kremlin meddling, without a comprehensive or practical remedy.

D. OVERVIEW OF CHAPTERS

In Chapter II, I outline the evolution and refinement of Russian interference campaigns from their genesis in the early days of the Soviet Union through to the era of Putin's second decade in power to highlight the scope and seriousness of the threat faced

by the United States and its Western allies. Chapter III is an in-depth look at how the Kremlin's refined disinformation system was deployed within the U.S. 2016 presidential election campaign, along with similar actions in EU member states' elections. In Chapter IV, I examine the fallout from Russia's meddling in the 2016 U.S. presidential campaign to determine plausible damage scenarios the United States may encounter if it fails to deter or mitigate against ongoing and future Russian disinformation efforts effectively.

THIS PAGE INTENTIONALLY LEFT BLANK

Page 3097 of 3957

II. A CENTURY OF KREMLIN INTERFERENCE: DIRTY TRICKS PAST AND PRESENT

Russia's present capabilities and strategies to destabilize rival governments are the product of a long history of refinement. This chapter chronicles three elements of Soviet influence campaigns: media manipulation, secret proxy organizations, forgeries and rumors, and manipulating and instigating multiple groups to distrust and attack each other. The present analysis then shows how such methods have evolved into the contemporary threat toolbox, which still features media manipulation and proxy organizations while adding novel cyberattacks as a force multiplier.

A. THE ORIGINAL THREAT

From its inception in the 1920s, the Soviet Union developed and refined a sophisticated series of subversive actions and manipulation techniques to employ against the United States and its allies. The Kremlin's main security agencies (in various incarnations including Cheka, NKVD, KGB, GRU, and FSB) have dedicated official departments to carrying out these attacks, known primarily as "active measures," for example, "dezinformatsiya"—disinformation.[39]

In a Cold War-era study of the long history of Soviet disinformation campaigns, Roy Godson and Richard Shultz defined "active measures" as:

> influencing the policies of another government, undermining confidence in its leaders and institutions, disrupting relations between other nations, and discrediting and weakening governmental and non-governmental opponents. This frequently involves attempts to deceive the target… and to distort the target's perceptions of reality.[40]

---

[39] Federal Security Service of the Russian Federation, all referred to herein using common anglicized transliterations of their Russian-language acronyms. "Cheka"—1917–1922, All-Russian Extraordinary Commission for Combating Counter-Revolution, Profiteering and Corruption; "NKVD"—1922–1943, People's Commissariat for Internal Affairs; "KGB"—1954–1991, Committee for State Security; "GRU"—1991–present, Foreign Intelligence Service of the Russian Federation; "FSB"—1995–present, Federal Security Service of the Russian Federation. Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (Washington, DC: Pergamon-Brassey's, 1984); Isikoff and Corn, *Russian Roulette*.

[40] Shultz and Godson, 2.

Page 3098 of 3957

"Dezinformatsiya" was one of the principal tools of a broader campaign to alter perceptions and attitudes in ways that benefited the Soviet Union, and proved to be one of its most insidious weapons. With the strategic use of this discipline, Moscow could cause covert damage in the West without drawing it into a potentially catastrophic armed conflict, and support behaviors and policy changes in rival states where threats and diplomatic entreaties could not succeed.

1. Media Manipulation

One of the earliest examples of calculated manipulation of Western audiences involved compromising a trusted source within a prominent American newspaper: *The New York Times*. In the 1930s, *Times* columnist Walter Duranty won a Pulitzer Prize for descriptions of Soviet dictator Joseph Stalin and conditions of life under his rule, but subsequent research reveals that his articles ranged from hagiographic to deeply disingenuous.[41] Duranty produced deliberately inaccurate dispatches from his post within the Soviet Union that aggressively contradicted reports of a brutal famine in the country's western regions (this mass starvation, known as *Holodomor*, is now widely believed to have been a purposefully created genocide conducted by Stalin against Ukrainian peasants).[42] Duranty not only presented a deceptively rosy picture of Ukrainian life in his articles during the time of mass famine, but also actively sought to discredit accurate Western reporting on it.[43] Most notably, he forcefully refuted the accurate press releases of Gareth Jones, a British reporter for prominent newspaper *The Times* whose subsequent murder was allegedly carried out by Soviet secret police ordered to put an end to his

[41] S. J. Taylor, *Stalin's Apologist: Walter Duranty, The New York Times's Man in Moscow* (New York: Oxford University Press, 1990); Askold Krushelnycky, "Ukrainians Want Pro-Stalin Writer Stripped of Pulitzer," *The Guardian*, sec. World News, May 4, 2003, http://www.theguardian.com/world/2003/may/04/russia.usa.

[42] Robert Conquest, *The Harvest of Sorrow: Soviet Collectivization and the Terror-Famine* (New York, NY: Oxford University Press, 1987), 320.

[43] Conquest, 320.

negative reporting.[44] Duranty's attempts to destroy Jones's credibility hint that his Soviet benefactors had both the intent and the means to influence Western opinion both through false information and the suppression of factual information it found unpalatable.

By all appearances, Duranty's actions were not the work of an objective, honest journalist, working independently without bias or coercion. Duranty enjoyed a lavish lifestyle during his tenure as a journalist in Moscow, to include awards and praise bestowed on him by Joseph Stalin.[45] By all appearances, the Soviet government made concerted efforts to ensure that its relationship with Duranty was a positive one with "benefits" to both sides; in a country known for its iron grip on control of the domestic press, the fact that Stalin praised and likely courted a renowned Western reporter is a telling sign of the Kremlin's strategy of information manipulation abroad.

According to Robert Conquest, Duranty may have had other incentives to write articles in service of the Soviet Union beyond being seduced by the opportunity to boost his career with interviews and unrivaled access to Stalin; he was possibly being blackmailed as well.[46] In one of the earliest potential examples of Soviet manipulation of Western citizens through *kompromat*, it has been alleged that Stalin's secret police used knowledge of Duranty's opium abuse and participation in bisexual orgies to ensure that his journalistic missives were acceptable to, if not laudatory of, the Communist Party of the Soviet Union.[47]

According to Duranty biographer S. J. Taylor, Duranty's Soviet-friendly *New York Times* articles influenced President Franklin Delano Roosevelt's 1933 decision to grant

---

[44] Marco Carynnyk, "The Famine the 'Times' Couldn't Find," *Commentary Magazine*, November 1, 1983; Ray Gamache, *Gareth Jones: Eyewitness to the Holodomor* (Cardiff, Wales: Welsh Academic Press, 2016); Anne Applebaum, "How Stalin Hid Ukraine's Famine from the World," *The Atlantic*, October 13, 2017, https://www.theatlantic.com/international/archive/2017/10/red-famine-anne-applebaum-ukraine-soviet-union/542610/.

[45] Carynnyk.

[46] Krushelnycky, "Ukrainians Want Pro-Stalin Writer."

[47] *Kompromat* is a Russian-language term for a political tool attributed to the Soviet and Russian government in which negative information about an individual, usually a politician or public figure, is obtained, cultivated, or manufactured for use in discrediting, intimidating, or blackmailing the individual. Krushelnycky, "Ukrainians Want Pro-Stalin Writer."

Page 3100 of 3957

diplomatic recognition of the Soviet Union.[48] Notably, Roosevelt's recognition of the Soviet Union was contingent on a guarantee from the Soviets that they would not interfere in domestic American affairs or disseminate propaganda within U.S. territory; the U.S. government already suspected such an agenda.[49] Declassified State Department documents show that diplomatic relations between the two nations soured within months of the recognition, as "evidence emerged that the Soviet Government had violated its pledge not to interfere in American domestic affairs" along with reports of state-sponsored killings known as "The Great Purge."[50]

Manipulation of the press to benefit the Soviet Union was a feature of *dezinformatsiya* in neutral states as well. A Central Intelligence Agency (CIA) report revealed that the Soviet Union managed to place more than 160,000 messages into India's ostensibly free press between the 1960s and 1980s by using several hundred bribed or compromised journalists across at least six English-language papers.[51] The smuggled notes of KGB dissident Vasili Mitrokhin later corroborated this report that indicated that no fewer than 10 Indian papers were under Kremlin control by 1973 and more than 5,500 KGB-tailored articles appeared in Indian papers in 1975 alone.[52] Along with allegedly outright coercing individual journalists to do their bidding, the Soviets also exercised other types of influence, both overt and clandestine, over foreign press to amplify their disinformation.[53] The CIA report describes two methods by which disinformation made its way into prestigious Indian papers that relied on credible sources. In one method, Soviet operatives debuted fraudulent articles in smaller and less-heralded publications—for

---

[48] Taylor, *Stalin's Apologist*.

[49] "Recognition of the Soviet Union, 1933," in *Milestones in the History of U.S. Foreign Relations: 1921–1936* (Department of State Office of the Historian, 2009), https://history.state.gov/milestones/1921-1936/ussr; Richard Gribble, "United States Recognition of Soviet Russia: 1917–1933—Church and State Responses," *American Catholic Studies* 119, no. 4 (December 1, 2008): 21–51.

[50] "Recognition of the Soviet Union, 1933."

[51] Director of Intelligence, *The Soviets in India: Moscow's Major Penetration Program," Intelligence Assessment* (Washington, DC: Central Intelligence Agency, 1985), https://www.cia.gov/library/readingroom/docs/CIA-RDP86T00586R000400490007-7.pdf.

[52] Christopher M. Andrew and Vasili N. Mitrokhin, *The World Was Going Our Way: The KGB and the Battle for the Third World* (New York: Basic Books, 2005), 324.

[53] Conquest, *Harvest of Sorrow*, 39.

example, the communist press—and then encouraged journalists at English-language publications to pen their own articles using these planted articles as sources. In the other method, the Soviets placed their articles directly into Indian press and wire services whose managers they had bribed and then used these services' bylines to add cover and legitimacy.

Such operations undoubtedly served to influence domestic Indian public perceptions, yet they carried another key benefit with even greater value for the Kremlin. These tactics gave the Soviets the ability to publish rumors, insinuation, and disinformation under respected Indian newspaper mastheads and then cite them as "neutral" international sources in disinformation campaigns throughout the globe.[54] By cloaking their damaging rumors and disinformation in the credibility of neutral foreign press, the Soviets could appear to merely amplify objective information, and thus infect Western audiences that had long since learned not to trust any accusations originating directly from Moscow. In one notable instance, a 1968 hoax—alleging that the U.S. military had been spreading weaponized epidemics in Vietnam and Thailand—was introduced by the Mumbai-based *Free Press Journal* and amplified in a weekly publication called *Blitz*.[55] This fabrication—fake news before the age of fake news—was based on a forged U.S. Office of Naval Research letter produced by the KGB active measures division known as "Service A" and gained enough traction and credibility from its coverage in the Indian press to achieve republication in the London *Times*.[56] Popular acceptance of this slanderous fabrication fueled anti-U.S. military sentiment that may still linger to this day, as persistent rumors

[54] Director of Intelligence, "The Soviets in India"; Nicholas J. Cull et al., *Soviet Subversion, Disinformation and Propaganda: How the West Fought against It: An Analytic History, with Lessons for the Present* (London: London School of Economics and Political Science, 2017), 22, 33–36, https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf.

[55] Max Holland, "The Propagation and Power of Communist Security Services Dezinformatsiya," *International Journal of Intelligence and CounterIntelligence* 19, no. 1 (January 1, 2006): 12, https://doi.org/10.1080/08850600500332342; Andrew and Mitrokhin, *The World Was Going Our Way*, 318.

[56] Holland, 12; Department of State, *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–1987* (Washington, DC: Department of State, 1987), Proquest.

Page 3102 of 3957

about U.S. military use of biological weapons may well have roots in stories based on Soviet sources.[57]

As shown in the alleged coercion or bribery of Walter Duranty, a key component of Soviet disinformation efforts was the courting and financing of Western journalists to promote a Kremlin-approved counter-narrative. Allegations and proven cases of such attempts throughout the Cold War abound, with the case of French journalist Pierre-Charles Pathé standing out as one of the most high-profile instances.[58] French officials observed Pathé, regarded as an expert on Soviet affairs by prominent French media outlets, in 1978 conducting a clandestine meeting with a KGB agent, when he was given money and documents instructing him on points and themes he was expected to publish under his own name.[59] Upon his subsequent trial and conviction, it became known that he had spent 20 years in the service of the KGB disinformation campaign and published articles under pseudonyms as well as in his own name. His Soviet-financed publications included a journal called *Centre d'Information Scientifique, Economique et Politique* and a newsletter called *Synthesis,* described as highly influential to the French political elite.[60] An analysis of the majority of *Synthesis* editions by Godson and Shultz revealed, along with multiple articles attempting to pin the assassination of President John F. Kennedy on the Federal Bureau of Investigation (FBI), several key themes amplifying Soviet positions, including:

> fostering mistrust among the NATO allies and their friends, denigrating Western weaponry and defense policies, criticizing French policy vis-à-vis American and NATO political and defense arrangements, and expressing distrust of and censuring the United States.[61]

---

[57] Holland, "Propagation and Power of Dezinformatsiya," 13.

[58] Sean M. Dixon, "Finding the Limit: The Strategic Potential of the Network-Based Actor" (master's thesis, Naval Postgraduate School, 2016), 10–13.

[59] Christopher M. Andrew and Vasili N. Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 2000), 471; Arnaud de Borchgrave, "The KGB's Bead on the Media," *Washington Post*, April 14, 1981, https://www.washingtonpost.com/archive/politics/1981/04/14/the-kgbs-bead-on-the-media/a58625f1-6959-470b-8afe-15ed92949304/.

[60] Shultz and Godson, *Dezinformatsia*, 134.

[61] Shultz and Godson, 136.

Page 3103 of 3957

The Kremlin had evidently cultivated Pathé's reputation as an expert on Soviet affairs in part by feeding him information and funding, and in part, by exploiting his status as the son of a prominent French filmmaker.[62] Once his credibility and bona fides were thus established, the subsequent propaganda and false information published under his name carried an air of legitimacy in the Western world far greater than the Soviets were able to achieve through their dissemination of overt propaganda.

2. Secret Proxy Organizations

Another early method of interference in domestic American affairs was Soviet support for such foreign communist organizations as the Communist Party of the United States of America (CPUSA). As shown by its own records (retrieved from Russia by emissaries from the U.S. Library of Congress after the fall of the Soviet Union), the CPUSA worked with its Kremlin financiers to exploit disaffected or oppressed segments of the U.S. population as early as the 1920s.[63] Such targeting included farm workers hit hard by the Great Depression and Black citizens suffering under oppressive Jim Crow discrimination. These efforts netted such victories as the recruitment of popular African American actor, singer, and sportsman Paul Robeson to promote, amid much contemporary controversy, the Soviet cause as superior to the oppressive U.S. government.[64] In the CPUSA and other ostensibly domestic organizations, the Kremlin cultivated valuable covert means to recruit spies, allies, and unwitting assistants, and to manipulate and exacerbate U.S. social unrest in support of its interference objectives.[65]

---

[62] Pathé's father Charles was a famous, successful businessman known for popularizing phonograph records and essentially pioneering the film industry in early 20th century France, and he invented many popular techniques and tropes along the way. The media production and distribution conglomerate he created, Pathé Frères, has remained in operation since 1896. Shultz and Godson, 135.

[63] Deb Riechmann, "Retrieved Papers Shed Light on Communist Activities in U.S.," *The Billings Gazette*, January 30, 2001, http://billingsgazette.com/news/world/retrieved-papers-shed-light-on-communist-activities-in-u-s/article_bd5e5ca5-38b7-5dcd-b645-b203cbaa0445.html.

[64] Scott Martelle, *The Fear within: Spies, Commies, and American Democracy on Trial* (New Brunswick: Rutgers University Press, 2011), 193–196, Proquest.

[65] Notably, the CPUSA has long outlived its Soviet benefactor. Though it has not formally fielded a presidential ticket since activist Angela Davis shared the ticket with CPUSA leader Gus Hall in 1984, the party proudly claimed elected city council representatives in Wisconsin and Pennsylvania as of 2020.

Page 3104 of 3957

After anti-communist sentiment in the United States began to crest at the onset of the Cold War, the Soviets made extensive use of international and multinational front organizations; many of them ostensibly dedicated to such laudable causes as disarmament or world peace.[66] This more subtle approach enabled the KGB to recruit potential sympathizers and unwitting allies who not only worked intentionally or directly to aid the Kremlin, but also gave the Soviet Union Trojan Horse-like propaganda dissemination and information gathering outlets within countries where overt Soviet influence would not be tolerated.[67] Perhaps the best known of these organizations is the World Peace Council (WPC), founded in 1950.[68] Along with such partners as the World Federation of Trade Unions and the dubiously named World Federation of Democratic Youth, the WPC led protests throughout Western democratic nations for several decades and published materials intended to generate mass anger against U.S. weapons development.[69] Specifically, these organizations produced inflammatory and spurious literature falsely accusing the United States of such crimes as conducting biological warfare in the Korean War.[70] These organizations were later used to foment domestic and international outrage against U.S. activity in the Vietnam War, followed by a sustained campaign to discredit and split or dissolve NATO including hosting an annual "Stockholm Conference on Vietnam" and supporting "anti–neutron-bomb" protests in European NATO member states.[71] Perhaps tipping their hand, these organizations nearly unanimously ignored the Soviet military buildup and such Soviet-dominated alliances as the Warsaw Pact. When they had to acknowledge them, these organizations defended them as Soviets' "alliances,"

---

[66] William Styles, "The World Federation of Scientific Workers, A Case Study of a Soviet Front Organisation: 1946–1964," *Intelligence and National Security* 33, no. 1 (January 2, 2018): 116–29, https://doi.org/10.1080/02684527.2017.1323479; Shultz and Godson, *Dezinformatsia*, 112–131.

[67] Andrew and Mitrokhin, *The Sword and the Shield*, 427; Shultz and Godson, *Dezinformatsia*, 112.

[68] Andrew and Mitrokhin, *The World Was Going Our Way*, 324; Shultz and Godson, 112–131; Andrew and Mitrokhin, 427.

[69] Shultz and Godson, 112–131.

[70] World Council of Peace, *World Peace Movement: Resolutions and Documents* (Vienna, Austria: Secretariat of the World Council of Peace, 1955), 102–103; Shultz and Godson, *Dezinformatsia*, 123.

[71] Shultz and Godson, 125–127.

Page 3105 of 3957

as well as being a necessary defensive posture, even as they called for U.S. disarmament in the interest of global peace.[72]

3. Forgeries and Rumors

Yet another method used by the Soviet Union to sway popular opinion and breed mistrust of the U.S. government among U.S. and allied citizens was through the creation and planting of forged documents and letters.[73] Soviet-made materials with meticulously mimicked Western handwriting, syntax, and signatures were disseminated both by Soviet-compromised publications, and by neutral or anti-Soviet publications duped by the fabrications; for example, the 1968 Office of Naval Research epidemic weapon forgery carried by the Indian press.[74] Contentious and painful social issues within U.S. society, such as the civil rights struggle, a rash of high-profile assassinations, and heated arguments about the U.S. military's role in the Vietnam War, were popular targets for forgery and slander attacks. Manipulation of the press to introduce or reproduce the KGB-generated allegations and false documents played a key role in helping rumors, doubt, and lies to spread throughout U.S. society.

According to Mitrokhin, the KGB launched a campaign to reduce the influence of nonviolent civil rights champion Martin Luther King, Jr. in favor of Stokely Carmichael, whom the Soviet Union saw as more radical and likely to incite violence and division.[75] KGB leaders authorized implantation of articles in English-language newspapers in African countries slandering King, ostensibly written by Black opponents of his ministry and movement.[76] Hoping these articles would be reprinted in U.S. newspapers, Soviet authors used such incendiary Western racial terms as "Uncle Tom" to describe King, and produced forged documents indicating that he was a paid mole injected into the movement

---

[72] Shultz and Godson, 126.

[73] Bureau of Public Affairs, *Soviet 'Active Measures' Forgery, Disinformation, Political Operations* (Washington, DC: Department of State, 1981), https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf; Shultz and Godson, *Dezinformatsia*, 151–157; Andrew and Mitrokhin, *The World Was Going Our Way*, 318; Andrew and Mitrokhin, *The Sword and the Shield*, 245.

[74] Bureau of Public Affairs; Shultz and Godson, *Dezinformatsia*, 151–157.

[75] Andrew and Mitrokhin, *The Sword and the Shield*, 237.

[76] Andrew and Mitrokhin, 238.

Page 3106 of 3957

by the Johnson administration.[77] When King's assassination the following year led to nationwide unrest and riots, the disinformation department quickly reversed course and began using its press operations to hail King as a martyr whose murder traced back to U.S. government attempts to silence him.[78]

Concurrently, the Mitrokhin archive chronicles KGB financing and assistance to publishers and authors responsible for advancing conspiracy theories that the CIA orchestrated the 1963 assassinations of Kennedy and his killer, Lee Harvey Oswald.[79] In hopes of capitalizing on popular mistrust created by President Richard Nixon's career-ending Watergate scandal a decade later, the disinformation department also created and circulated a forged request for information—ostensibly from Oswald—to disgraced Watergate operative and former CIA agent E. Howard Hunt, in an effort to further imply that the CIA was behind Kennedy's murder.[80] Though the KGB's clumsy use of initials in this forgery led some readers to conclude erroneously that a right-wing oil magnate with the same surname was its ostensible recipient, the letter's subsequent publishing and "verification" by multiple handwriting experts helped accomplish the main goal of convincing some Americans that CIA operatives had killed the President.[81]

Similar forgery efforts sought to frame FBI chief J. Edgar Hoover on a variety of fronts, including that he was alternately a right-wing extremist, a corrupt abuser of the FBI office, and even a secret transvestite bent on seeding the FBI with fellow homosexual activists.[82] Though some of the more outlandish insinuations against Hoover may have failed to gain mainstream credibility initially, such allegations as unproven speculation regarding Hoover's sexual preferences gained widespread acceptance within U.S. society

---

[77] Andrew and Mitrokhin, 237.

[78] Andrew and Mitrokhin, 238. Note: Mitrokhin's original files in Cyrillic are only available for viewing at the Churchill College in Cambridge, England. Manipulation regarding Dr. King can be found in *The Papers of Vasiliy Mitrokin*, volume 6, chapter 14, part 2.

[79] Andrew and Mitrokhin, 225–229.

[80] Holland, "Propagation and Power of Dezinformatsiya," 18; Andrew and Mitrokhin, 228–229.

[81] "Lawyer Says Texan Told Him Oswald Had Aid in '63 Plot," *New York Times*, sec. Archives, April 3, 1977, https://www.nytimes.com/1977/04/03/archives/lawyer-says-texan-told-him-oswald-had-aid-in-63-plot.html; Andrew and Mitrokhin, 228–229.

[82] Andrew and Mitrokhin, 235.

Page 3107 of 3957

and have continued to resurface for decades.[83] The lack of definitive evidence regarding aspects of Hoover's personal life makes it difficult to ascertain for certain whether Soviet operatives invented such stories or simply used its disinformation techniques to capitalize on existing rumors or even facts. Regardless, such techniques amplified public awareness of controversial Hoover rumors at the very least, and demonstrate that Kremlin interference efforts included both disinformation and amplification of legitimate information it felt was advantageous yet getting insufficient attention organically.

4. Manipulating Multiple Sides, Instigating Groups against Each Other, and Inciting Violence

In some cases, Kremlin subversive measures sought to create kinetic impact and create physical casualties. Evidence of such attempts highlights the multi-faceted nature of Soviet interference techniques and the multilateral danger to U.S. interests presented therein. For example, Mitrokhin's smuggled KGB archive details a diabolical plot to exacerbate racial tensions in the 1960s, seeking not just to provoke conflicts and arguments or influence political narratives but actually to incite violence within U.S. society. One of the most alarming examples is a 1971 plot, codenamed "Operation Pandora," to detonate an explosive device at a predominantly Black college in New York and anonymously call several Black organizations attributing the explosion to the Jewish Defense League (JDL).[84] Mitrokhin's notes indicate that this idea was not an isolated one but rather one element of an elaborate campaign to incite a deadly race war between Jewish and African-American communities. To accomplish this plot, the Soviets produced insulting racist material made to look like it was written by the JDL and distributed the letters to militant black power groups. Along with these forgeries, the Soviets sent anonymous letters to African-American organizations listing made-up atrocities against the Black community committed by the JDL, and calling Black citizens to retaliate violently against the league's leadership. Whether such plots were designed to harm the future electoral prospects of presidents Lyndon Johnson or Nixon, tarnish the U.S. reputation internationally, or simply

[83] Andrew and Mitrokhin, 236.

[84] Andrew and Mitrokhin, 238.

Page 3108 of 3957

to cause ongoing division or chaos as a more general goal is unclear, but each is plausible in the context of concurrent Soviet disinformation schemes. Whatever the aim, attempts to create tangible impacts and casualties added a dangerous new dimension to Soviet interference operations beyond propaganda, bribes, and disinformation.

5. Diminishing Returns, Lasting Impacts

Moscow's various strategies in its interference campaigns during the Cold War demonstrate the breadth and adaptability of its subversive influence arsenal, but such diversity may have been born of necessity or pragmatism as some of its most successful tools began to lose power with repeat usage. Most of the Soviet active measures and disinformation tactics achieved varying levels of success over the course of the Cold War, but many waned in effectiveness as targets began to identify them or at least grow reasonably suspicious. For example, Western observers eventually caught on to the robust forgery operations, and occasionally managed to undermine their effectiveness by shining a light on the practice. One such failed operation was a KGB attempt to deflect blame for a 1981 assassination attempt against Pope John Paul II away from itself and onto the CIA. In this incident, two forgeries purported to be cables from the U.S. embassy in Rome were published by a communist-friendly Italian newspaper, but quickly discredited due to formatting errors and correctly labeled a "Soviet active measure" by other Italian newspapers.[85] Another diabolical yet ineffective operation involved sending forged letters purportedly from the Ku Klux Klan to African and Asian nations ahead of the 1984 Summer Olympic Games in Los Angeles warning that Black athletes would be shot, burned, or lynched if they attempted to compete.[86] Such apparent misfires do not indicate a broader failure of Soviet influence operations, however. To the contrary, the presence of seemingly unsuccessful attempts amid a series of successes merely indicates that the Kremlin's subversion strategy involves placing a large number of low-risk bets, or lighting

[85] Dennis Kux, "Soviet Active Measures and Disinformation: Overview and Assessment," *Parameters, Journal of the U.S. Army War College* 15, no. 4 (December 1, 1985): 24–25; "Two Diplomatic Cables Called KGB Forgeries," United Press International, July 14, 1983, https://www.upi.com/Archives/1983/07/14/Two-diplomatic-cables-called-KGB-forgeries/2457427003200/.

[86] Andrew and Mitrokhin, *The Sword and the Shield*, 238.

a series of small flames to see which ones ignite into destructive fires. It is also notable that some attempts, such as the Kennedy assassination forgery project, lay dormant for years before eventually bearing fruit and enduring for decades.

Despite growing Western awareness of Soviet dezinformatsiya and U.S. efforts to challenge it aggressively under Ronald Reagan's administration, many active measures plots continued to achieve some degree of success, even during the tentative thaw in U.S.-Russia relations, and even after being positively identified as disinformation. In 1983, the KGB published a fake letter in *Patriot*, an Indian newspaper formed two decades earlier with Soviet aid for the purpose of seeding disinformation.[87] The letter, ostensibly from an American scientist who wished to remain anonymous, claimed that the burgeoning human immunodeficiency virus/acquired immunodeficiency syndrome (HIV/AIDS) virus had been developed by the Pentagon as a biological-weapons experiment.[88] After the letter initially failed to gain international attention, a spurious scientific paper crafted by Kremlin loyalists in East Germany was issued to bolster it, with Soviet press deliberately misidentifying the paper's origin as French to further obscure the Kremlin connection.[89] While other Soviet proxies around the world spread stories related to and building on the Pentagon/AIDS myth, traditional Soviet media in turn amplified them, and by 1987, the story had been shared in more than 30 languages and 80 countries.[90] More than 35 years since the Soviet Union set out to convince the world that the U.S. government had created the AIDS virus, and more than 25 years after the KGB admitted the entire ploy, U.S. and global public health officials and medical workers continue to struggle against popular

[87] Thomas Boghardt, "Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence* 53, no. 4 (December 1, 2009): 4–7.

[88] Department of State, *Soviet Influence Activities*.

[89] Department of State; Andrew and Mitrokhin, the *Sword and the Shield*, 244–245.

[90] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *Institute for National Strategic Studies: Strategic Perspectives*, no. 11 (June 1, 2012): 155.

acceptance of the fabrication and the knock-on consequences of it.[91] For example, a 2005 study revealed that more than one out of every four African-Americans surveyed believed that AIDS was produced in a government laboratory, and that more than 15 percent of respondents believed the government had created the virus to control or reduce the Black population.[92] As demonstrated by political controversy that jeopardized mass acceptance of a potential COVID-19 vaccine among U.S. citizens during a global pandemic in 2020, conspiracies that undermine the credibility of government administration of health resources, or frame the government for disease outbreaks, can have significant and durable negative political and public health impacts.[93]

B. CONTEMPORARY ADAPTATIONS AND NEW THREATS

Russian active measures and disinformation against the West did not end with the demise of the Cold War. Indeed, modern Russian influence campaign methods build on Soviet active measures and exploit new technology that appears to increase their effectiveness. This section borrows the framework of the previous section to demonstrate how recent Kremlin interference operatives have adopted and adapted the techniques of their forebears, and to highlight areas in which such tools may be even more potent today.

1. Media Manipulation

Sinikukka Saari noted in 2011 that Russia's "active measures" influence strategies were evolving to include:

---

[91] Jacob Heller, "Rumors and Realities: Making Sense of HIV/AIDS Conspiracy Narratives and Contemporary Legends," *American Journal of Public Health* 105, no. 1 (November 13, 2014): e43–e50, https://doi.org/10.2105/AJPH.2014.302284; David Robert Grimes, "Russian Fake News Is Not New: Soviet AIDS Propaganda Cost Countless Lives," *The Guardian*, sec. Science, June 14, 2017, https://www.theguardian.com/science/blog/2017/jun/14/russian-fake-news-is-not-new-soviet-aids-propaganda-cost-countless-lives.

[92] Laura M. Bogart and Sheryl Thorburn, "Are HIV/AIDS Conspiracy Beliefs a Barrier to HIV Prevention among African Americans?," *JAIDS Journal of Acquired Immune Deficiency Syndromes* 38, no. 2 (February 1, 2005): 213–218.

[93] Sarah Kreps et al., "Factors Associated with U.S. Adults' Likelihood of Accepting COVID-19 Vaccination," *Journal of the American Medical Association Network Open* 3, no. 10 (October 20, 2020), https://doi.org/10.1001/jamanetworkopen.2020.25594; Jonathan Chait, "Trump Determined to Get Vaccine before Election, Overrules FDA Guidelines," *New York Magazine: Intelligencer*, October 5, 2020, https://nymag.com/intelligencer/2020/10/trump-vaccine-overrules-fda-election-coronavirus-science.html.

> 1) Proactive political involvement, e.g. creating links to a variety of political actors, assisting reorganisation and coordination of pro-Russian parties, export of political technologies and consultation around elections, 2) 'NGO diplomacy' e.g. creating and assisting pro-Russian youth groups, minority and separatist civil organisations and think tanks, [and] 3) Creation and management of favourable media environment, e.g. the establishment of Russian media ventures, launching media campaigns in the Russian media, or influencing the local national media.[94]

To Saari's last point, modern Russian media ventures have been used as an integral tool in its interference campaigns against Western democracies, overtly operating within the states it seeks to influence.

Since 2005, the Russian government has operated and expanded its own international media outlets, for example the television and online video enterprise RT (originally called Russia Today) and the internet-based news and commentary agency Sputnik. Both widely regarded by Western intelligence sources as mouthpieces of official Kremlin propaganda, these outlets have established multi-language ventures throughout the world and used a range of marketing strategies to build a substantial public audience. RT, Sputnik, and other government-sponsored Russian outlets with an international outreach mission provide factual coverage and interesting content on a variety of topics, yet they also clearly support agendas and messages that the Kremlin wishes to spread.[95] These outlets amplify news and opinions Russia wishes to promote, whitewash or cast doubt on the veracity of negative stories involving Russian interests, promote conspiratorial theories and interpretations, and give remarkably high amounts of coverage and airtime to representatives of political groups and parties seen as controversial or "fringe."[96] Opinions Russia wishes to promote with its news broadcast networks include

---

[94] Sinikukka Saari, "Putin's Eurasian Union Initiative: Are the Premises of Russia's Post-Soviet Policy Changing?," *Swedish Institute of International Affairs UI Brief*, no. 9 (November 1, 2011): 4, https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/putins-eurasian-union-initiative-are-the-premises-of-russias-post-soviet-policy-changing-min.pdf.

[95] Galina Miazhevich, "Nation Branding in the Post-Broadcast Era: The Case of RT," *European Journal of Cultural Studies* 21, no. 5 (October 1, 2018): 575–93, https://doi.org/10.1177/1367549417751228; Steven Erlanger, "Russia's RT Network: Is It More BBC or KGB?," *New York Times*, sec. World, March 8, 2017, https://www.nytimes.com/2017/03/08/world/europe/russias-rt-network-is-it-more-bbc-or-kgb.html.

[96] "Shadow Puppets: Russian Meddling in Europe," *The Economist*, April 15, 2017.

denigration of NATO and defense of Russia's 2014 annexation of Ukraine's Crimean peninsula.[97] Examples of conspiracy promotion include attempts to portray the shootdown of Malaysian Airlines Flight MH17, said to be done accidentally by Kremlin proxies in occupied east Ukraine with a Russian anti-aircraft missile, and GRU agents' alleged poisoning of a former Russian spy in Great Britain, as deliberate acts perpetrated by rivals scheming to frame and slander Moscow.[98]

At times, Russian officials have openly acknowledged these media outlets' purpose as a powerful tool or even weapon against the Western world. In explaining the importance of RT's American TV channel in 2011, editor-in-chief Margarita Simonyan appeared to hint at the network's role as a strategic defense weapon:

> It's important that there is a channel that people are used to, that they like, so then when you need to, you show them what you need to show them. In a sense, not having your own "inoveshaniye" [foreign broadcasting] is the same as not having a ministry of defense. When there is no war, it seems as though it is not necessary. But damn, when there is war, it's absolutely critical. But you can't create an army a week before the war begins.[99]

In a satellite video appearance with the president of Argentina commemorating the beginning of RT's Spanish-language broadcasting in South America in 2014, Putin himself stated, "With accelerated development of electronic media, this sphere has acquired immense importance and has perhaps become a formidable weapon to potentially manipulate public consciousness."[100]

---

[97] Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies* 40, no. 6 (September 19, 2017): 779–799, https://doi.org/10.1080/01402390.2016.1273830.

[98] Gordon Ramsay and Sam Robertshaw, *Weaponising News: RT, Sputnik and Targeted Disinformation* (London, England: King's College, 2019), 21–44, https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf; Adam Holland, "RT "Covers" the Shooting down of MH17," July 18, 2014, *The Interpreter*, https://www.interpretermag.com/rt-covers-the-shooting-down-of-mh17/.

[99] "Russkiye Media Iznutri: Margarita Simonyan, Glavny Redaktor Russia Today [Russian Media from within: Margarita Simonyan, Editor-in-Chief of Russia Today]" Afisha [Poster], October 18, 2011, https://daily.afisha.ru/archive/gorod/archive/ministry-of-truth-simonyan/. NOTE: The text as it appears in the thesis is the author's personal translation from the original Russian.

[100] Vladimir Putin, "Telekanal Russia Today nachal veshchaniye v Argentine [Russia Today TV channel began broadcast in Argentina]," Prezident Rossii [Office of the President of Russia], October 9, 2014, http://kremlin.ru/events/president/news/46762.

Page 3113 of 3957

It is no surprise, then, that an interagency report on Russian interference published in 2017 by the Director of National Intelligence concluded that RT and Sputnik are key components of "Russia's state-run propaganda machine" and a vital tool in its foreign influence campaigns.[101]

According to a 2019 study from King's College London analyzing all English-language content produced by RT and Sputnik during two four-week periods in 2017 and 2018, the Kremlin news agencies flooded the market with more than 2,100 articles highlighting political dysfunction in Western countries and Ukraine, which represented 81.7 percent of all content the agencies wrote about these nations.[102] Of the March 2018 RT and Sputnik articles studied, a staggering 138 of them sought to sow confusion and doubt about the Kremlin's recent poisoning of a former spy in the United Kingdom, in many cases by offering competing and contradictory counternarratives, such as lies that the U.S. or British government created the Novichok poison used in the attack.[103] Such misdirection and noise are hallmarks of RT and Sputnik's defense of Kremlin scandals, particularly regarding infamous large-scale incidents such as the Russian military's seizure of the Crimea peninsula and the downing of Malaysian Airlines Flight MH17.[104] The anti-Ukrainian rhetoric and dishonesty coming from Russia's English-language RT channels in London and the United States during these two events were so prolific and reprehensible that two of its anchors publicly resigned out of frustration with the network's deceptive

[101] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections* (Washington, DC: Office of the Director of National Intelligence, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[102] Ramsay and Robertshaw, *Weaponising News*, 73.

[103] Ramsay and Robertshaw, 44.

[104] "MH17 Crash, 17 July 2014," Dutch Safety Board, October 13, 2015, https://www.onderzoeksraad.nl/en/page/3546/crash-mh17-17-july-2014.

Page 3114 of 3957

reporting, while a third forcefully condemned the network's disinformation campaign on air during a live broadcast.[105]

Disturbingly, the King's College report also discovered that RT and Sputnik's English-language content infected British news sources as well; 21 different articles across five prominent British newspapers in an eight-week sample replicated at least 30 percent of the text found in articles that RT or Sputnik had published previously, including 11 directly related to political issues.[106] Only two of the 21 articles gave credit or attribution to the earlier RT or Sputnik articles, meaning British audiences had no reason to suspect a Kremlin-friendly bias. Taken alongside other studies' findings, for example a report that conspiracy-minded U.S. media outlet InfoWars had republished more than 1,000 RT articles, it appears that the old Soviet method of publishing stories with the hope that Western media outlets would later amplify their messages is now more successful than ever.[107]

Government-run propagandistic media outlets represent only the tip of the iceberg of Russia's modern-day foreign influence apparatus, however. Beneath the surface, the Kremlin also appears to continue employing such practices as co-opting journalists and covertly manipulating the foreign press, playing puppet master to proxy organizations designed to stir up social divisions, fabricating and spreading false information, and providing material and financial support to foreign political candidates and campaigns.[108]

---

[105] Elizabeth Wahl, "I Was Putin's Pawn," *Politico Magazine*, March 21, 2014, https://www.politico.com/magazine/story/2014/03/liz-wahl-quit-russia-today-putins-pawn-104888.html; John Plunkett, "Russia Today Reporter Resigns in Protest at MH17 Coverage," *The Guardian*, sec. Media, July 18, 2014, http://www.theguardian.com/media/2014/jul/18/mh17-russia-today-reporter-resigns-sara-firth-kremlin-malaysia; Antonia Paget, "Russia Today Host Condemns Ukraine 'Occupation," *The Times*, March 4, 2014, https://www.thetimes.co.uk/article/russia-today-host-condemns-ukraine-occupation-rgmqv036jcj.

[106] Ramsay and Robertshaw, *Weaponising News*, 85.

[107] Jane Lytvynenko, "InfoWars Has Republished More than 1,000 Articles from RT without Permission," BuzzFeed News, November 8, 2017, https://www.buzzfeednews.com/article/janelytvynenko/infowars-is-running-rt-content.

[108] Anton Shekhovtsov, *Russia and the Western Far Right: Tango Noir* (Abingdon, United Kingdom: Routledge, 2017), 2181–2768 of 9823, Kindle.

a. Co-opting Journalists and Using Outside Media to Influence News Coverage

Echoing past Soviet use of Indian, East German, and African publications to hide its authorship of disinformation, the internet is awash with obscure and low-level news portals throughout the world that fail to disclose the editorial control or influence of the Kremlin. In particular, the FSB and Russia's Main Intelligence Directorate of the Russian General Staff (GRU), work with loyal supporters to enact this scheme.[109] Hungarian news media website Hídfő.net, whose content was eventually found to have been almost entirely produced by Russia's GRU, was used to dramatic effect in a Kremlin campaign to turn Ukraine's neighbors against its fledgling post-revolutionary government.[110] The site caused a massive uproar by falsely reporting that Hungarian tanks had been seen rolling across the Ukrainian border.[111] The site also published false assertions regarding such topics as Crimea-related sanctions, the 2016 U.S. presidential election, NATO aggression, and an "exposé" alleging a U.S.-run hybrid war campaign against its rivals.[112] As in Soviet times, the site's articles could be cited by the Russian media as though it were a credible foreign news source, without the stories appearing to be state-generated propaganda.

b. Inventing and Planting Stories in the Internet Age

As the hidfo.net incident illustrates, the Kremlin is able to leverage such significant technological advances as the internet to enhance the efficiency and expand the reach of Soviet disinformation tools. In a hyper-connected digital age in which much of the world receives information from sources outside traditional news networks, Russia is now able to accomplish its goals of spreading disinformation without needing to explicitly

---

[109] Andrew Higgins, "Intent on Unsettling E.U., Russia Taps Foot Soldiers from the Fringe," *New York Times*, sec. Europe, December 24, 2016, https://www.nytimes.com/2016/12/24/world/europe/intent-on-unsettling-eu-russia-taps-foot-soldiers-from-the-fringe.html; Dezső Szabolcs and Panyi András, "Russian Diplomats Exercised with Hungarian Cop Killer's Far-Right Gang," Index, October 28, 2016, http://index.hu/belfold/2016/10/28/russian_diplomats_exercised_with_hungarian_cop_killer_s_far-right_gang/

[110] Szabolcs and András.

[111] Szabolcs and András.

[112] At the time of this thesis' publication, Hidfo.net links automatically redirect to SputnikNews.com, an English-language arm of the Russian state-owned news agency, and are thus not cited directly.

Page 3116 of 3957

compromise or exploit journalists or news publications, nor even to create its own Western-leaning information portals. The advent of social media, in particular, has helped modern Russian influence campaigns reach an exponentially wider audience than Soviet operations were able to, and with considerably less difficulty and risk.

Since at least 2013, active measures harnessing the power of the internet and social media to stoke artificial public interest in a topic, spread disinformation, and attack Russia's foes have proliferated.[113] *Novaya Gazeta*, a Moscow newspaper whose critical investigative work since Putin rose to power is believed to have prompted the assassination of several of its prominent employees, reported in August 2013 that its journalists had infiltrated a St. Petersburg "troll factory" called Internet Research Agency (IRA).[114] The IRA offered weekly salaries and free food to employees for writing blogs, article comments, and social media posts on prescribed themes.[115] According to this exposé, young Russian citizens working for the agency were given a list of topics and targets about which to produce content across Russian and Western traditional and social media.[116] These topics included praise for Putin, the Group of Twenty (G20) summit (held in St. Petersburg that year), and Russian activity in the Syrian war, along with negative content directed at Russian opposition politician Aleksei Navalny, *Forbes* magazine, and various American entities. Burnished by other media reports corroborating these findings, the *Novaya Gazeta* investigation discovered that similar operations were planned for or already working in Moscow, and also found evidence that the agency's influence campaign

[113] Casey Michel, "America's Neo-Nazis Don't Look to Germany for Inspiration. They Look to Russia," *Washington Post*, August 22, 2017, https://www.washingtonpost.com/news/democracy-post/wp/2017/08/22/americas-neo-nazis-dont-look-to-germany-for-inspiration-they-look-to-russia/.

[114] Tony Halpin, "Journalists from Novaya Gazeta Are 'Assassination Targets,'" *The Times*, January 23, 2009, https://www.thetimes.co.uk/article/journalists-from-novaya-gazeta-are-assassination-targets-cjbv5nzp2sg; Aleksandra Garmazhapova, "Gdye zhivut trolli. Kak rabotayut internet-provokatory v Sankt-Peterburge i kto Imi zapravlyayet [Where the trolls live: How internet provocateurs work in St. Petersburg and who leads them]," Novaya Gazeta [New Gazette], August 9, 2013, https://www.novayagazeta.ru/articles/2013/09/09/56265-gde-zhivut-trolli-kak-rabotayut-internet-provokatory-v-sankt-peterburge-i-kto-imi-zapravlyaet.

[115] Garmazhapova.

[116] Garmazhapova.

predated its July 2013 business registration.[117] Subscribers to British newspaper *The Guardian* complained that the online comment section of articles related to Ukraine's ongoing revolution were all so inundated by a torrent of Kremlin-friendly propaganda that legitimate conversation was impossible.[118] A May 2014 column filed by *The Guardian*'s readers' editor in response recalled that the newspaper had reported two years earlier about Russian troll influence campaigns, implying that it had subsequently become a target of such attacks.[119] Indeed, a February 2012 *Guardian* report about hacked emails to and from the leader of a Russian political youth organization, many of which dated back at least to 2010, outlines a well-financed campaign to amplify pro-Russia internet content and smear a list of 168 enemies of the organization, including Navalny, journalists, and human rights activists, on social media and blog sites.[120]

A 2018 RAND Corporation analysis posits that the Kremlin's interest in social media information warfare may have stemmed from Putin believing that such mass unrest incidents as the 2011 Moscow post-election protests and various revolutions in former Soviet republics had been fomented by the United States and coordinated via Facebook and Twitter.[121] These U.S.-based social media platforms were widely reported as critical tools for the launch and coordination of revolutionary uprisings in Egypt and Tunisia that same year, which Putin decried as U.S.-orchestrated interference in his speech justifying

---

[117] Andrey Soshnikov, "Stolitsa politicheskovo trollinga, [Capital of political trolling]" moy rayon [my neighborhood], March 11, 2015, https://mr-7.ru/articles/112478/; Viktor Rezunkov, "Oni lyubyat Putina 12 chasov podryad,[They love Putin 12 hours straight]" Radio Svoboda [Radio Liberty]," March 14, 2015, https://www.svoboda.org/a/26899521.html; Hannah Levintova, "Russian Journalists Just Published a Bombshell Investigation about a Kremlin-Linked "Troll Factory,"" *Mother Jones*, October 18, 2017, https://www.motherjones.com/politics/2017/10/russian-journalists-just-published-a-bombshell-investigation-about-a-kremlin-linked-troll-factory/; Adrian Chen, "The Agency," *New York Times*, sec. Magazine, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[118] Chris Elliot, "The Readers' Editor On… The Pro-Russia Trolls below the Line on Ukraine Stories," *The Guardian*, May 4, 2014, https://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online.

[119] Elliot.

[120] Miriam Elder, "Emails Give Insight into Kremlin Youth Group's Priorities, Means and Concerns," *The Guardian*, February 7, 2012, https://www.theguardian.com/world/2012/feb/07/nashi-emails-insight-kremlin-groups-priorities.

[121] Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND, 2018), 1–15, https://www.rand.org/pubs/research_reports/RR2237.html.

the annexation of Crimea.[122] This perception may have cemented Putin's resolve to build up Russia's so-called "information confrontation" capability to counter what he believed to be a grave new American threat. Though a number of studies later found that the role of social media in the Arab Spring had been somewhat overstated, the 2014 Ukrainian revolution that prompted Putin's seizure of Crimea would have nevertheless proven this hypothesis anyway.[123] The mass demonstrations in Kyiv that year began with a journalist's Facebook post and relied heavily on social media to organize protests, recruit volunteers, and capture the attention of the Western world.[124]

Following *The Guardian*'s report, and increasingly cognizant of robust pro-Russia sentiment within the comment sections of prominent news sites, the American news media gradually began to take notice of the story. News and entertainment aggregator site Buzzfeed published a lengthy exposé in June 2014 that used leaked emails from alleged troll factory financiers to describe the Russian troll operation in great detail.[125] The feature showed the troll factory to be a well-financed and sophisticated operation and revealed attempts to hire English tutors for employees, a list of such media targets as *Politico* and Fox News, and orders for employees to operate six active Facebook accounts or 10 Twitter accounts and post 50 comments to news sites per day. Yet, in response to the Buzzfeed article, a *Washington Post* column highlighting the newspaper's own interaction with suspected Kremlin trolls downplayed the impact of the alleged influence campaign and suggested that domestic commentators were clever enough to mock, refute, or ignore any

---

[122] Taylor Dewey et al., *The Impact of Social Media on Social Unrest in the Arab Spring* (Stanford, CA: Stanford Public Policy Program, 2012), https://publicpolicy.stanford.edu/publications/impact-social-media-social-unrest-arab-spring; Vladimir Putin, "Address by President of the Russian Federation," President Rosiyi [President of Russia], March 18, 2014, http://en.kremlin.ru/events/president/news/20603.

[123] Dewey et al., *Impact of Social Media*, 49; Heather Brown, Emily Guskin, and Amy Mitchell, "Arab-American Media: Bringing News to a Diverse Community: The Role of Social Media in the Arab Uprisings," Pew Research Center, 14–15, November 28, 2012, http://www.journalism.org/2012/11/28/role-social-media-arab-uprisings/.

[124] Brown, Guskin, and Mitchell; Marci Shore, *The Ukrainian Night: An Intimate History of Revolution* (New Haven, CT: Yale University Press, 2018), 1358–1386 of 3050, Kindle.

[125] Max Seddon, "Documents Show How Russia's Troll Army Hit America," Buzzfeed News, June 2, 2014, https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america.

false claims from foreign invaders.[126] Though many outlets reported on the troll campaign as a nuisance offshoot of Russia's adventurism in Crimea, none seemed at the time to recognize it as a threat to U.S. domestic affairs, and neither did prominent U.S. officials.

By April 2015, "malicious cyber activity" was well known and taken seriously enough that President Barack Obama issued Executive Order 13694: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. This order was a directive declaring a national emergency and threatening harsh sanctions on any foreign actors whose cyber activities threatened U.S. national or economic security, financial stability, or foreign policy.[127] Regrettably, in what now seems like a colossal oversight and missed opportunity, the focus around this executive order did not appear to include Russian troll activity. Rather, the text of the executive order centered on such contemporary events as financial cyber crimes, state-sponsored Chinese hacking for the purposes of espionage and intellectual property theft, ISIS propaganda and recruitment through social media, and an incident in which North Korea levied a crippling hacking operation on Sony Pictures in retaliation for its production of a film depicting the assassination of Kim Jong Un.[128] Notably, Obama attempted to correct this oversight in the waning days of his presidency by issuing Executive Order 13757: Taking Additional Steps

---

[126] The *Washington Post* article focused on flagrantly absurd Russian comments, summarizing one thusly: "Halloo, egghead! Let's go! "Oink-oink-oink-oink-oink …" hahaha-haha-ha….)))))))))) [He then launches into an anti-American screed in Russian.]," as well as typical banter, such as a seemingly domestic commentator rapidly responding dismissively to a comment that Obama should avoid involvement with Ukraine-Russia conflict. It did not appear to account for the possibility of more subtle efforts to stir up division without revealing pro-Russian bias. Caitlin Dewey, "Hunting for Paid Russian Trolls in the Washington Post Comments Section," *Washington Post*, June 4, 2014, https://www.washingtonpost.com/news/the-intersect/wp/2014/06/04/hunting-for-paid-russian-trolls-in-the-washington-post-comments-section/.

[127] Barack Obama, Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," Code of Federal Regulations, title 3 (2015), https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[128] Robert Hackett, "Sanctions: America's Best New Weapon against Cyber Crime," *Fortune*, April 2, 2015, http://fortune.com/2015/04/02/us-cyber-crime-sanctions/; David E. Sanger and Katie Benner, "U.S. Accuses North Korea of Plot to Hurt Economy as Spy Is Charged in Sony Hack," *New York Times*, August 6, 2018, https://www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html.

Page 3120 of 3957

to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities to amend Executive Order 13694 after Russia's 2016 election interference.[129]

2. Proxy Organizations

Just as the Soviet Union was able to implant advocates for its causes and policies into foreign states' political and social environments via surrogates such as the CPUSA and WPC, modern Russia offers support and assistance to (and sometimes creates) proxy organizations in the West. This strategy includes support for oft-discounted political parties in other countries, including neo-Nazis and white supremacists.[130] As in the Soviet past, this support and these alliances had nothing to do with shared ideology and everything to do with perceived usefulness to national goals; especially regarding potential collaborators who could assist against a shared enemy. Just as with the leaders of Cuba, North Korea, Vietnam, and such non-communist nations as Egypt and Iraq during Soviet rule, the key question was who was the enemy. The enemy of Moscow's enemy (the West and the United States) was thus the Kremlin's friend.[131]

András Rácz describes Russia's strategy as "scattershot… placing small bets, directly or through proxies, on ready-made fringe groups in an effort to destabilize or simply disorient" such rivals as the EU.[132] An Atlantic Council report titled *The Kremlin's Trojan Horses* agreed and warned that Russia was waging a subtle destabilization effort focused on:

> (1) building political alliances with ideologically friendly political group and individuals, and (2) establishing pro-Russian organizations in civil

---

[129] Barack Obama, Executive Order 13757, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," Code of Federal Regulations, title 3 (2017), https://www.govinfo.gov/content/pkg/FR-2017-01-03/pdf/2016-31922.pdf.

[130] Marlene Laruelle, "Russia's Bedfellowing Policy and the European Far Right," *Russian Analytical Digest*, no. 167 (May 6, 2015): 1–12; Political Capital Institute, *The Russian Connection: The Spread of Pro-Russian Policies on the European Far Right* (Budapest, Hungary: Political Capital Policy Research and Consulting Institute, 2014), 1–9, http://www.riskandforecast.com/useruploads/files/pc_flash_report_russian_connection.pdf.

[131] Robert H. Donaldson, Joseph L. Nogee, and Vidya Nadkarni, *The Foreign Policy of Russia: Changing Systems, Enduring Interests*, 5th ed. (Armonk, New York: M.E. Sharpe, 2014); Andrew and Mitrokhin, *The World Was Going Our Way*.

[132] Higgins, "Intent on Unsettling E.U."

Page 3121 of 3957

> society, which help to legitimate and diffuse the regime's point of view. The web of political networks is hidden and nontransparent by design, making it purposely difficult to expose. Traceable financial links would inevitably make Moscow's enterprise less effective: when ostensibly independent political figures call for closer relations with Russia, the removal of sanctions, or criticize the EU and NATO, it legitimizes the Kremlin's worldview. It is far less effective, from the Kremlin's point of view, to have such statements come from individuals or organizations known to be on the Kremlin's payroll.[133]

The appearance of Russia's support for fringe groups is alarming for a variety of reasons, especially its apparent effect of amplifying far right, ultranationalist, and even neo-Nazi parties and organizations in Slovakia, Austria, France, Germany, Hungary, and other Western nations.[134] Alleged beneficiaries of Russian support include members of European Parliament representing such far-right or nationalist parties as Alternative for Germany and France's National Rally (formerly National Front), as well as such agitator organizations as Austrian Technologies GmbH and Italy's Eurasia Coordination Project.[135] A common thread among the majority of these disparate fringe groups with Kremlin backing has been their assertion that Russia's annexation of Crimea was legitimate and that the sanctions levied as a result of it should be repealed.[136] Another use for this hodgepodge of policy-agnostic alliances also seems to be their members' participation as monitors, neutral observers, or official recognizers of elections in Russia or its intended sphere of influence, where they can dubiously vouch for or cast doubt on the elections' credibility and fairness.[137]

---

[133] Alina Polyakova et al., *The Kremlin's Trojan Horses: Russian Influence in France, Germany, and the United Kingdom*, 3rd ed. (Washington, DC: Atlantic Council, 2016), 4, https://www.atlanticcouncil.org/in-depth-research-reports/report/kremlin-trojan-horses/.

[134] Shekhovtsov, *Russia and the Western Far Right*.

[135] Shekhovtsov, loc. 1196, 4444, 5334, 6473.

[136] For example, members of the Freedom Party of Austria, Italy's Liga Nord, and France's National Front vocally supported, visited, or served as election observers for the referendum in Crimea, and recorded votes against a resolution criticizing the annexation in the European Parliament. Shekhovtsov; Laruelle, "Russia's Bedfellowing Policy."

[137] Shekhovtsov, loc. 4212–4345; Csaba Tóth, "Pro-Russian Jobbik 'Election Observers' Banned from Ukraine," *The Budapest Beacon*, November 4, 2014, https://budapestbeacon.com/pro-russian-jobbik-election-observers-banned-ukraine/.

Page 3122 of 3957

These parties and groups can also be used to cause problems domestically, for example, sowing domestic unrest and stymieing the work of their nations' governments from within using veto power or obstructionism. Even support for less successful fringe parties has a detrimental effect on the nations in which they practice. In October 2016, septuagenarian neo-Nazi Istvan Gyorkos, leader of a small organization known as the Hungarian National Front, murdered a police officer during a raid on his illegal weapons cache in a western Hungarian village.[138] A parliamentary committee later briefed on the incident by the intelligence community was informed that Gyorkos had been under surveillance for years due in part to collaboration with extremists in Russia, and that Russian GRU military intelligence personnel posing as diplomats had regularly engaged in combat drills with him and his followers.[139]

Support for a tiny militant and antagonistic party in Hungary seems duplicitous considering the warm relations already established between the Kremlin and both Hungary's prime minister Viktor Orban, and his leading challenger, the Jobbik Party.[140] Russian support for groups that glorify or co-opt the fascist ideology of the Soviet Union's bitterly hated World War II opponent seems even more jarring. These seeming contradictions, however, underscore the assertion that Russia is willing to place small bets on a plurality of parties, so long as they show signs of being able to weaken the powers that be or disrupt the European status quo. Since such support is pragmatic and sinister rather than ideological, even groups with policies and worldviews antithetical to those of the Russian government may still receive assistance. Such is the case throughout Europe; political parties strongly rumored to have Russian backing in Germany include the left-leaning Social Democratic Party, hard-left Die Linke, and far-right Alternative für

[138] Higgins, "Intent on Unsettling E.U."

[139] Higgins.

[140] Balázs Jarábik, "Putin's Budapest Bargain Is Built on Shaky Ground," Carnegie Endowment for International Peace, August 28, 2017, http://carnegieendowment.org/2017/08/28/putin-s-budapest-bargain-is-built-on-shaky-ground-pub-72939.

Page 3123 of 3957

Deutschland.[141] In Greece, the ruling far-left Syriza party has come under fire due to its rumored Russian financing and ties to such radical Russian nationalists as Alexander Dugin, who is also accused of supporting far-right neo-Nazi opposition party Golden Dawn.[142] The story is similar in Italy, where the resurrected center-right Forza Italia party and right-leaning nationalist Lega Nord parties are both believed to enjoy Russian backing.[143] The United Kingdom's British National Party and UK Independence Party have drawn suspicion on this subject as well due to the effusive praise heaped on Putin by some of their members and the alleged Russian interference in their favor during the Brexit referendum.[144] The evident promiscuity of Russia's foreign political support, even to multiple fringe candidates within a single country, reveals that an aspect of the Kremlin's strategy is to amass a large number of levers to pull in the name of destabilization and ability to impose its will on foreign governments; it is accumulating spoilers and trump cards wherever it can.

Alarm bells about Russian influence sounded in Spain almost immediately upon an explosion of chaos and violence centered on a secessionist movement in Catalonia in September 2017. Citing Catalonian disinformation, Russian media amplification, and Russian Twitter bots' frenzied sharing of both, Spanish media quickly speculated that a

---

[141] One notable instance of Russian support for Germany's Social Democratic Party is its relationship with former German Chancellor and SDP leader Gerhard Schröder. After a setback in Germany's federal election cost him the Chancellorship, he announced his resignation and then controversially signed a deal allowing Russia to build a gas pipeline between the two nations under the Baltic Sea just before his final day in office. Russia, to which the pipeline carried enormous strategic importance, swiftly rewarded Schröder for his assistance by naming him the head of shareholders for the pipeline project and hiring him to a lucrative position as board chairman for the nation's ROSNEFT energy company. Schröder has since served as a reliable defender of controversial Russian actions in the news to include partially rationalizing the Crimea annexation. Polyakova et al., *The Kremlin's Trojan Horses*, 15; "Anger as German Ex-Chancellor Schroeder Heads up Rosneft Board," BBC News, sec. Europe, September 29, 2017, https://www.bbc.com/news/world-europe-41447603.

[142] Courtney Weaver, Kerin Hope, and Sam Jones, "Alarm Bells Ring over Syriza's Russian Links," *Financial Times*, January 28, 2015, https://www.ft.com/content/a87747de-a713-11e4-b6bd-00144feab7de; Peter Foster and Matthew Holehouse, "Russia Accused of Clandestine Funding of European Parties as U.S. Conducts Major Review of Vladimir Putin's Strategy," *The Sunday Telegraph*, January 16, 2016, http://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html.

[143] Max Seddon and James Politi, "Putin's Party Signs Deal with Italy's Far-Right Lega Nord," *Financial Times*, March 6, 2017, https://www.ft.com/content/0d33d22c-0280-11e7-ace0-1ce02ef0def9; Laqueur, *Putinism*.

[144] Polyakova et al., *The Kremlin's Trojan Horses*, 18.

Page 3124 of 3957

Kremlin hand had been stirring the pot.[145] Subsequent reports from German and Spanish intelligence agencies later found that a surge of Russian disinformation and support had indeed been a key provocation for Catalonia's illegal separatist referendum and the bloody riot that followed.[146]

The 2016 Internet Research Agency Facebook advertisements included a series of conservative-targeting posts calling for Texas's secession from the Union; a campaign that all but disappeared after the election but may have intensified had Clinton won.[147] On the other end of the political spectrum, RT reported within one month of Trump's victory that an "embassy" dedicated to California's secession from the United States had been opened in an expensive area of downtown Moscow.[148] Contemporaneous reporting from more credible news outlets revealed that the California secessionist behind this apparent stunt was a New York-born Russophile and Russian resident with a history of right-wing U.S. political activism.[149] It was soon discovered that the dubious diplomatic outpost managed to secure its improbable real estate bonanza only because the space was being provided for free by a Kremlin-financed party that was also supporting a fledgling Texas rebellion.[150]

---

[145] David Alandete, "Russian Meddling Machine Sets Sights on Catalonia," *El País*, September 28, 2017, https://elpais.com/elpais/2017/09/26/inenglish/1506413477_994601.html; "Catalan Referendum Stokes Fears of Russian Influence," Politico Europe, September 29, 2017, https://www.politico.eu/article/russia-catalonia-referendum-fake-news-misinformation/.

[146] Vidya Narayanan et al., *Russian Involvement and Junk News during Brexit*, Computational Propaganda Project (Oxford: University of Oxford, 2017); Graham Keeley, "Russia Meddled in Catalonia Independence Referendum, Says German Intelligence Boss," *The Times*, sec. World, May 15, 2018, https://www.thetimes.co.uk/article/russia-meddled-in-catalonia-vote-p6g5nttpm; Robin Emmott, "Spain Sees Russian Interference in Catalonia Separatist Vote," *Reuters*, November 13, 2017, https://www.reuters.com/article/us-spain-politics-catalonia-russia-idUSKBN1DD20Y.

[147] Tim Lister and Clare Sebastian, "Stoking Islamophobia and Secession in Texas—From an Office in Russia," CNN, October 6, 2017, https://www.cnn.com/2017/10/05/politics/heart-of-texas-russia-event/index.html.

[148] Casey Michel, "The Kremlin's California Dream," *Slate*, May 4, 2017, http://www.slate.com/articles/news_and_politics/foreigners/2017/05/why_russia_cultivates_fringe_groups_on_the_far_right_and_far_left.html.

[149] Lister and Sebastian, "Stoking Islamophobia and Secession in Texas"; Patrick Reevell, "Texas, California Separatists Attend Kremlin-Funded Conference," ABC News, September 27, 2016, https://abcnews.go.com/International/texas-california-separatists-attend-pro-kremlin-conference/story?id=42395066.

[150] Lister and Sebastian; Reevell, "Texas, California Separatists Attend Kremlin-Funded Conference."

The Anti-Globalization Movement of Russia, as this group is called, exists to offer support and encouragement to separatists in nations all over the world.[151]

At a Senate Intelligence Committee hearing regarding Russia's social media influence campaigns in November 2017, Russia was accused of using social media bots, state media amplification, and even clandestine financial and material aid to support and amplify recent secession movements.[152] Among these campaigns were Catalonia's contentious unauthorized referendum against Spain in 2017, a narrowly defeated 2014 referendum regarding Scotland's independence from the United Kingdom, the United Kingdom's unexpected 2016 vote to exit the European Union, illegal sham referenda in Crimea and Ukraine's Donbass region in 2014, and activity in other "frozen conflict" zones.[153] Evidence presented at this hearing suggested that Russia also attempted to provoke Hawaiian, Puerto Rican, and Native American tribal rebellion in addition to the Texas secession.[154] Russian support for secession movements serves as evidence of a broad trial-and-error strategy. That Russia appears to have directly advocated violence and fear among U.S. citizens and attempted to coordinate confrontations between rival groups in 2016, further reinforces the notion that they are experimenting with ways to stoke something akin to a civil war or unrest reminiscent of Soviet race war plots in the 1960s.[155] This notion is further bolstered by such stunts as an incendiary Internet Research Agency troll group called Black Fist funding self-defense classes for African-American activists

---

[151] Not only can secession movements cause chaos and force national governments to focus attention and resources on internal matters, they also serve as a useful propaganda tool for Russia to justify and normalize its near-universally condemned takeover of Crimea. Reevell, "Texas, California Separatists Attend Kremlin-Funded Conference."

[152] Jan Martínez Ahrens, "U.S. Senate Addresses Russian Interference in Catalonia on Social Media," *El País*, November 3, 2017, https://elpais.com/elpais/2017/11/03/inenglish/1509707476_016214.html; Narayanan et al., *Russian Involvement and Junk News during Brexit*; David Leask, "SNP Claims Russia Is Likely to Have Interfered in Referendum," *The Herald*, December 14, 2017, https://www.heraldscotland.com/news/15771388.yes-leaders-dont-be-naive-about-russian-online-meddling-in-independence/; Daniel Treisman, "Why Putin Took Crimea," *Foreign Affairs*, April 18, 2016, https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-putin-took-crimea.

[153] Ahrens; Narayanan et al.; Leask; Treisman.

[154] Casey Michel, "Russia Wants Texas and Puerto Rico to Secede," *The Daily Beast*, sec. world, September 24, 2015, https://www.thedailybeast.com/articles/2015/09/24/russia-wants-texas-and-puerto-rico-to-secede.

[155] Andrew and Mitrokhin, *The Sword and the Shield*, 238.

Page 3126 of 3957

throughout the United States ahead of the election.[156] With sometimes-violent unrest popping up in cities across the United States in 2020 over coronavirus mitigation measures, political campaigns, election results, and social justice issues—including at least one foiled plot to assassinate a state governor and provoke a rebellion—some of Russia's longshot bets have a legitimate chance of paying out to some degree.[157]

3. New Threats and Force Multipliers: Cyberattacks

In addition to the resurgence of active measures techniques that appeared dormant in the years following the collapse of the Soviet Union, new tactics have emerged as complements and accelerants to such measures in present-day influence campaigns. In many cases, longstanding interference methods have adapted and improved, often with the benefit of technological advances, such as the internet and social media. Espionage, reconnaissance, propaganda distribution, recruitment, and many other elements of interference tradecraft have been made much easier and more successful by the availability of data and social media on the internet. Contemporary Russia has thus been able to expand greatly the size and scope of its activities compared to Soviet influence efforts. Along with legal means of information harvesting and dissemination, Russia uses the internet as a powerful new toolset for its influence campaigns: cyberattacks, to include hacking, infrastructure disruption, and file manipulation.

Twenty-first-century Russian hacking operations have proven to be useful disruptors in their own right, as well as accelerators for other influence methods, such as

---

[156] Donie O'Sullivan, Drew Griffin, and Curt Devine, "In Attempt to Sow Fear, Russian Trolls Paid for Self-Defense Classes for African Americans," CNNMoney, October 18, 2017, https://money.cnn.com/2017/10/18/media/black-fist-russia-self-defense-classes/index.html.

[157] Katie Shepherd, "Tensions over Restrictions Spark Violence and Defiance among Protesters as Trump Pushes States to Reopen," *Washington Post*, May 13, 2020, https://www.washingtonpost.com/nation/2020/05/13/protest-violence-coronavirus/; Derrick Bryson Taylor, "George Floyd Protests: A Timeline," *New York Times*, sec. U.S., July 10, 2020, https://www.nytimes.com/article/george-floyd-protests-timeline.html; Susan Miller and Jordan Culver, "'It's Not Over': Trump Supporters Flock to State Capitols after Biden Victory Is Announced," USA Today, November 7, 2020, https://www.usatoday.com/story/news/nation/2020/11/07/election-protests-updates-trump-supporters-state-capitols-biden-win/6203271002/; Robert Snell and Melissa Nann Burke, "Plans to Kidnap Whitmer, Overthrow Government Spoiled, Officials Say," *Detroit News*, October 8, 2020, https://www.detroitnews.com/story/news/local/michigan/2020/10/08/feds-thwart-militia-plot-kidnap-michigan-gov-gretchen-whitmer/5922301002/.

Page 3127 of 3957

slander, forgery, and political influence. The information obtained from a hack can be used to inform future influence campaigns, identify vulnerabilities and strategies that can be exploited and countered, or to embarrass or compromise the target upon public release.[158] Worse yet, the stolen material can even be doctored to create compromising material where none naturally exists.[159] The theft or even insinuation of theft of sensitive information can be used as blackmail if release is threatened. Finally, attribution of a cyberattack's origin can be difficult, so a perpetrator can avoid detection, and thus also avoid consequences. It is in this space that Russian influence campaigns have been masterful. Cyberattacks are now a staple of the Kremlin's influence campaigns, whether targeting a nation's candidates, election systems, government services, or even critical infrastructure sectors.[160]

The ways in which any hostile power could conceivably disrupt infrastructure or commerce grows with every new interconnected device and advance in networking, limited only by a potential attacker's capacity and the intended victim's ability to thwart, punish, or effectively counterattack. By this metric, the threats posed by Russian cyberattacks are among the most severe imaginable, as the GRU has spent years honing its craft. Also in the Kremlin's favor is the fact that its nuclear weapons arsenal provides the ultimate strategic defense against a physical or military counterattack to its cyber meddling; an advantage very few of the world's other hackers and groups can boast. As the full range of possible cyberattack capabilities is too broad to list, it may be more useful to analyze actions allegedly already taken by Kremlin agents.

A bellwether case study for the havoc Russian-origin cyberattacks can wreak on a society is a 2007 Estonian cyberattack. In the wake of Estonian authorities' decision to move a controversial Soviet World War II memorial from downtown Tallinn to a military cemetery, and fueled by disinformation on Russian-language media saying the monument

---

[158] Joshua D. Christian, "Russian Cyber Operations to Destabilize NATO" (master's thesis, Naval Postgraduate School, 2020); Alexander M. Perkins, "Soviet Active Measures Reborn for the 21st Century: What Is to Be Done?" (master's thesis, Naval Postgraduate School, 2018).

[159] Thomas Brewster, "Russian 'Fancy Bear' Hackers Tainted Their Huge Leaks with Fake Data," *Forbes*, May 26, 2017, https://www.forbes.com/sites/thomasbrewster/2017/05/26/russian-dnc-hackers-planted-leaks-with-fake-data/.

[160] Christian, "Russian Cyber Operations To Destabilize NATO"; Perkins, "Soviet Active Measures Reborn."

Page 3128 of 3957

was set to be destroyed, riots among the Russian-language population ensued. The following night, Estonian network systems were beset by a weeks-long siege including computer script-driven "distributed denial of service" (DDoS) attacks that caused sporadic outages in the banking, media, and government sectors, to include failure of automated teller machines, public servant email accounts, and news broadcasts. In a taunting and unpersuasive denial, Putin wryly suggested the attack might have been the work of independent "patriotic hackers" motivated by love for Russia and incensed at the exaggerated news of the statue's removal rather than official state actors.[161] The Russian government refused to assist Estonian law enforcement's investigation of the perpetrators despite a standing treaty compelling them to do so, and significant evidence that the attack originated with Russian IP addresses.[162]

This incident, which rattled Estonian society and led the government to bolster its cybersecurity posture significantly, offered an example of the unpredictable chaos Russia could unleash on a foe under the guise of domestic tensions and difficult-to-attribute cyberattacks. The attack also put Russia's potential foes on notice that the nation is capable of inflicting substantial damage on a rival society without crossing a border or firing a shot. Perhaps most troubling to U.S. observers, the Estonian attack hinted at Russia's apparent ability and willingness to wound a NATO member state at a significant level without triggering the alliance's Article Five agreement, which states that an attack against any member is an attack against all and must be met with a unified response.[163]

Perhaps less risky for Russia though is the following option: a hybrid campaign that cripples essential services in a NATO country via a devastating yet difficult to definitively attribute cyberattack, yet does not involve physical weaponry deployment or border

---

[161] Krishnadev Calamur, "Putin Says 'Patriotic Hackers' May Have Targeted U.S. Election," *The Atlantic*, June 1, 2017, https://www.theatlantic.com/news/archive/2017/06/putin-russia-us-election/528825/.

[162] Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News, sec. Europe, April 27, 2017, https://www.bbc.com/news/39655415.

[163] "The North Atlantic Treaty," North Atlantic Treaty Organization, April 4, 1949, http://www.nato.int/cps/en/natohq/official_texts_17120.htm; Michael R. Kristek, "The Nature of Russia's Threat to NATO's Enhanced Forward Presence in the Baltic States" (master's thesis, Naval Postgraduate School, 2017), 38; Kaspars Galkins, "NATO and Hybrid Conflict Unresolved Issues from the Past or Unresolvable Threats of the Present" (master's thesis, Naval Postgraduate School, 2012), 9.

Page 3129 of 3957

incursion. Such a "gray area" attack could trigger alliance infighting and a lack of consensus regarding a full-scale Article Five response, thus undermining the alliance's main purpose. Perhaps cognizant of such a novel scenario, NATO quickly founded the Cooperative Cyber Defence Center of Excellence in Tallinn not long after the 2007 Estonian cyberattack.[164] More than a decade after the Estonia incident, however, ambiguity continues to surround each NATO member's stance on the threshold a cyberattack must hit before signifying an act of war. Questions include whether it makes a difference if the attack is definitely state-sponsored or possibly carried out by its "patriotic" residents (as Putin has smugly suggested more than once), and whether it is definitively safe to declare a cyberattack an act of war while also engaging in offensive cyber activity, such as Stuxnet (a malicious cyber worm of alleged U.S. and Israeli origin used to damage Iran's nuclear program severely).[165] A June 2017 statement issued by NATO Secretary General Jens Stoltenberg in the wake of a mysterious global cyberattack hinted that questions still remain even as the alliance seeks to harden its cyber defenses, as he warned those responsible that NATO nations had agreed that a cyberattack *could* trigger Article Five (emphasis added).[166]

Notably, the attack Stoltenberg referred to (known as "NotPetya") originated in Ukrainian tax software and wreaked havoc on the nation in a manner similar to the 2007 Estonia attack, before spreading sporadically and uncontrollably to public and private sector entities worldwide. U.S. CIA and British intelligence reports identified with high

---

[164] "NATO Opens New Centre of Excellence on Cyber Defence," North Atlantic Treaty Organization, May 14, 2008, https://www.nato.int/docu/update/2008/05-may/e0514a.html.

[165] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, 1st ed. (New York: Crown Publishers, 2014).

[166] Roland Oliphant and Cara McGoogan, "NATO Warns Cyber Attacks 'Could Trigger Article 5' As World Reels from Ukraine Hack," *The Telegraph*, June 28, 2017, https://www.telegraph.co.uk/news/2017/06/28/nato-assisting-ukrainian-cyber-defences-ransom-ware-attack-cripples/.

confidence the GRU as the perpetrator for this attack, which concurred with earlier Ukrainian intelligence assessments.[167]

Whereas NotPetya may have been an out-of-control juggernaut affecting as many sectors as possible, Russia has demonstrated that it can also target infrastructure and communications equipment with precision. In June 2015, 12-channel French television network TV5 Monde was hit with a devastating cyberattack that appeared to have been meticulously tailored to destroy its broadcast transmission hardware.[168] Seven different components simultaneously fell under attack, including a Netherlands-based remote-control camera company used by the network. The network website was maliciously reprogrammed to display a message indicating the Islamic State took credit for the mayhem, but French authorities quickly traced the attack to the GRU.[169] Six months later, a well-coordinated and highly sophisticated remote takeover of multiple Ukrainian power grid control center distribution systems, later attributed to the GRU by the UK Cyber Security Centre, shut off power to hundreds of thousands of residents in western Ukraine.[170] The GRU has also been blamed by Western governments for a litany of infractions to include a pre-war attack on Georgia's government agency systems in 2008, the penetration of various Eastern European countries' defense ministries in 2014, and a significant 2015 network takeover and data destruction attack against Germany's

[167] Ellen Nakashima, "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, January 12, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html; David Meyer, "Russia Blamed for 'Costliest Cyberattack in History," *Fortune*, February 16, 2018, http://fortune.com/2018/02/16/russia-notpetya-cyberattack-damage/.

[168] "'Russian Hackers' behind TV Attack," BBC News, sec. Europe, June 9, 2015, https://www.bbc.com/news/world-europe-33072034.

[169] Gordon Corera, "How France's TV5 Was Almost Destroyed by 'Russian Hackers,'" BBC News, sec. Technology, October 10, 2016, https://www.bbc.com/news/technology-37590375.

[170] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid; Marc Bennetts, "Fancy Bear, Voodoo Bear and Sandworm: Who Are the Russian Hackers?," *The Times*, sec. News, October 4, 2018, https://www.thetimes.co.uk/article/cybertattak-fancy-bear-voodoo-bear-and-sandworm-who-are-the-russian-hackers-g5698hrwz.

Bundestag parliamentary system.[171] In light of the broad array of cyber-based disruptions it has been practicing and refining, it is clear the Kremlin has a new toolset to deploy strategically as a means to sow division, influence, or thwart communications during a critical event or time period, and disrupt the normal functioning of a foreign government. For example, Russian operatives could unleash a precise, narrowly targeted attack against a media network during an election cycle that could materially affect voters' ability to access information about a candidate or result, or a targeted attack on critical infrastructure in a given municipality that could cause chaos and disruption at polling locations and undermine the integrity of the outcome.

4. Relative Impunity

When confronted with the fact that more than a dozen GRU operatives were under criminal indictment in the United States for cyber-based election interference, Putin denied that the suspects worked for the Russian government, demanded the United States reveal its evidence, and bluntly swore that Russia would never cooperate with other nations' attempts to prosecute its hackers: "Never. Never. Russia does not extradite its citizens to anyone."[172] By always denying responsibility for cyberattacks and refusing to extradite or cooperate with investigations, the Kremlin has mostly escaped consequences for these intrusions thus far, which has allowed them to enjoy a measure of freedom to test and refine their capabilities. Similarly, the risk of prosecution for an army of citizens paid through proxies to create and amplify disinformation on social media and hide behind fake foreign personas is low due to the high volume of content and relative anonymity of its operatives. Any rival nation's attempt at in-kind retaliation would likely be thwarted by the Russian government's strict control of the internet within its borders, which allows it to block any

[171] Bennetts; Patrick Beuth et al., "Cyberattack on the Bundestag: Merkel and the Fancy Bear," *Die Zeit*, sec. Digital, May 12, 2017, https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia#fancy-bear-cyber-attacks-info-2-tab; Nicole Perlroth and David E. Sanger, "Times's Moscow Bureau Hit by Attempted Hacking," *New York Times*, sec. Technology, August 24, 2016, https://www.nytimes.com/2016/08/24/technology/new-york-timess-moscow-bureau-was-targeted-by-hackers.html.

[172] Josh Lederman, "Putin: Russia Will 'Never' Extradite Citizens Accused by U.S.," *Associated Press*, sec. United States, March 4, 2018, https://apnews.com/article/c5180bffb84d424ba11cf3384a665eb5.

Page 3132 of 3957

content it chooses swiftly.[173] Finally, Russia's support and cultivation of fringe parties and organizations in rival states in some cases may give it allies capable of thwarting investigations into its interference, vetoing penalties such as sanctions, and sponsoring or attacking legislation to suit the Kremlin's interests.[174] Taken in aggregate, it becomes clear that in the current environment, Moscow has a large array of well-honed interference tools and little to dissuade it from using them.

[173] Justin Sherman, "Russia Is Trying Something New to Isolate Its Internet from the Rest of the World," *Slate Magazine*, September 25, 2020, https://slate.com/technology/2020/09/russia-internet-encryption-protocol-ban.html; Justin Myles-Primakoff and Justin Sherman, "Russia's Internet Freedom Shrinks as Kremlin Seizes Control of Homegrown Tech," *Foreign Policy*, October 26, 2020, https://foreignpolicy.com/2020/10/26/russia-internet-freedom-kremlin-tech/.

[174] Shekhovtsov, *Russia and the Western Far Right*, loc. 8682–8756.

III. ELECTION INTERFERENCE

This chapter focuses on a Russian interference attack type that may have the greatest potential for destructive, lasting impact: meddling and manipulation in the process of electing leaders in democratic societies. Russia's methods of foreign political interference were on full display in such pivotal world events as the 2016 U.S. presidential election, the "Brexit" referendum regarding Great Britain's membership in the EU, and other elections throughout Europe. Just as in Soviet times, some of the primary goals of this interference appear to include the weakening of Western rivals and alliances such as NATO, the promotion of leaders with favorable attitudes toward Moscow, attacks smearing politicians seen as hostile toward Russia, the deflection and denial of Russia's role in nefarious events, and the stoking of mistrust and division in Western societies.[175]

To understand U.S. vulnerability to Russian election interference and establish the plausibility of the threat, this chapter first details known instances of Soviet attempts to influence U.S. politicians and tilt the scales toward a Kremlin-favored outcome. Next, it analyzes the broad range of tools that Russia used in its bid to influence the 2016 U.S. presidential election. Finally, this chapter explores other recent instances of Russian meddling in Western elections to identify tactics and efficacy further.

A. SOVIET MEDDLING IN U.S. ELECTIONS

During the Cold War, Moscow made overt offers to potential U.S. presidential candidates on multiple occasions by offering to help them defeat anti-Kremlin rivals in exchange for the expectation of friendly treatment. For example, John Bartlow Martin reported in 1977 that Adlai Stevenson, the Democratic Party candidate whose unsuccessful 1952 and 1956 campaigns included nuclear nonproliferation rhetoric that Kremlin officials

[175] Perkins, "Soviet Active Measures Reborn," 7–9; Galkins, "NATO and Hybrid Conflict Unresolved Issues from the Past or Unresolvable Threats of the Present"; Ramsay and Robertshaw, *Weaponising News*, 69–91.

Page 3134 of 3957

saw as beneficial, reported one such overture.[176] According to Stevenson, Soviet ambassador Mikhail Menshikov set up a one-on-one meeting ahead of the 1960 presidential election to persuade him to run against sitting Vice President Richard Nixon.[177] To Stevenson's alarm, the ambassador offered to use the Soviet press to help him win election, in part by publishing either positive or critical stories about the campaign; whichever Stevenson thought would get him the most votes.[178]

Soviet leader Nikita Khrushchev later acknowledged that he continued to do everything in his power to prevent Nixon from winning the 1960 election, citing as motivation animosity following an infamously tense exchange between the two at an American technology exhibition the year before.[179] Aleksandr Feklisov, a Soviet spy serving as the KGB's Washington, DC, station chief during this time, later admitted to having been "instructed… to propose measures, diplomatic, propagandist, or other, to encourage [John F.] Kennedy's victory" and revealed that an agent had attempted to offer assistance to Kennedy's campaign against Nixon through his brother Robert F. Kennedy.[180]

Upon meeting President Kennedy for the first time after his victory, Khrushchev took credit for tipping the close race by bragging that he had weakened Nixon by refusing to release American pilots from Soviet captivity until after the election.[181] When Nixon again ran for president in 1968, Soviet intervention attempts were even more direct. Anatoly Dobrynin, Moscow's ambassador to the United States at the time, admitted

---

[176] John Bartlow Martin, *Adlai Stevenson and the World: The Life of Adlai E. Stevenson* (Garden City, NY: Anchor Books, 1977), 472; Bruce W. Dearstyne, "The Russians Tried Once before to Meddle in a U.S. Presidential Election," History News Network: George Washington University Columbian College of Arts and Sciences, December 29, 2016, https://historynewsnetwork.org/article/164769.

[177] David Shimer, *Rigged: America, Russia and One Hundred Years of Covert Electoral* Interference (New York: Knopf, 2020), 87–88.

[178] Shimer, 87–88.

[179] William Safire, "The Cold War's Hot Kitchen," *New York Times*, sec. Opinion, July 23, 2009, https://www.nytimes.com/2009/07/24/opinion/24safire.html.

[180] Vladislav Zubok and Konstantin Pleshakov, *Inside the Kremlin's Cold War: From Stalin to Khrushchev* (Cambridge, MA: Harvard University Press, 1996).

[181] Adam Taylor, "This Kremlin Leader Bragged about Tipping a U.S. Presidential Election," *Washington Post*, January 6, 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/01/06/this-kremlin-leader-bragged-about-tipping-a-u-s-presidential-election/.

carrying out an order to offer campaign assistance secretly to Nixon's opponent Hubert Humphrey including financial aid.[182] Mitrokhin also notes that even after Nixon's resignation due to the Watergate scandal, then-KGB chairman Yuriy Andropov ordered his bureau to make overtures to officials in Nixon's administration—including speechwriter William Safire and eventual presidential candidate Pat Buchanan—in attempts to use them for the Soviet cause. In each case, the Americans refused the offers.[183]

Though most if not all U.S. politicians appear to have known better than to accept Soviet offers for aid, the practice may have still been of value to the KGB's active measures apparatus. Directly offering assistance to potential U.S. presidential candidates could have served multiple purposes: aside from providing the offered boost to the Kremlin's desired candidates, any accepted offer could have also served as leverage for blackmail or a foolproof way to ruin the acceptor's reputation should the relationship ever sour. In addition, any evidence that an offer of assistance was made, or that contact between foreign influence agents and anyone involved in a candidate's campaign or administration had taken place, could be used by that candidate's opponents or detractors. Opponents could use evidence of a Russian attempt to render aid to smear or slander the candidate as corrupt, even if the candidate rejected the offer. Additionally, if a credible suggestion that the Kremlin might have influenced a U.S. election or compromised a lawmaker were introduced in the American press or even leaked deliberately by Soviet agents, domestic and international belief in the legitimacy of elected leaders could be undermined, which would then lead to a constitutional crisis.

According to Mitrokhin's archives, the KGB launched a concerted effort to doom hawkish anti-Soviet Senator Henry "Scoop" Jackson's presidential aspirations in 1976 by forging FBI documents falsely indicating that he was a homosexual (at a time when U.S. voters were seen as likely to reject such a candidate), and distributing them to his political rivals, as well as popular magazines in hopes that the rumor would catch on.[184] Though no

---

[182] Anatoly Dobrynin, *In Confidence: Moscow's Ambassador to America's Six Cold War Presidents (1962–1986)*, 1st ed. (New York: Times Books, Random House, 1995).

[183] Andrew and Mitrokhin, *The Sword and the Shield*.

[184] Andrew and Mitrokhin, *The Sword and the Shield*, 240.

evidence suggests these rumors played a significant role in derailing Jackson's presidential bid, the KGB continued attacking the Senator by disseminating forged documents regarding his sexual preferences more than a year after he ended his campaign.[185]

B. MODERN MEDDLING IN U.S. ELECTIONS

The initial years after the Soviet Union's collapse marked an apparent respite in concerted Russian attempts to influence the outcome of Western elections, but by the second decade of the twenty-first century, it became increasingly clear that the lull was over. Particularly since 2014, the concept and scope of Russian interference campaigns has become extremely well known in Western nations, even as Moscow issues repeated denials. Along with U.S. elections, allegations of Russian interference have surfaced in recent British, Bulgarian, German, French, Scottish, Spanish, and Ukrainian elections and referenda within a five-year period.[186] One of the largest and arguably most consequential Kremlin attempts to tip the scales for or against political candidates in recent years is the 2016 U.S. presidential election, in which a variety of mechanisms were allegedly deployed in support of candidate Donald Trump and against Putin foe Hillary Clinton. This section attempts to analyze the various subversive avenues Russia used in its attempt to sway the election, as well as a few others occurring in the same general timeframe, to include overt Russian media, social media, hacking theft, and other cyberattacks.

1. State-Run Media

In 2017, the U.S. Director of National Intelligence (DNI) released an interagency report on Russian interference in the 2016 presidential election, which revealed that the

---

[185] Andrew and Mitrokhin, 241.

[186] Narayanan et al., *Russian Involvement and Junk News during Brexit*; "Huge Hack Attack on Bulgaria Election Authorities 'Not to Affect Vote Count," Novinite Sofia News Agency, October 27, 2015, https://www.novinite.com/articles/171533/Huge+Hack+Attack+on+Bulgaria+Election+Authorities+%27Not+to+Affect+Vote+Count%27; Constanze Stelzenmüller, "The Impact of Russian Interference on Germany's 2017 Elections," Brookings, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/; "The Macron Leaks: Are They Real, and Is It Russia?," Lawfare, May 8, 2017, https://www.lawfareblog.com/macron-leaks-are-they-real-and-it-russia; Keeley, "Russia Meddled in Catalonia Independence Referendum"; Katya Gorchinskaya, Olga Rudenko, and William Schreiber, "Authorities: Hackers Foiled in Bid to Rig Ukraine Presidential Election Results," *Kyiv Post*, May 25, 2014, https://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html.

Page 3137 of 3957

nation had used both overt and covert means to affect the outcome. This document extensively referenced state-owned media outlets RT and Sputnik and highlighted their role in attempting to tilt the previous year's U.S. presidential election in favor of Trump.[187] The report cites the Kremlin-backed media companies' frequent denigration of Democratic candidate Hillary Clinton and the U.S. presidential election process as a calculated, years-long program aimed specifically at damaging her electability. Russia's English-language media outlets are not only used to spread negative information, to be sure. These news networks also take advantage of their apparent legitimacy as news sources to boost coverage of events and political actors not widely covered by traditional media, and thus boost the candidates' profiles and expand their audiences. Far-left U.S. Green Party presidential candidate Jill Stein, derided by many Democratic Party supporters as an unserious candidate whose presence on the ballot served primarily to split the liberal vote, and thus, to benefit Republicans, received outsized support and publicity from RT and Sputnik during the 2012 and 2016 presidential campaigns.[188] Such support included a number of interviews and a primetime 2016-debate broadcast that allowed her to showcase her campaign platform.[189] Stein's enthusiastic appearance at a 2015 gala celebrating RT's 10th anniversary, along with her outspoken advocacy for such Kremlin obsessions as lifting Crimea-related sanctions and criticism of Ukraine, raised alarm in light of the DNI report.[190] Evidently suspicious of RT's outsized coverage of Stein, the U.S. Senate Investigative Committee in 2017 announced a probe of her campaign to look for evidence of illegal Russian support.[191] Stein denied any improper collusion with the Kremlin but

---

[187] Office of the Director of National Intelligence, *Assessing Russian Activities*.

[188] Casey Michel, "The Pro-Kremlin Talking Points of Jill Stein," *ThinkProgress* (blog), December 19, 2017, https://archive.thinkprogress.org/jill-stein-campaign-russia-ecf424ac3b7e/; "'Atone!' Democrats Blame Jill Stein Voters for Trump's Chance to Appoint a 3rd Supreme Court Justice," RT, September 26, 2020, https://www.rt.com/usa/501803-jill-stein-bill-maher-supreme-court-trump/.

[189] "Green Party Candidates to Face Off in Debate Hosted by RT (Watch Live)," RT, May 9, 2016, https://www.rt.com/usa/342395-green-party-rt-debate/; "Jill Stein Offers Third Party Perspective on Final Debate," RT, October 20, 2016, https://www.rt.com/usa/363379-jill-stein-debates-live/.

[190] Robert Windrem, "Guess Who Came to Dinner with Flynn and Putin," NBC News, April 18, 2017, https://www.nbcnews.com/news/world/guess-who-came-dinner-flynn-putin-n742696.

[191] Robert Windrem, "Senate Russia Investigators Are Interested in Jill Stein," NBC News, December 19, 2017, https://www.nbcnews.com/news/us-news/why-are-senate-russia-investigators-interested-jill-stein-n831261.

initially resisted cooperating with the investigations, and at least two separate reports commissioned by the U.S. Senate found strong evidence of longstanding Russian support for her campaigns beginning soon after RT's launch.[192] Such support was not unprecedented, as RT had also frequently played host to former Republican congressman Ron Paul, one of Stein's 2012 presidential election opponents.[193] For his part, Paul, who conducted three combative, nontraditional populist presidential campaigns as a Libertarian and a Republican, has been described as one of the most outspoken defenders of Putin ever to have held U.S. federal office.[194] RT also provided significant support and airtime to former Minnesota governor and professional wrestler Jesse Ventura, an avid conspiracy theorist and U.S. government critic who occasionally announces exploratory presidential campaigns.[195]

Though not a candidate himself, U.S. Lieutenant General Michael Flynn was also frequently invited to appear as a guest speaker on RT to advocate for positions supported by the Kremlin.[196] A sharp critic of U.S. foreign policy since being ousted from his role as President Obama's Defense Intelligence Agency director, Flynn found a very receptive

[192] To clarify, Stein denied any deliberate connection with Russia to benefit Trump or financial ties to the Kremlin, but did not deny her appearances on RT. Robert Windrem, "Russians Launched Pro-Jill Stein Social Media Blitz to Help Trump, Reports Say," NBC News, December 22, 2018, https://www.nbcnews.com/politics/national-security/russians-launched-pro-jill-stein-social-media-blitz-help-trump-n951166; Molly Roberts, "Jill Stein Isn't Doing the Left Any Favors," *Washington Post*, May 2, 2018, https://www.washingtonpost.com/blogs/post-partisan/wp/2018/05/02/jill-steins-attitude-toward-the-russia-investigation-isnt-doing-the-left-any-favors/.

[193] Lincoln Mitchell, "Ron Paul's Appearances on Kremlin TV Could Damage His Son's Presidential Aspirations," *Observer* (blog), November 17, 2014, https://observer.com/2014/11/ron-pauls-appearances-on-kremlin-tv-could-damage-his-sons-presidential-aspirations/.

[194] Lucia Graves, "Ron Paul Is Putin's New Best Friend," *The Atlantic*, July 21, 2014, https://www.theatlantic.com/politics/archive/2014/07/ron-paul-is-putins-new-best-friend/439533/.

[195] Katie Mettler, "Jesse Ventura's New Russian State TV Show: 'I Am Working for the Enemy of Mainstream Media Now," *Washington Post*, June 8, 2017, https://www.washingtonpost.com/news/morning-mix/wp/2017/06/08/jesse-venturas-new-russian-state-tv-show-i-am-working-for-the-enemy-of-mainstream-media-now/; "Jesse Ventura Considering Running for President, 'Trump Will Not Have a Chance!," TMZ, November 28, 2018, https://www.tmz.com/2018/11/28/jesse-ventura-running-president-trump-wrestlemania/.

[196] Windrem, "Guess Who."

audience for his criticisms in RT.[197] Flynn's acceptance of $45,000 from the network to give a speech at the same network gala Stein attended later played a role in his forced resignation as President Trump's National Security Advisor due to improper contacts with the Russian ambassador before Obama's term ended, along with a federal indictment and trial that dragged on for the entirety of Trump's presidency.[198]

2. Social Media

On the covert side of its operation, Russia's attempts to interfere in the 2016 U.S. election made extensive use of its internet troll and bot armies on U.S.-based social media platforms. Even as Western newspapers began to grapple with the trolls' invasion of online comments sections, such social media titans as Facebook and Twitter appeared clueless or unconcerned by contrast. Just after Trump's victory in November 2016, Facebook founder Mark Zuckerberg publicly scoffed at accusations that fake news on social media or foreign manipulation of the platform had any noteworthy impact, and insisted, "to think it influenced the election in any way is a pretty crazy idea."[199]

---

[197] Rosalind S. Helderman and Tom Hamburger, "Trump Adviser Flynn Paid by Multiple Russia-Related Entities, New Records Show," *Washington Post*, sec. Politics, March 16, 2017, https://www.washingtonpost.com/politics/new-details-released-on-russia-related-payments-to-flynn-before-he-joined-trump-campaign/2017/03/16/52a4205a-0a55-11e7-a15f-a58d4a988474_story.html.

[198] Mark Mazzetti and Matthew Rosenberg, "Michael Flynn Misled Pentagon about Russia Ties, Letter Says," *New York Times*, May 22, 2017, https://www.nytimes.com/2017/05/22/us/politics/michael-flynn-fifth-amendment-russia-senate.html; Robert Windrem, "Mike Flynn's RT Headache Won't Go Away," NBC News, April 27, 2017, https://www.nbcnews.com/news/us-news/mike-flynn-s-rt-headache-won-t-go-away-n752216.

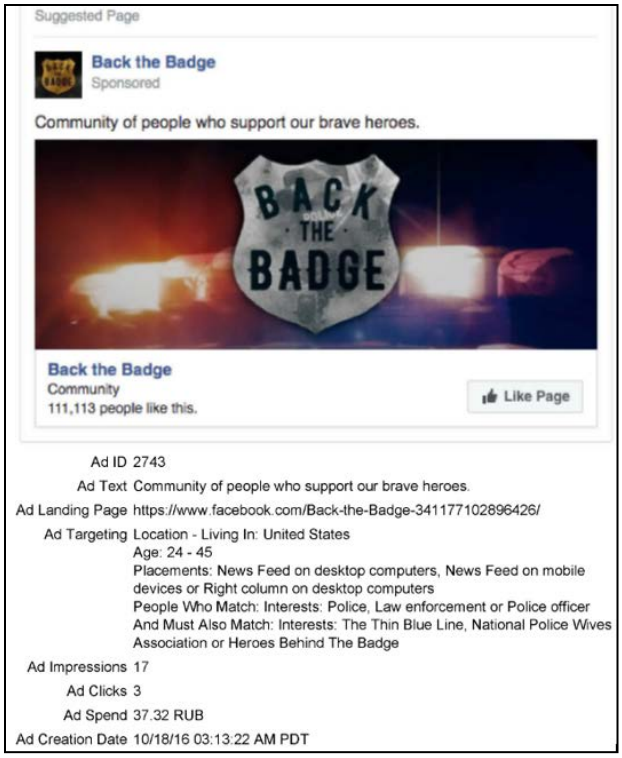
[199] Shanika Gunaratna, "With Trump's Election, Facebook Wrestles with the Power of Fake News," CBS News, November 11, 2016, https://www.cbsnews.com/news/with-trumps-election-facebook-wrestles-with-broader-impact-of-fake-news/.

At the same time, however, Facebook offered to embed staff in both the Trump and Clinton campaigns to help them use company algorithms to tailor paid content to optimal audiences; the company was clearly confident that its advertising service could be used to influence voters.[200] Additionally, the social media giant accepted Russian rubles as payment from a company buying more than $100,000 worth of divisive U.S. political ads; thus, arguably, Facebook also knew or should have known that foreign entities were using the platform to attempt to exert their own influence on the election.[201] See Figure 1. To Facebook's credit, it evidently had alerted the FBI of anomalous domestic political activity originating from Russia that it had detected on its platform in June 2016. Unfortunately, the company misidentified the nature of the abnormal activity as relating to possible espionage rather than an election influence campaign, and thus missed an important early signal of the operation.[202]

[200] Daniel Kreiss and Shannon C. McGregor, "Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google with Campaigns during the 2016 U.S. Presidential Cycle," *Political Communication* 35, no. 2 (April 3, 2018): 155–77, https://doi.org/10.1080/10584609.2017.1364814.

[201] *Committee on the Judiciary, Extremist Content and Russian Disinformation Online: Working with Tech to Find Solution*, Senate, 105th Cong. 1st sess., 2017, https://www.judiciary.senate.gov/meetings/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions.

[202] Adam Entous, Elizabeth Dwoskin, and Craig Timberg, "Obama Tried to Give Zuckerberg a Wake-up Call over Fake News on Facebook," *Washington Post*, September 24, 2017, https://www.washingtonpost.com/business/economy/obama-tried-to-give-zuckerberg-a-wake-up-call-over-fake-news-on-facebook/2017/09/24/15d19b12-ddac-4ad5-ac6e-ef909e1c1284_story.html.



Targeted Facebook Advertisement identified as part of a Russian interference effort, paid for in Rubles and advertising a Russian-operated page sharing additional content.

Figure 1. Back the Badge Facebook Advertisement.[203]

Approximately one year after the election, Facebook executives were called to appear before the Senate Judiciary Committee regarding the role the platform unwittingly played in Russia's influence campaign. At this hearing, a company representative testified that internal analysis showed that Russian influence agents had reached 126 million unique users over a period of three years leading up to the 2016 election.[204] These figures included at least 3,517 advertisements purchased by the IRA as highly targeted sponsored content (e.g., paid posts seen only by a narrow audience fitting demographics specified by the advertiser). Much more of the volume came from the creation of interest-based groups and false American identities producing and sharing such free content as pop culture-based

[203] Source: Permanent Select Committee on Intelligence, "Social Media Advertisements, 2016, Quarter 4, 2016-10: P(1)0005278," U.S. House of Representatives, accessed December 6, 2020, https://intelligence.house.gov/social-media-content/social-media-advertisements.htm.

[204] S., *Committee on the Judiciary*.

memes, however.[205] The campaign also exploited the company's subsidiary photo- and video-sharing site Instagram, which hosted at least 170 Russian interference-linked accounts and duplicated a number of the insidious ads purchased on Facebook.[206] Russia's disinformation was then amplified on both sites by unsuspecting Americans sharing and reposting the tainted content to even wider audiences.[207] See Figures 2 and 3. Content known or suspected to have come from coordinated Russian activity covered a wide range of election-adjacent topics, including but not limited to the following:

- promotion or attack of political policies
- commentary on social issues
- inflammatory religious imagery
- election logistics disinformation, such as false advertisements with phone numbers encouraging readers to text their votes rather than waiting in line at a polling location.[208]

[205] A meme is a popular image or video, often humorous in nature, shared widely by Internet users. Nick Penzenstadler, Brad Heath, and Jessica Guynn, "We Read Every One of the 3,517 Facebook Ads Bought by Russians. Here's What We Found," *USA Today*, May 11, 2018, https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/.

[206] Mike Isaac and Daisuke Wakabayashi, "Russian Influence Reached 126 Million through Facebook Alone," *New York Times*, sec. Technology, October 31, 2017, https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

[207] Isaac and Wakabayashi.

[208] On a document for Congress showing a series of English and Spanish tweets encouraging Clinton supporters to vote via text or Twitter hashtag and/or falsely claiming that each voter would need to bring a birth certificate, "IL driving license record", naturalization certificate, social security card, government ID card AND a U.S. or foreign passport to vote, Twitter appended a disclaimer that they had not definitively attributed Russian origin to those particular ads, but attributed them to automated accounts. The House Intelligence Committee Minority subsequently released the document showing these tweets along with a comprehensive list or IRA Twitter account names and RT network's paid Twitter advertisements in a release titled: "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," U.S. House of Representatives, Permanent Select Committee on Intelligence, accessed September 30, 2020, https://intelligence.house.gov/social-media-content/default.aspx; Penzenstadler, Heath, and Guynn, "Every One of the 3,517 Facebook Ads"; AnneClaire Stapleton, "No, You Can't Vote by Text Message," CNN, November 7, 2016, https://www.cnn.com/2016/11/07/politics/vote-by-text-message-fake-news/index.html.

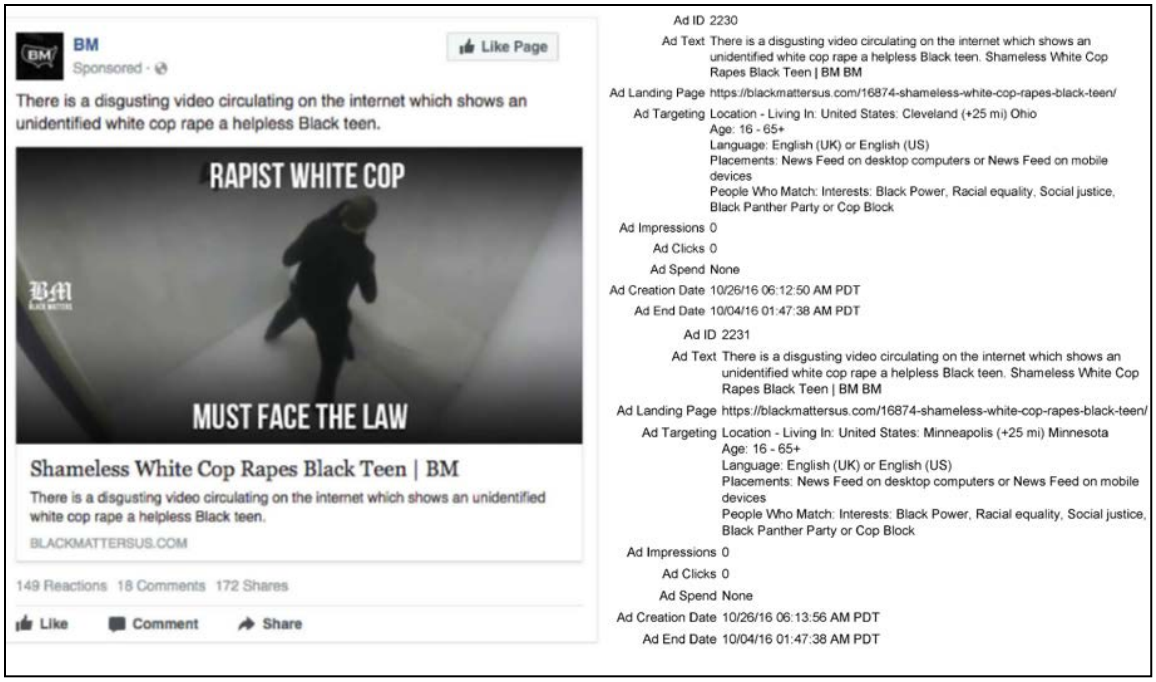
Page 3143 of 3957

Targeted Russian Facebook advertisement, paid in rubles, attempting to capitalize on social and political issues by promoting its "Stop All Invaders/Stop A.I." page in May 2016.

Figure 2. Stop A.I. (AKA Stop All Invaders) Facebook Advertisement.[209]

[209] Source: Permanent Select Committee on Intelligence, "Social Media Advertisements, 2016, Quarter 2, 2016-05: P(1)0000410," U.S. House of Representatives, accessed December 6, 2020, https://intelligence.house.gov/social-media-content/social-media-advertisements.htm.

Page 3144 of 3957



Russian Facebook advertisements using incendiary racial and social content to drive traffic to a fake Black social justice website operated by the IRA and narrowly targeted to Facebook users within 25 miles of Cleveland and Minneapolis, in the final weeks before the 2016 U.S. election. A Senate Intelligence Committee report found that "no single group of Americans was targeted by IRA information operatives more than African-Americans" and that two-thirds of IRA Facebook advertisements included words related to race; the report also illuminated efforts to dissuade African-Americans from voting in 2016, or to support Green Party candidate Jill Stein.

Figure 3. BM (AKA Black Matters) Facebook Advertisement.[210]

Exact figures on Kremlin-produced content are unattainable for a variety of reasons. Deleted or suspended accounts cannot always be recovered for review, definitively identifying the origin of every single well-produced fake profile is likely impossible, and distinguishing impersonators and amplifier accounts from authentic users is challenging. Nevertheless, a sense of the scope and breadth of Russia's operation can be gleaned from a review of statistics put forth by social media companies and investigative reports following the 2016 election.[211] At the same Senate Judiciary Committee hearing where

[210] Source: Permanent Select Committee on Intelligence, "Social Media Advertisements, 2016, Quarter 4, 2016-10: P(1)0004496," U.S. House of Representatives, accessed December 6, 2020, https://intelligence.house.gov/social-media-content/social-media-advertisements.htm.

[211] Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency* (Austin, TX: New Knowledge, 2018); Penzenstadler, Heath, and Guynn, "Every One of the 3,517 Facebook Ads"; S., *Committee on the Judiciary*.

Facebook disclosed its initial findings, Google admitted its streaming platform YouTube had been host to more than 43 hours of content across over 1,100 videos produced by suspected Russian interference agents. Google also shared that its AdSense online advertisement service had accepted more than $4,700 from the IRA to advertise on web pages and in search results.[212] In its turn at the same hearing, Twitter divulged the discovery of more than 2,700 IRA-affiliated accounts that had produced 130,000 tweets.[213]

Each of these platforms substantially raised the totals in subsequent reporting on Russian interference in the ensuing months and years as investigations continued. In October 2018, Twitter released more than nine million messages generated by 3,841 IRA-linked accounts.[214] Facebook later announced that it had deleted roughly 583 million fraudulent accounts and 837 million spam posts in the first quarter of 2018 alone, and that it believed that an additional four percent of its more than two billion active users were likely fake accounts that had gone undetected.[215] Though Russian interference was not likely responsible for every one of these fraudulent accounts, the sheer volume highlights the high degree of vulnerability of social platforms to misuse and illustrates the tremendous difficulty of detection and removal on so grand a scale.[216] Concurrently with Facebook and Twitter's announcements, such additional platforms as blog-hosting site Tumblr were found to have been exploited as well. After first reporting the suspension of 84 accounts that the company says "engaged in state-sponsored disinformation and propaganda campaigns" in March 2018 following months of media pressure, Tumblr added an additional 113 names to this list by mid-November.[217]

---

[212] S.

[213] S.

[214] Twitter News Desk, "Twitter's Focus Is on a Healthy Public Conversation," *Elections Integrity* (blog), October 17, 2018, https://about.twitter.com/en_us/values/elections-integrity.html.

[215] Guy Rosen, "Facebook Publishes Enforcement Numbers for the First Time," *Facebook Newsroom* (blog), May 15, 2018, https://newsroom.fb.com/news/2018/05/enforcement-numbers/.

[216] Rosen.

[217] Issie Lapowsky, "Tumblr IDs 84 Accounts that Spread Propaganda," Wired, March 23, 2018, https://www.wired.com/story/tumblr-russia-trolls-propaganda/; "Public Record of Usernames Linked to State-Sponsored Disinformation Campaigns," *Tumblr Help Center* (blog), November 16, 2018, http://tumblr.zendesk.com/hc/en-us/articles/360002280214-Public-record-of-usernames-linked-to-state-sponsored-disinformation-campaigns.

3. Microtargeting

One of the reasons Russia's 2016 social media influence campaign escaped mainstream scrutiny for as long as it did likely owed to its ability to tailor specific messages to different groups.[218] By partitioning the content, Russian actors ensured that only those likely to accept or appreciate a given message would even see it; indeed, the Senate Judiciary hearings into Russian social media influence campaigns indicated that much of the content was tailored and distributed to specific audiences.[219] While the trolls may have simply exploited publicly visible biographical and interest-based information on users' social media profile pages and user-generated content, they also may have capitalized on the availability of public records data in U.S. jurisdictions and thus extrapolated this data by using political or societal stereotypes.[220]

Worryingly, speculation abounded in the months after the 2016 election that Russia's targeted influence efforts may have also relied on criminally obtained information. One popular early theory was that Russian hackers might have stolen voter data by hacking the Democratic or Republican National Committee or even election commission offices.[221] Another incendiary accusation was that the Trump campaign might have provided information about voter rolls to the Russian operatives.[222] Though neither story was proven, the implication is terrifying; immense troves of data concerning potential voters exist in nearly all developed Western democracies. Much of this data is maintained

---

[218] Filipe N. Ribeiro et al., "On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook," in *Proceedings of the Conference on Fairness, Accountability, and Transparency—FAT* '19*, 140–49, January 29, 2019, https://doi.org/10.1145/3287560.3287580.

[219] S., *Committee on the Judiciary*.

[220] Robert E. Walker, "Combating Strategic Weapons of Influence on Social Media" (master's thesis, Naval Postgraduate School, 2019), https://www.hsdl.org/?view&did=828243.

[221] Violet Blue, "What If Russian Voter Hacks Were Just Part of Its Facebook Ad Campaign?," Engadget, October 6, 2017, https://www.engadget.com/2017-10-06-russian-voter-hacks-support-facebook-ad-campaign.html.

[222] Peter Stone and Greg Gordan, "Trump-Russia Investigators Probe Jared Kushner-Run Digital Operation," McClatchey DC Bureau, July 12, 2017, https://www.mcclatchydc.com/news/nation-world/national/article160803619.html; Issie Lapowsky, "Did Trump's Data Team Help Russians? Facebook Might Have the Answer," Wired, July 14, 2017, https://www.wired.com/story/trump-russia-data-parscale-facebook/; Martin Longman, "Did the Russians Mess with the Voter Rolls?," *Washington Monthly*, June 1, 2018, https://washingtonmonthly.com/2018/06/01/did-the-russians-mess-with-the-voter-rolls/.

Page 3147 of 3957

by private entities outside the federal government's purview to protect or regulate.[223] Moreover, nearly all this data can be obtained through a variety of means, to include legitimate purchases, theft, espionage, or collusion with a compromised actor.

4. Hacking and Cyberattacks

One of the most widely known and consequential examples of Russia's use of cyberattacks to influence an election is the hacking, attributed to the GRU, of the Democratic National Committee (DNC) and Hillary Clinton campaign team members' emails around 2016. According to a July 2018 indictment filed by Special Counsel Robert Mueller against 12 GRU officers, the intelligence agency used a variety of techniques including spearfishing through spoofed Google security notification messages and Microsoft files.[224] Once inside the DNC's networks, they monitored staff activity, implanted malware, and stole additional documents. The intrusion was not wholly unnoticed, but it was not stopped. The FBI had alerted the DNC of suspicious Russian-based activity on their servers on multiple occasions beginning in September 2015, though miscommunications and insufficient technical scans within the DNC failed to act properly on these tips.[225]

In June 2016, the hackers used anonymous online personas called DCLeaks and Guccifer 2.0 to "leak" selectively and promote links to thousands of the emails and other documents to the public without revealing obvious Kremlin fingerprints. The hackers also appeared to partner with WikiLeaks, a renowned international trafficker of stolen

---

[223] Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh, *Data Protection Law: An Overview*, CRS Report No. R45631 (Washington, DC: Congressional Research Service, 2019), 79.

[224] *Department of Justice, Indictment: United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morganchev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev, Defendants* (Washington, DC: Department of Justice, 2018), https://www.justice.gov/file/1080281/download.

[225] Isikoff and Corn, *Russian Roulette*.

Page 3148 of 3957

information and government secrets.[226] U.S. media outlets reported extensively on the contents of the emails each time a new batch was released, to damaging effect; a *Columbia Journalism Review* study conducted after the election argued that *The New York Times*' extreme focus on the hack and leak played an outsized role in costing Clinton the presidency.[227] Among other controversial issues, information in the emails revealed DNC chairwoman Debbie Wasserman Schultz's apparent bias toward Clinton and disdain for her primary opponent Bernie Sanders.[228] This disclosure led to Wasserman Schultz's immediate resignation on the eve of the Democratic National Convention, as well as high tension between Sanders and Clinton supporters that overshadowed Clinton's nomination ceremony and potentially cost her some of the Sanders supporters' votes in the general election.[229]

Somewhat surprisingly, Moscow's scheme with the stolen emails was not entirely met with bipartisan condemnation, and may have even received some measure of tacit encouragement. In July 2016, Trump generated a scandal by publicly asking Russia to "find the 30,000 emails that are missing" from Clinton's server during a televised campaign speech, saying Moscow's hackers would "probably be rewarded mightily by our press" for doing so.[230] Occurring soon after public reports that intelligence officials believed Russia was behind the DNC server hack emerged, Trump's request was criticized by some as a literal entreaty to an adversarial foreign state to intervene on his behalf in the election via

---

[226] *Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 5: Counterintelligence Threats and Vulnerabilities*, S. Rep. 116-XX, Senate, 116th Cong. 1st sess., 2020, https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf; Isikoff and Corn, 66.

[227] Duncan J. Watts and David M. Rothschild, "Don't Blame the Election on Fake News. Blame It on the Media," *Columbia Journalism Review*, December 5, 2017, https://www.cjr.org/analysis/fake-news-media-election-trump.php.

[228] Isikoff and Corn, *Russian Roulette*, 130–131, 164–175; Alana Abramson and Shushannah Walshe, "The 4 Most Damaging Emails from the DNC WikiLeaks Dump," ABC News, July 25, 2016, https://abcnews.go.com/Politics/damaging-emails-dnc-wikileaks-dump/story?id=40852448.

[229] Sean Illing, "Division and Tension at the DNC: The Democrats' Night of Unity Is Marred by Dissent," Salon, July 26, 2016, https://www.salon.com/2016/07/26/division_and_tension_at_the_dnc_the_democrats_night_of_unity_is_marred_by_dissent/.

[230] Ashley Parker and David E. Sanger, "Donald Trump Calls on Russia to Find Hillary Clinton's Missing Emails," *New York Times*, sec. U.S., July 27, 2016, https://www.nytimes.com/2016/07/28/us/politics/donald-trump-russia-clinton-emails.html.

illegal activity.[231] In 2017, reports emerged that Trump's son Donald Jr. and son-in-law Jared Kushner, along with Trump campaign manager Paul Manafort, had met with a Kremlin-linked Russian attorney offering damaging information about the Clintons the same week that documents stolen from the email hack were released.[232] To Trump's rage and dismay, his opponents seized on this meeting, along with inconsistent explanations of it from Trump and his legal advisors, to accuse his campaign of collusion with Russia in the hacking and influence campaign or at least inappropriate behavior in the face of improper offers of assistance from a top U.S. foe.[233]

Moscow's hacking efforts targeted not just communications and documents from political campaigns, but also attacked U.S. election infrastructure; a chilling escalation that has the potential to cause longer-term damage to democratic societies than the defeat of a single candidate. Two months before the 2016 election, U.S. voters were alarmed by reports that the Department of Homeland Security (DHS) had detected hacking attempts on the election systems of 21 states, with Russia as the likely culprit.[234] A month before that disclosure, the Illinois Board of Elections had already confirmed that its database of registered voters had been breached in what the FBI considered a sophisticated foreign

---

[231] Parker and Sanger.

[232] Phillip Bump, "What We Know about the Trump Tower Meeting," *Washington Post*, August 7, 2018, https://www.washingtonpost.com/news/politics/wp/2018/08/07/what-we-know-about-the-trump-tower-meeting/; Isikoff and Corn, *Russian Roulette*.

[233] Further fanning the flames of collusion accusations was the revelation that major Trump campaign supporter Roger Stone had been in contact with WikiLeaks and seemed familiar with the contents of stolen emails before their release. Stone was later convicted on seven felony counts related to his obstruction of a Congressional inquiry into Russia's attempts to influence the election in favor of Trump, including lying under oath and attempting to block the testimony of other witnesses. Even if no actual coordination occurred between the Trump campaign and Russia with regard to stolen and leaked emails, these incidents at the very least illustrate how the DNC and the Clinton campaign hacking operation managed to cause problems for both candidates at different times, and contribute more generally to exacerbating mistrust and division among American voters. Isikoff and Corn, *Russian Roulette*, 74; Parker and Sanger, "Donald Trump Calls on Russia"; Sara Murray and Kate Sullivan, "Text Messages Show Roger Stone Discussing WikiLeaks Plans Days before Hack," CNN, November 26, 2018, https://www.cnn.com/2018/11/14/politics/text-messages-roger-stone-wikileaks-hack/index.html; Isikoff and Corn, *Russian Roulette*; Sharon LaFraniere and Zach Montague, "Roger Stone Is Convicted of Impeding Investigators in a Bid to Protect Trump," *New York Times*, sec. U.S., November 15, 2019, https://www.nytimes.com/2019/11/15/us/politics/roger-stone-trial-guilty.html.

[234] Cynthia McFadden et al., "Red Alert? Hackers Target Election Systems in 20 States," NBC News, September 29, 2016, https://www.nbcnews.com/news/us-news/red-alert-election-systems-20-states-targeted-hackers-n657036.

attack.[235] In July 2018, the office of Special Counsel Mueller took action on these claims and announced an indictment charging that two GRU operatives probed websites and networks of counties in Georgia, Florida, and Iowa for back-end server vulnerabilities one week before the 2016 election.[236] In 2019, reports from the Senate Intelligence Committee, DHS, and FBI eventually acknowledged that Russia had actually attacked the election infrastructure of all 50 U.S. states in 2016, with a possible intent to use the fruits of these attacks at a later time.[237]

C. OTHER MODERN RUSSIAN EFFORTS TO INFLUENCE FOREIGN ELECTIONS

Such a multi-faceted and sophisticated blitz (e.g., support for preferred candidates, slander against opponents, media manipulation, internet trolls, cyberattacks, and other interference tactics) has troubled democratic elections across the world. In fact, the United States could have looked toward NATO partner Bulgaria's elections in 2015 and 2016 as a warning of the potential danger to come in its own election cycle. On the day of its local elections and referendum on future electronic voting in 2015, the networks of Bulgaria's Central Elections Commission and various government ministries were besieged by a DDoS attack.[238] Such assaults are commonly used to overwhelm sites and servers with automated connection requests to the point of a catastrophic crash. The Central Election Commission announced that it was confident that the integrity of the results remained intact despite the attack, but subsequent U.S. government and private sector analysis of the attack

---

[235] Cynthia McFadden, William Arkin, and Kevin Monahan, "Russians Penetrated U.S. Voter Systems, Top Official Says," NBC News, February 7, 2018, https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721; Ellen Nakashima, "Russian Hackers Targeted Arizona Election System," *Washington Post*, July 29, 2016, https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html.

[236] Department of Justice, Indictment: United States of America v. Viktor Borisovich Netyksho.

[237] *Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts against Election Infrastructure with Additional Views*, S. Rep. 116-XX, Senate, 116th Cong., 1st sess., 2018, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

[238] Novinite Sofia News Agency, "Huge Hack Attack on Bulgaria Election Authorities 'Not to Affect Vote Count.'"

Page 3151 of 3957

accusing GRU as the culprit raised alarms about the extent of Russian influence campaigns.[239]

Ahead of the country's 2016 presidential election, multiple Bulgarian government officials reported that its national security service had intercepted an election strategy dossier produced by a Kremlin-linked Russian think tank and prepared for Bulgaria's Socialist Party.[240] Delivered by a Russian official sanctioned by the United States for spying, the document proposed the distribution of false polling data favoring the party's candidate and anti-NATO position to help the party win.[241] Polls predicting the Socialist Party candidate's victory and alleging that a majority of Bulgarians trusted Russia more than NATO had indeed mysteriously surfaced during the election campaign season.[242] The poll had been conducted by a mysterious Bulgarian company called Gallup International, which bore no relation to and was the target of a name-infringement lawsuit from renowned U.S.-based polling company Gallup Incorporated.[243] Per former Bulgarian ambassador to Russia, Ilian Vassilev, regarding the anti-NATO Gallup International report:

> This wrapped-in-secrecy poll had no details on methodology nor funding sources. Russian media strategists and their Bulgarian proxies used the Western name to fool people about its credibility and spread their message.[244]

Along with this assessment, Vassilev published a warning about Russia's use of RT, Sputnik, and various proxies to sway the Bulgarian vote and ultimately drive the nation out

---

[239] Gordon Corera, "Bulgaria Warns of Russian Attempts to Divide Europe," BBC News, sec. Europe, November 4, 2016, https://www.bbc.com/news/world-europe-37867591.

[240] Joe Parkinson and Georgi Kantchev, "Document: Russia Uses Rigged Polls, Fake News to Sway Foreign Elections," *Wall Street Journal*, sec. World, March 23, 2017, https://www.wsj.com/articles/how-does-russia-meddle-in-elections-look-at-bulgaria-1490282352.

[241] Parkinson and Kantchev.

[242] Parkinson and Kantchev.

[243] Parkinson and Kantchev.

[244] Ilian Vassilev, "Thinking the Unthinkable—Bulgaria's Silent Exit from NATO and the EU," *Bulgaria Analytica* (blog), February 28, 2017, https://bulgariaanalytica.org/en/2017/02/28/thinking-the-unthinkable-bulgarias-silent-exit-from-nato-and-the-eu/.

Page 3152 of 3957

of NATO.[245] In the end, the Socialist Party's preferred candidate, Rumen Radev, won the election and became president.[246]

The attack on Bulgaria's elections system was not unprecedented, as Russia had allegedly attempted the same in Ukraine one year prior during its 2014 presidential and parliamentary elections. Days before the election, self-proclaimed Russian "hacktivists" hacked the Central Election Commission's website in an effort to publish false information declaring a well-known far-right extremist as the election winner.[247] Not long after this came to light, the head of Ukraine's SBU security service announced two days before the election that a virus meant to destroy election results had been detected and removed from its Central Election Center services.[248]

At the same time Bulgaria and the United States endured Russian election interference campaigns, yet another NATO country found itself in the Kremlin's crosshairs. French National Rally candidate Marine Le Pen's 2016–2017 presidential campaign benefited from $13 million in loans from a Moscow bank, likely approved and quite possibly directed by the Kremlin.[249] This substantial funding was seen as vital to keeping the once-fringe candidate's campaign afloat, and helped her achieve a shocking second-place finish. During a highly publicized meeting between Le Pen and Putin ahead of the election, the Russian leader appeared to be trying hard not to smile as he ominously stated that "of course" Russia did not want to meddle in the French election.[250] Such outside support has been critical to National Rally's survival as French and other Western banks

---

[245] Vassilev.

[246] Reuters Staff, "Socialist Ally Rumen Radev Wins Bulgaria Presidency: Exit Polls," *Reuters*, November 13, 2016, https://www.reuters.com/article/us-bulgaria-election-exitpoll-idUSKBN1380Q7.

[247] Andy Greenberg, "Russia's Cyberwar on Ukraine Is a Blueprint for What's to Come," Wired, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

[248] "SBU likviduvala virus, shcho mav znyshchyty rezul'taty vyboriv [SBU eliminates virus that was meant to destroy election results]," Ukrayins'ka Pravda [Ukrainian Truth], May 23, 2014, https://www.pravda.com.ua/news/2014/05/23/7026217/; Gorchinskaya, Rudenko and Schreiber, "Authorities: Hackers Foiled."

[249] At the time of the 2016–2017 election, National Rally was called "National Front." Henry Samuel, "Marine Le Pen's Links to Russia under U.S. Scrutiny," *The Telegraph*, December 21, 2016, http://www.telegraph.co.uk/news/2016/12/21/marine-le-pens-russian-links-us-scrutiny/.

[250] Gabriel Gatehouse, "Who's Funding France's Far Right?," BBC News, sec. Europe, April 3, 2017, http://www.bbc.com/news/world-europe-39478066.

had refused to finance a party seen by many as racist and xenophobic.[251] A BBC report citing hacked emails and conversations with multiple Le Pen associates heavily suggested prior clandestine meetings between Le Pen and Putin and detailed her intended role in legitimizing Russia's Crimea annexation.[252] It should be noted that financial support offered by Russia is often obscured through intermediaries for plausible deniability, and that support need not be explicitly monetary.[253] Hungary's Political Capital Policy Research and Consulting Institute opined in 2014 that in exchange for fealty to the Kremlin, parties are given "valuable professional, organizational and media assistance, i.e., access to networks and political know-how."[254]

During France's 2017 presidential election, Russia's state-run Sputnik news agency published false reports that François Fillon had overtaken Emmanuel Macron as Le Pen's strongest challenger.[255] At minimum, the ploy seemed geared to ensure that her opponent in a potential runoff round would be Filion—another Russia-friendly, NATO-criticizing candidate—rather than Kremlin skeptic Macron.[256] Russian foreign media relentlessly attacked and smeared Macron throughout France's election season with a wide variety of topics and tactics.[257] Sputnik and other Russian media outlets published baseless

---

[251] Paul Sonne, "A Russian Bank Gave Marine Le Pen's Party a Loan. Then Weird Things Began Happening," *Washington Post*, December 27, 2018, https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html.

[252] Gatehouse, "Who's Funding France's Far Right?"

[253] Political Capital Institute, *The Russian Connection*.

[254] Political Capital Institute.

[255] Richard Balmforth and Michael Rose, "French Polling Watchdog Warns over Russian News Agency's Election Report," *Reuters*, April 3, 2017, https://www.reuters.com/article/us-france-election-russia-idUSKBN1740JG.

[256] "France Warns Russia against Meddling in Presidential Election," Deutsche Welle, February 16, 2017, https://www.dw.com/en/france-warns-russia-against-meddling-in-presidential-election/a-37572358.

[257] Adam Plowright, "France and Macron Have Buried Allegations of Russian Meddling," *Washington Post*, May 23, 2018, https://www.washingtonpost.com/news/global-opinions/wp/2018/05/23/france-and-macron-have-buried-allegations-of-russian-meddling/.

accusations that Macron was homosexual, mentally ill, and financially supported by a mysterious and powerful "gay lobby."[258]

The Kremlin also repeated the hack-and-leak stunt it used against the Clinton campaign during its interference in France's presidential election, albeit with diminished success. Two days before the 2017 presidential election runoff between Le Pen and Macron, nine gigabytes of data stolen from the Macron campaign including 21,075 emails were posted to the internet and promoted on social media by a large network of automated accounts, as well as WikiLeaks.[259] Disturbingly, the stolen Macron emails were purportedly mixed with falsified documents attempting to frame him for fraud; a trick that seems difficult for readers to discern or investigators to prove, given the illicit nature of the genuine documents' theft and release.[260] Bolstering the theory that Russia had altered the emails, a report from the University of Toronto released that same month revealed similar tactics used by the GRU against journalist and Putin critic David Satter, whose stolen emails were deliberately modified in an effort to smear Putin critic Aleksei Navalny.[261] Such tactics represent a perhaps overlooked element of danger to hacked and stolen documents; they can be used as cover to add legitimacy to forgeries that thus put a digital twist on an age-old KGB dezinformatsiya trick.

Possibly due to its mistimed release within the mandatory media blackout period of French eve-of-voting "election silence" laws, or perhaps because voters had already made

---

[258] "Ex-French Economy Minister Macron Could Be 'U.S. Agent' Lobbying Banks' Interests," *Sputnik International*, February 4, 2017, https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq/; Darya Aslamova, "Vybory vo Franci: Oni zasluzhili Macrona [Elections in France: They deserve Macron]," Komsomolskaya Pravda [Komsomol Truth], May 7, 2017, https://www.kp.ru/daily/26676.7/3698458/.

[259] Eric Auchard and Bate Felix, "French Candidate Macron Claims Massive Hack as Emails Leaked," *Reuters*, May 6, 2017, https://www.reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ; Richard Lough, Eric Auchard, and Ingrid Melander, "WikiLeaks Publishes Searchable Archive of Macron Campaign Emails," *Reuters*, July 31, 2017, https://www.reuters.com/article/us-france-politics-wikileaks-idUSKBN1AG1TZ.

[260] Rachel Donadio, "Why the Macron Hacking Attack Landed with a Thud in France," *New York Times*, sec. World, December 22, 2017, https://www.nytimes.com/2017/05/08/world/europe/macron-hacking-attack-france.html; Andy Greenberg, "Hacked Macron Emails Leak Online Ahead of French Presidential Runoff Election," Wired, May 5, 2017, https://www.wired.com/2017/05/macron-email-hack-french-election/.

[261] Brewster, "Russian 'Fancy Bear' Hackers Tainted Their Huge Leaks with Fake Data."

up their minds or were wary of email leaks after the recent Clinton hacking debacle, the episode seemingly had no major effect on the election result.[262] Though Russia denied responsibility, an analysis conducted by cybersecurity company Flashpoint attributed the attack to the GRU.[263] This finding supported an earlier Trend Micro report warning of Russian phishing attempts against Macron and his campaign.[264] On October 19, 2020, the U.S. Justice Department unsealed indictments against six GRU officers for their roles in "spearphishing" hacks against Macron and his party, along with other cyberattacks including NotPetya, the Ukraine cyber grid disruption, and a 2018 Winter Olympic Games cyberintrusion.[265]

These European countries' recent experiences with Russian election interference contain many of the same elements the United States was subjected to in 2014: disinformation, media manipulation, leak of stolen documents, forgeries, support for fringe candidates, and even attacks on election infrastructure. The diversity, frequency, and broad range of Kremlin efforts to intervene in its rivals' electoral affairs, along with the obvious harm manipulating the outcome of a country's democratic process can cause in the short and long term, illustrate that election interference may be the most potent and dangerous of Russia's covert influence tactics.

---

[262] Michelle Caruso-Cabrera, "France's Election Laws Mean near Silence on Massive Campaign Hack," CNBC News, May 6, 2017, https://www.cnbc.com/2017/05/06/frances-election-laws-mean-near-silence-on-massive-campaign-hack.html.

[263] Patrick Howell O'Neill, "Researchers Link Macron Hack to APT28 with 'Moderate Confidence," Cyberscoop, May 11, 2017, https://www.cyberscoop.com/researchers-link-macron-hack-to-apt28-with-moderate-confidence/.

[264] Felix Hacquebord, "Two Years of Pawn Storm: Examining an Increasingly Relevant Threat," Trend Micro TrendLabs, April 25, 2017, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm.

[265] *Department of Justice, Indictment: United States of America v. Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valaryevich Ochichenko, and Petr Nikolayevich Pliskin, Defendants* (Washington, DC: Department of Justice, 2020), https://int.nyt.com/data/documenttools/russian-cyberattacks-indictments/144ea8fe6680730c/full.pdf.

Page 3156 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 3157 of 3957

IV. FALLOUT AND VULNERABILITIES

This chapter explores a range of vulnerabilities and possible consequences faced by the U.S. should such attacks on elections succeed. To do so, this chapter explores several examples of fallout from Russia's efforts against the 2016 U.S. presidential election.

Though the Special Counsel finding and myriad intelligence reports definitively point to deliberate Russian interference in the 2016 U.S. election in support of a Trump victory, assessing the operation's effect on the outcome is necessarily an inexact science. While it is impossible to know, for example, how many voters would have chosen Clinton rather than Trump, Stein, or another option had it not been for encounters with Russian disinformation or the leaked email controversy specifically, it is not difficult to trace clear examples of damage to the Kremlin plot.

One obvious consequence of Russian interference in the 2016 U.S. election was reputational harm for candidates and their surrogates. For one, the email leaks had a demonstrable effect on the DNC when Wasserman Schultz resigned as chairwoman due to the content of her exposed conversations.[266] Media coverage and public perception in light of the strategically damaging leaks was undeniably negative for Clinton as she sought to win over undecided and reluctant voters. Trump, his family, and his campaign team all clearly viewed coverage of the Trump Tower meeting and other allegations of the campaign's ties to Russia as unpalatable, given their efforts to deny accusations and shut down the Special Counsel investigation. Jill Stein, too, bristled at accusations that her campaign had been supported by Russia once the investigations of interference triggered additional scrutiny of her warm relationship with RT.[267] It is clear, however, that reputational harm from the fallout of Moscow's meddling extended far beyond that of

[266] Anne Gearan, Philip Rucker, and Abby Phillip, "DNC Chairwoman Will Resign in Aftermath of Committee Email Controversy," *Washington Post*, sec. Politics, July 24, 2016, https://www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html.

[267] Martin Johnson, "Jill Stein: 'I Am Not a Russian Spy," The Hill, October 19, 2019, https://thehill.com/homenews/campaign/466594-jill-stein-i-am-not-a-russian-spy.

Page 3158 of 3957

political candidates and their campaign associates, likely to an extent that surprised even the leaders of the malign influence operations.

Another example of how the ever-present possibility of Moscow meddling can lead to confusion and controversy occurred in October 2019, when a quote by Hillary Clinton warning that Russia was likely "grooming" a third-party disrupter like Stein to help defeat the 2020 Democratic candidate made waves in the media.[268] Many U.S. news outlets reported that Clinton had accused 2020 Democratic presidential candidate Tulsi Gabbard of being a Russian asset, which then prompted a public feud between the two that led other 2020 Democratic candidates to take sides amid a small rift within the party.[269] Such organizations as the Alliance for Securing Democracy reported that Gabbard received outsized coverage on RT and that "bot-like activity" periodically boosts her profile on social media.[270] This finding raised several alarming possibilities, including that Russia could have either been boosting Gabbard as Clinton insinuated, or that it could be framing her as a distraction or a form of campaign-sinking slander. Even if the accusation could be proved false, this incident could nevertheless illustrate how the specter of Russian interference can be weaponized against a candidate and contribute to division without Russia even having to take action. This incident—and its knock-on effects—were only possible because of successful Russian influence operations and the effect it had on U.S. voters' perceptions.

---

[268] Glenn Kessler, "Tulsi Gabbard Misquotes Hillary Clinton's Jab at Her," *Washington Post*, October 31, 2019, https://www.washingtonpost.com/politics/2019/10/31/tulsi-gabbard-misquotes-hillary-clintons-jab-her/.

[269] Nicholas Wu, "What's the Dispute between Hillary Clinton and Tulsi Gabbard about?," *USA Today*, October 24, 2019, https://www.usatoday.com/story/news/politics/elections/2019/10/24/what-feud-between-tulsi-gabbard-and-hillary-clinton-about/4082268002/; Benjamin Fearnow, "Timeline of the Tulsi Gabbard, Hillary Clinton Spat: Why the Two Democrats Fought," *Newsweek*, November 20, 2019, https://www.newsweek.com/timeline-tulsi-gabbard-hillary-clinton-russian-asset-spat-why-two-democrats-fought-1473084.

[270] Lisa Lerer, "What, Exactly, Is Tulsi Gabbard up to?," *New York Times*, sec. U.S., October 12, 2019, https://www.nytimes.com/2019/10/12/us/politics/tulsi-gabbard.html.

Notably, Gabbard, Stein, and Trump have all publicly labeled criticism of their seemingly pro-Russia policies and associations as "McCarthyist."[271] McCarthyism describes a period of time in which the U.S. government subjected thousands of its own citizens to loyalty tests, harsh investigations, and accusations of treason in service of the Soviet Union.[272] Though Soviet espionage undeniably posed a threat at the time, this period is generally regarded negatively due to government overreach, baseless political persecutions, and exaggerated fears of communist influence.[273] Today, RT journalists repeatedly publish articles decrying "McCarthyism's return" in an effort to protest mounting restrictions against their operation in Western countries.[274] Such disingenuous protests are reminiscent of Kim Philby, the notorious London *Times* journalist and Soviet double agent within British intelligence services who provided Moscow with top-secret communications between U.S. and British operatives in the CIA and MI6. Philby claimed to be an innocent victim of McCarthyist slander when his cover began to be blown, and used the success of his disingenuous protest to prolong his espionage for a time.[275] Though erroneously exonerated of the accusations, Philby did resign from his position at MI6 amid ongoing speculation; though he continued work as a journalist, his value to the Kremlin

[271] Jill Stein, "Hillary Clinton Called Me a 'Russian Asset.' The Establishment Is Losing Its Grip," *The Guardian*, sec. Opinion, October 24, 2019, https://www.theguardian.com/commentisfree/2019/oct/24/hillary-clinton-called-me-a-russian-asset-the-establishment-is-losing-their-grip; Tulsi Gabbard, "Stand with Tulsi against Clinton's new McCarthyism and warmongering," Facebook, October 21, 2019, https://www.facebook.com/TulsiGabbard/posts/2622169801172756; David Jackson and Kevin Johnson, "President Trump Accuses Special Counsel Robert Mueller of McCarthyism, Trying to Coerce Witnesses," *USA Today*, November 28, 2018, https://www.usatoday.com/story/news/politics/2018/11/28/donald-trump-robert-mueller-mccarthy/2135863002/.

[272] Ellen Schrecker, "McCarthyism: Political Repression and the Fear of Communism," *Social Research* 71, no. 4 (December 1, 2004): 1041–86.

[273] Schrecker.

[274] Bryan McDonald, "McCarthyism 2.0: Real Skill of U.S. 'Disinformation Experts' Is Spreading Disinformation," RT International, August 1, 2018, https://www.rt.com/op-ed/434846-twitter-russia-disinformation-mccarthyism/; Earl Rasmussen, "How the U.S. Stifles Free Speech: Reviving McCarthyism & Nurturing Orwellian Society," RT International, May 10, 2018, https://www.rt.com/op-ed/426351-us-free-speech-mccarthyism/.

[275] Andrew and Mitrokhin, *The Sword and the Shield*, 160.

was greatly diminished. Eventually outed by a Soviet defector, Philby ultimately defected himself, but received a cooler-than-anticipated reception in the Soviet Union.[276]

Ultimately, the 2016 U.S. election influence campaign paid more dividends than even Russia likely expected. One likely unplanned windfall of the DNC and Clinton campaign hacking operation for Moscow is that the U.S. response to the attack managed to entangle the FBI, long a target of Soviet *dezinformatsiya* smear campaigns, in extreme controversy that tarnished its reputation among a significant portion of the U.S. population. The Clinton email leaks added fuel to an ongoing, unrelated scandal regarding her improper use of a private email server for official business during her tenure as Secretary of State, as it hinted the possibility of security breaches with classified information.[277] This development put FBI director James Comey in a bind as he struggled to decide what the bureau should and should not disclose to the public about both the private server investigation and the DNC hack investigation, because he feared any disclosures could imply or reveal improper conduct by a presidential candidate and thus potentially impact voters' choices.[278] Comey's decisions on these matters led many Democrats to accuse him

[276] Andrew and Mitrokhin, 415.

[277] Washington Post Staff, "Read the Full Testimony of FBI Director James Comey in Which He Discusses Clinton Email Investigation," *Washington Post*, May 3, 2017, https://www.washingtonpost.com/news/post-politics/wp/2017/05/03/read-the-full-testimony-of-fbi-director-james-comey-in-which-he-discusses-clinton-email-investigation/; Isikoff and Corn, *Russian Roulette*.

[278] Washington Post Staff.

of demonstrating undue bias against Clinton and deliberately swinging the election for Trump.[279]

Notably, Comey's decisions were said to have been influenced by another facet of Russian interference and disinformation: the FBI's discovery of a suspicious Russian intelligence document alleging that Attorney General Loretta Lynch had pre-emptively reassured Clinton's team that the server investigation would tread softly.[280] This document involved purported but possibly fabricated emails involving Lynch and Wasserman Schultz.[281] Though the bureau's own analysis concluded that the report was unreliable and possibly deliberately manufactured to fluster U.S. intelligence agencies, its existence helped persuade Comey that a public explanation was needed as a defensive measure against future accusations of corruption.[282]

Unfortunately, for the FBI, Trump, along with many of his supporters, came to view Comey as biased against *him* due to the bureau's further investigation into Russian interference after the election, as it implied that Trump's narrow victory might have been

---

[279] James B. Comey, "Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System," Press Release, Federal Bureau of Investigation, July 5, 2016, https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system; Eamon Javers, "FBI's Comey Opposed Naming Russians, Citing Election Timing: Source," CNBC News, October 31, 2016, https://www.cnbc.com/2016/10/31/fbis-comey-opposed-naming-russians-citing-election-timing-source.html; James B. Comey, *A Higher Loyalty: Truth, Lies, and Leadership*, 1st ed. (New York: Flatiron Books, 2018); Joseph Tanfani, "Comey Strongly Defends Decision to Reopen FBI Probe into Clinton Emails 11 Days before the Election," *Los Angeles Times*, May 3, 2017, https://www.latimes.com/politics/washington/la-na-essential-washington-updates-comey-says-the-late-disclosure-of-1493824301-htmlstory.html; Adrienne Shih, "FBI Director James Comey: 'You Can Call Us Wrong, But Don't Call Us Weasels," CNN, September 26, 2016, https://www.cnn.com/2016/09/28/politics/james-comey-congress-hearing-weasel/index.html; Eric Tucker and Chad Day, "Watchdog Finds Comey 'Insubordinate,' Not Biased in Clinton Email Investigation," *Chicago Tribune*, June 14, 2018, https://www.chicagotribune.com/news/nationworld/ct-clinton-email-case-20180613-story.html.

[280] Karoun Demirjian and Devlin Barrett, "How a Dubious Russian Document Influenced the FBI's Handling of the Clinton Probe," *Washington Post*, May 24, 2017, https://www.washingtonpost.com/world/national-security/how-a-dubious-russian-document-influenced-the-fbis-handling-of-the-clinton-probe/2017/05/24/f375c07c-3a95-11e7-9e48-c4f199710b69_story.html.

[281] Demirjian and Barrett.

[282] Demirjian and Barrett.

Page 3162 of 3957

assisted by a top rival state.[283] Trump also complained throughout his presidency that Comey and a cabal of "deep state" actors within the DOJ and FBI had engaged in illegal spying activity against his campaign to prevent or end his presidency.[284] Post-election polling indicates that the bureau experienced a loss of trust from both Congress and a significant portion of the U.S. population immediately following these episodes.[285] A 2018 poll conducted by Penn State University found that since this episode, voters who lean Republican or independent trusted the FBI less than half the time, and that less than half of Americans believed that "most FBI agents enforce the law fairly."[286]

Other U.S. government intelligence agencies suffered from the fallout from Russia's election interference as well. The DNI released a declassified joint CIA, National Security Agency (NSA), and FBI report two months after the 2016 election, which unequivocally accused the Kremlin of meddling in the election to Trump's benefit:

> Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump… Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him…Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by

---

[283] Eric Tucker, "The Comey Firing, As Retold by the Mueller Report," *Associated Press*, sec. Criminal investigations, April 23, 2019, https://apnews.com/article/4ff1ecb621884a728b25e62661257ef0; Mary Claire Jalonick, "Comey Faces off with GOP over Clinton Emails, Alleged Bias," *Associated Press*, December 7, 2018, https://apnews.com/article/734284dd1aa746c19bf209770ae1ce54.

[284] Eric Tucker and Jonathan Lemire, "Trump, GOP Launch Broad Attack on Russia Probe Foundations," *Associated Press*, May 13, 2020, https://apnews.com/article/ebcd45c5d89ac3cf8cc61ed3d6e1ac1a; Patricia Zengerle and Warren Strobel, "FBI Head Denies Trump Wiretap Claim, Confirms Russia Election Probe," *Reuters*, March 20, 2017, https://www.reuters.com/article/usa-trump-russia-idUSL2N1GX1L8.

[285] Douglas M. Charles, "Trump and Nunes Torch Tradition of Trust between Congress and FBI," The Conversation, February 3, 2018, http://theconversation.com/trump-and-nunes-torch-tradition-of-trust-between-congress-and-fbi-91140; Kyle Cheney, "Comey Offers to Testify in Public about GOP's FBI Bias Claims," *Politico*, October 1, 2018, https://politi.co/2DK4Aj9.

[286] Michael Berkman and Eric Plutzer, "Mood of the Nation Poll: Republicans No Longer Trust the FBI," *The McCourtney Institute for Democracy*, February 20, 2018, 8.

Page 3163 of 3957

> Russian Government agencies, state-funded media, third party intermediaries, and paid social media users or "trolls."[287]

Upset that it undermined the degree or legitimacy of his victory, Trump forcefully rejected the report's finding even before it was published.[288] In December 2016, he issued a derisive rebuttal to the CIA's reported findings that starkly undermined his own intelligence agency's credibility, "These are the same people that said Saddam Hussein had weapons of mass destruction."[289]

Siding with a principal U.S. adversary over his own intelligence community, Trump repeatedly insisted that he believed Putin's denials about responsibility for the hack.[290] On multiple occasions, Trump also suggested that the operation could have been the work of China, other countries, a morbidly obese domestic hacker, or even the DNC itself as a distraction from Clinton's private server scandal.[291] The public spat touched off lasting friction between Trump and the intelligence agencies, particularly once Trump expressed public disdain for the Special Counsel investigation and sought a one-on-one meeting with Putin without alerting or consulting the DNI.[292]

The outgoing administration struggled to respond appropriately to the Clinton email release operation as it unfolded. President Obama initially chose to tread lightly and sought

---

[287] Office of the Director of National Intelligence, *Assessing Russian Activities*.

[288] David Nakamura and Greg Miller, "Trump, CIA on Collision Course over Russia's Role in U.S. Election," *Washington Post*, December 10, 2016, https://www.washingtonpost.com/politics/trump-cia-on-collision-course-over-russias-role-in-us-election/2016/12/10/ad01556c-bf01-11e6-91ee-1adddfe36cbe_story.html.

[289] Nakamura and Miller.

[290] Erica R. Hendry, "The Many Different Ways Trump Has Described Putin and Russian Election Interference," PBS NewsHour, July 16, 2018, https://www.pbs.org/newshour/politics/the-many-different-ways-trump-has-described-putin-and-russian-election-interference.

[291] Krishnadev Calamur, "Some of the People Trump Has Blamed for Russia's 2016 Election Hack," *The Atlantic*, July 18, 2018, https://www.theatlantic.com/international/archive/2018/07/trump-russia-hack/565445/.

[292] Matthew Rosenberg, "U.S. Intelligence Community Reacts with Fury to Trump's Rebuke," *New York Times*, sec. U.S., July 17, 2018, https://www.nytimes.com/2018/07/16/us/politics/us-intel-community-reacts-with-fury-to-trumps-rebuke.html; David Priess, "The 'Time of Troubles' Is Back for America's Spies," *Foreign Policy*, July 26, 2018, https://foreignpolicy.com/2018/07/26/the-time-of-troubles-is-back-for-americas-intelligence-community/.

Page 3164 of 3957

to avoid appearing to aid Clinton's chances of victory.[293] Later deciding to alert the public of Russia's hand in election manipulation, Obama found himself thwarted by Mitch McConnell, the Republican Senate Majority Leader.[294] McConnell espoused skepticism of the available intelligence and refused to cooperate in a joint warning about election interference.[295] DHS Secretary Jeh Johnson's offer to provide state election officials with federal cybersecurity assistance was similarly thwarted by incidents such as Georgia Secretary of State Brian Kemp accusing the Obama administration of "a politically calculated move" and refusing to cooperate lest the Democratic administration seek to use the situation to aid its party's candidates in some way.[296]

The Obama administration's eventual punitive response—the expulsion of 35 Russian diplomats and the closure of two Russian embassy compounds—resulted in further collateral damage to the credibility of certain U.S. government officials when curiosity regarding Russia's uncharacteristic restraint from retaliation later ensnared two members of Trump's cabinet in scandals.[297] Mike Flynn, Trump's National Security Advisor, was found to have engaged in, and lied to the FBI and administration officials about, undisclosed conversations with Russia's ambassador to the United States before Trump took office, along with other omissions such as failing to report a $45,000 payment for his speech at the RT gala referenced earlier.[298] These findings led to Flynn's swift departure from Trump's cabinet, which sparked investigations surrounding his alleged service as an

---

[293] Greg Miller, Ellen Nakashima, and Adam Entous, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault," *Washington Post*, June 23, 2017. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/; Isikoff and Corn, *Russian Roulette*.

[294] Miller, Nakashima, and Entous.

[295] Miller, Nakashima, and Entous.

[296] Miller, Nakashima, and Entous.

[297] Devlin Barrett and Greg Miller, "Transcripts of Calls between Flynn, Russian Diplomat Show They Discussed Sanctions," *Washington Post*, May 29, 2020, https://www.washingtonpost.com/national-security/transcripts-of-calls-between-flynn-russian-diplomat-show-they-discussed-sanctions/2020/05/29/cc3d29c6-a1f0-11ea-b5c9-570a91917d8d_story.html.

[298] Barrett and Miller.

undisclosed foreign agent and potential violations of the U.S. Constitution's Foreign Emoluments Clause, and eventually drew indictments and a guilty plea from Flynn.[299]

Attorney General Jeff Sessions was also embroiled in controversy over his own initially undisclosed contacts with the Russian ambassador prior to Trump's inauguration, when Sessions was a U.S. senator.[300] Amid calls for his resignation from Senate Democrats who felt he had misled them by failing to inform them of these contacts, Sessions swiftly recused himself from any DOJ investigations regarding Russian election interference.[301] Sessions' recusal led to the appointment of a Special Counsel investigation led by former FBI Director Robert Mueller, which infuriated Trump and ultimately led to Sessions's forced departure.[302]

Furious at accusations that his campaign had colluded with Russia, Trump sought to discredit the Special Counsel investigation throughout its duration by decrying it as a witch hunt and accusing Mueller and his team of being "angry Democrats" and "Trump haters" with a partisan agenda to sabotage him.[303] The investigation ultimately led to, among other things, 14 referrals of criminal matters to the DOJ, 37 indictments, and a report finding "numerous links between the Russian government and the Trump campaign"

---

[299] "Cummings Releases New Documents Confirming That Flynn Received Funds from Instrument of Russian Government," House Committee on Oversight and Reform, March 16, 2017, https://oversight.house.gov/news/press-releases/cummings-releases-new-documents-confirming-that-flynn-received-funds-from; *Indictment: United States of America v. Michael T. Flynn, Defendant*, Case 1:17-cr-00232-RC 1 (D.D.C. 2017), https://www.justice.gov/file/1015126/download.

[300] Isikoff and Corn, *Russian Roulette*; Michael A. Memoli, "Trump National Security Advisor Michael Flynn Resigns over Contacts with Russia," *Los Angeles Times*, February 13, 2017, https://www.latimes.com/politics/la-na-pol-trump-flynn-20170213-story.html.

[301] Mark Landler and Eric Lichtblau, "Jeff Sessions Recuses Himself from Russia Inquiry," *New York Times*, sec. U.S., March 2, 2017, https://www.nytimes.com/2017/03/02/us/politics/jeff-sessions-russia-trump-investigation-democrats.html.

[302] Office of Public Affairs, "Appointment of Special Counsel," Department of Justice, May 17, 2017, https://www.justice.gov/opa/pr/appointment-special-counsel; Peter Baker, Katie Benner, and Michael D. Shear, "Jeff Sessions Is Forced Out as Attorney General as Trump Installs Loyalist," *New York Times*, sec. U.S., November 7, 2018, https://www.nytimes.com/2018/11/07/us/politics/sessions-resigns.html.

[303] Rachel Frazin, "Trump Knocks Mueller over Russia Probe: '18 Angry Democrats' and '0 Collusion," The Hill, April 19, 2019, https://thehill.com/homenews/administration/439855-trump-knocks-mueller-over-russia-probe-18-angry-democrats-and-0.

Page 3166 of 3957

along with evidence of "sweeping and systemic" Kremlin election interference.[304] William Barr, Sessions' eventual successor as Attorney General, generated controversy and questions of credibility by issuing a summary letter of the Special Counsel report to the congressional Judiciary Committees in March 2019 that appeared to gloss over some of the report's findings.[305] This report was assailed by many legal analysts, journalists, and Special Counsel members, including Mueller himself, as an inadequate or even deliberately misleading portrayal of the investigation's findings. The ensuing controversy resulted in further accusations of DOJ partisan corruption, and led to more than 2,000 former DOJ employees publicly calling for Barr's resignation, as well as 27 members of the DC Bar requesting sanctions against him in a formal disciplinary complaint.[306] In aggregate, the nation's top law enforcement, justice administration, and intelligence bodies weathered a torrent of attacks on their credibility in the course of investigating Russian interference in the 2016 U.S. presidential election. Historically low faith in the DOJ, FBI, and intelligence community is an indisputable boon for future Russian election interference attempts.

As with the AIDS and Kennedy assassination *dezinformatsiya* episodes, Russia could not have predicted or controlled the aftermath and consequences of their initial cyberattack against the DNC and social media trolling campaign, but can only be delighted by the outsized and lingering results. As it stands, the fallout of a hacking and

---

[304] Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Election Vol. I* (Washington, DC: Department of Justice, 2019), 1–5.

[305] Mark Mazzetti and Michael S. Schmidt, "Mueller Objected to Barr's Description of Russia Investigation's Findings on Trump," *New York Times*, sec. U.S., April 30, 2019, https://www.nytimes.com/2019/04/30/us/politics/mueller-barr.html.

[306] Gershon (Gary) Ratner et al., "Ethics Complaint Re: Professional Responsibility Investigation of William P. Barr," Lawyers Defending American Democracy, July 23, 2020, https://lawyersdefendingdemocracy.org/reprofessional-responsibility-investigation-of-william-p-barr/; "Open Letter Supporting the 100,000 Lawyers, Agents, and Staff Members of the U. S. Department of Justice," *Lawyers Defending American Democracy* (blog), accessed October 19, 2020, https://lawyersdefendingdemocracy.org/open-letter-supporting-the-us-doj/; Savannah Behrmann and Kristine Phillips, "More than 2,000 Ex-DOJ Employees Call for Attorney General Barr's Resignation," *USA Today*, February 17, 2020, https://www.usatoday.com/story/news/politics/2020/02/16/william-barr-doj-alumnus-call-ag-resign/4779721002/; Dartunorro Clark et al., "All Four Roger Stone Prosecutors Resign from Case after DOJ Backpedals on Sentencing Recommendation," NBC News, February 11, 2020, https://www.nbcnews.com/politics/politics-news/doj-backpedalling-sentencing-recommendation-trump-ally-roger-stone-n1134961; Erik Larson, "Flynn Prosecutor Steps Down as Case Is Reportedly Being Dropped," *Bloomberg*, May 7, 2020, https://www.bloomberg.com/news/articles/2020-05-07/flynn-prosecutor-van-grack-steps-down-from-criminal-case.

Page 3167 of 3957

disinformation operation perpetrated by the Russian government helped induce a staggering amount of damage to a variety of targets. These include but are not limited to the following:

- undermining Clinton's election campaign and damaging her prospects of victory
- sowing lasting discord within the DNC
- alienating and enraging potential left-leaning voters who had favored Sanders
- setting in motion multiple events resulting in distrust for the FBI and DOJ and the ruination of prominent officials' careers
- provoking lasting animosity between Trump and the U.S. intelligence community
- creating legal and political headaches along with embarrassing distractions for Trump, his children, and associates
- spurring the firing and criminal prosecution of the National Security Advisor
- leaving a large number of U.S. citizens believing their leader conspired with a major U.S. foe to take power

The degree of damage to the credibility of U.S. government leaders and institutions affected by Russia's 2016 interference campaign is varied and difficult to quantify, but it is undeniable that some harm was sustained; and worryingly, could occur again. Even where evidence of Kremlin interference is elusive, the specter of such attacks hangs over subsequent elections and stokes long-term damage in voters' faith that elections are secure and free of outside tampering.

To wit, a minor incident in the 2020 U.S. presidential election offered a warning that the specter of Russian interference remains, and is still capable of inflicting damage

Page 3168 of 3957

on the nation and its leaders. With early voting already underway, *The New York Post* controversially published a trove of emails allegedly sent to and from the son of Democratic candidate Joe Biden.[307] Many media outlets and analysts investigating the story identified significant questions about its veracity, including speculation that suspected and indicted Russian influence agents had provided the material to a U.S. intermediary.[308] Within days, reports emerged that an FBI investigation had been launched regarding whether the emails were hacked and doctored as part of a foreign disinformation campaign.[309] Soon after, the DNI, John Ratcliffe, publicly denied the ongoing investigation and declared the story "not part of some Russian disinformation campaign" and excoriated House Permanent Select Committee on Intelligence chairman Adam Schiff for publicly linking the story to a Russian disinformation plot.[310] Notably, Facebook and Twitter both took immediate steps to limit posts linking to the *Post* article due to its questionable veracity, its use of possibly stolen private personal information, and its status as possible election-related disinformation; decisions that Trump campaign officials immediately decried as undue election interference by the social media titans.[311] While this incident does not appear to have had a major impact on the election results, it illustrates the fact that either Russian interference or accusations thereof may be an ever-present facet of future elections and has the capacity to provoke questions of credibility for U.S. government officials tasked with securing elections and national interests.

---

[307] Emma-Jo Morris and Gabrielle Fonrouge, "Smoking-Gun Email Reveals How Hunter Biden Introduced Ukrainian Businessman to VP Dad," *New York Post*, October 14, 2020, https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/.

[308] Katie Robertson, "New York Post Published Hunter Biden Report Amid Newsroom Doubts," *The New York Times*, sec. Business, October 18, 2020, https://www.nytimes.com/2020/10/18/business/media/new-york-post-hunter-biden.html; Shane Harris et al., "White House Was Warned Giuliani Was Target of Russian Intelligence Operation to Feed Misinformation to Trump," *Washington Post*, October 15, 2020, https://www.washingtonpost.com/national-security/giuliani-biden-ukraine-russian-disinformation/2020/10/15/43158900-0ef5-11eb-b1e8-16b59b92b36d_story.html.

[309] Ken Dilanian, "Feds Examining Whether Alleged Hunter Biden Emails Are Linked to a Foreign Intel Operation," NBC News, October 15, 2020, https://www.nbcnews.com/politics/national-security/feds-examining-if-alleged-hunter-biden-emails-are-linked-foreign-n1243620.

[310] Olivia Beavers and Joe Concha, "Ratcliffe, Schiff Battle over Biden Emails, Politicized Intelligence," TheHill, October 19, 2020, https://thehill.com/policy/national-security/521712-ratcliffe-schiff-battle-over-biden-emails-politicized-intelligence.

[311] Roose, "Facebook and Twitter Dodge a 2016 Repeat, and Ignite a 2020 Firestorm."

Page 3169 of 3957

V. CONCLUSION

Investigative findings by bodies including the bipartisan Senate Intelligence Committee demonstrate unequivocally that Russia's preferred influence operation outcomes in the 2016 U.S. presidential election came to pass, potentially along with "victories" in other elections.[312] Much argument and investigation has ensued over the degree to which Kremlin meddling influenced such outcomes, but its presence and potential is virtually undeniable. With nearly a century of experience in covert influence techniques and plenty of practice trying to interfere in Western elections, Russia has many skills and tools, such as disinformation and cyberattacks with which to continue meddling in the democratic affairs of its rivals. The persistence of such decades-old Soviet-made myths as the Pentagon AIDS connection and Kennedy assassination conspiracies point to a sobering truth regarding Russia's modern disinformation campaigns: it is impossible to forecast the long-term effect a given Kremlin fabrication may have, but history strongly suggests that at least a few may potentially cause damage even after discovery and attribution. Unfortunately, Russia appears all too willing to continue stressing the system with a variety of techniques and targets.

Covert Kremlin operations may be capable of corrupting a political candidate, framing one to make it appear that they had, or reaping the paranoia-inducing fruits of prior influence campaigns even when not directly intervening in an incident. Examinations of Soviet precedent and recent Kremlin tactics in democratic campaigns reveal that true or fabricated rumors of corruption and election fraud, exploitation, and exacerbation of domestic civil tensions, and even promotion of secession movements and rebellion, loom as possible threats. Challenges to the legitimacy of some future elections are plausible, whether because of successful Russian interference or even a good faith or disingenuous inaccurate accusation of such. These accusations could even be bolstered by a variety of

[312] *Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia's Use of Social Media with Additional Views*, S. Rep. 116-XX, Senate, 116th Cong., 1st sess., 2018, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

Page 3170 of 3957

well-honed Kremlin tradecraft, such as the production or dissemination of genuine, doctored, or fabricated material designed to lend credence to allegations.

It is therefore critically important for intelligence communities, investigative bodies, and other experts to evaluate the Kremlin's capacity for future operations, as well as their possible response to less favorable outcomes in future campaigns. Russia has the motivation, the capability, and a century of experience preparing it for future interference in U.S. affairs, and denying them the prize of election-related chaos and ruination of the U.S. government and electoral systems' credibility should be a top priority for national and homeland security entities.

Page 3171 of 3957

LIST OF REFERENCES

Abramson, Alana, and Shushannah Walshe. “The 4 Most Damaging Emails from the DNC WikiLeaks Dump.” ABC News, July 25, 2016. https://abcnews.go.com/Politics/damaging-emails-dnc-wikileaks-dump/story?id=40852448.

Afisha [Poster]. “Russkiye Media Iznutri: Margarita Simonyan, Glavny Redaktor Russia Today [Russian Media from within: Margarita Simonyan, Editor-in-Chief of Russia Today],” October 18, 2011. https://daily.afisha.ru/archive/gorod/archive/ministry-of-truth-simonyan/.

Ahrens, Jan Martínez. “U.S. Senate Addresses Russian Interference in Catalonia on Social Media.” *El País*, November 3, 2017. https://elpais.com/elpais/2017/11/03/inenglish/1509707476_016214.html.

Alandete, David. “Russian Meddling Machine Sets Sights on Catalonia.” *El País*, September 28, 2017. https://elpais.com/elpais/2017/09/26/inenglish/1506413477_994601.html.

Allcott, Hunt, and Matthew Gentzkow. “Social Media and Fake News in the 2016 Election.” *Journal of Economic Perspectives* 31, no. 2 (February 16, 2017): 211–36. https://doi.org/10.1257/jep.31.2.211.

Alvarez, R. Michael, Thad E. Hall, and Susan D. Hyde, eds. *Election Fraud: Detecting and Deterring Electoral Manipulation*. Washington, DC: Brookings Institution Press, 2008.

Andrew, Christopher M., and Vasili N. Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books, 2000.

———. *The World Was Going Our Way: The KGB and the Battle for the Third World*. New York: Basic Books, 2005.

Applebaum, Anne. “How Stalin Hid Ukraine’s Famine from the World.” *The Atlantic*, October 13, 2017. https://www.theatlantic.com/international/archive/2017/10/red-famine-anne-applebaum-ukraine-soviet-union/542610/.Carynnyk.

Aslamova, Darya. “Vybory vo Franci: Oni zasluzhili Macrona [Elections in France: They deserve Macron].” Komsomolskaya Pravda [Komsomol Truth], May 7, 2017. https://www.kp.ru/daily/26676.7/3698458/.

Page 3172 of 3957

Auchard, Eric, and Bate Felix. “French Candidate Macron Claims Massive Hack as Emails Leaked.” *Reuters*, May 6, 2017. https://www.reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ.

Baker, Peter, Katie Benner, and Michael D. Shear. “Jeff Sessions Is Forced Out as Attorney General as Trump Installs Loyalist.” *New York Times*, sec. U.S., November 7, 2018. https://www.nytimes.com/2018/11/07/us/politics/sessions-resigns.html.

Balmforth, Richard, and Michael Rose. “French Polling Watchdog Warns over Russian News Agency’s Election Report.” *Reuters*, April 3, 2017. https://www.reuters.com/article/us-france-election-russia-idUSKBN1740JG.

Barrett, Devlin, and Greg Miller. “Transcripts of Calls between Flynn, Russian Diplomat Show They Discussed Sanctions.” *Washington Post*, May 29, 2020. https://www.washingtonpost.com/national-security/transcripts-of-calls-between-flynn-russian-diplomat-show-they-discussed-sanctions/2020/05/29/cc3d29c6-a1f0-11ea-b5c9-570a91917d8d_story.html.

BBC News. “Anger as German Ex-Chancellor Schroeder Heads up Rosneft Board.” Sec. Europe, September 29, 2017. https://www.bbc.com/news/world-europe-41447603.

———. “‘Russian Hackers’ behind TV Attack.” Sec. Europe, June 9, 2015. https://www.bbc.com/news/world-europe-33072034.

Beavers, Olivia, and Joe Concha. “Ratcliffe, Schiff Battle over Biden Emails, Politicized Intelligence.” The Hill, October 19, 2020. https://thehill.com/policy/national-security/521712-ratcliffe-schiff-battle-over-biden-emails-politicized-intelligence.

Behrmann, Savannah, and Kristine Phillips. “More than 2,000 Ex-DOJ Employees Call for Attorney General Barr’s Resignation.” *USA Today*, February 17, 2020. https://www.usatoday.com/story/news/politics/2020/02/16/william-barr-doj-alumnus-call-ag-resign/4779721002/.

Bennetts, Marc. “Fancy Bear, Voodoo Bear and Sandworm: Who Are the Russian Hackers?.” *The Times*, sec. News, October 4, 2018. https://www.thetimes.co.uk/article/cybertattak-fancy-bear-voodoo-bear-and-sandworm-who-are-the-russian-hackers-g5698hrwz.

Berkman, Michael, and Eric Plutzer. “Mood of the Nation Poll: Republicans No Longer Trust the FBI.” *The McCourtney Institute for Democracy*, February 20, 2018.

Beuth, Patrick, Kai Biermann, Martin Klingst, and Holger Stark. “Cyberattack on the Bundestag: Merkel and the Fancy Bear.” *Die Zeit*, sec. Digital, May 12, 2017. https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia#fancy-bear-cyber-attacks-info-2-tab.

Page 3173 of 3957

Blue, Violet. “What If Russian Voter Hacks Were Just Part of Its Facebook Ad Campaign?.” Engadget, October 6, 2017. https://www.engadget.com/2017-10-06-russian-voter-hacks-support-facebook-ad-campaign.html.

Bogart, Laura M., and Sheryl Thorburn. “Are HIV/AIDS Conspiracy Beliefs a Barrier to HIV Prevention among African Americans?.” *JAIDS Journal of Acquired Immune Deficiency Syndromes* 38, no. 2 (February 1, 2005): 213–218.

Boghardt, Thomas. “Soviet Bloc Intelligence and Its AIDS Disinformation Campaign.” *Studies in Intelligence* 53, no. 4 (December 1, 2009): 1–24.

Brewster, Thomas. “Russian ‘Fancy Bear’ Hackers Tainted Their Huge Leaks with Fake Data.” *Forbes*, May 26, 2017. https://www.forbes.com/sites/thomasbrewster/2017/05/26/russian-dnc-hackers-planted-leaks-with-fake-data/.

Brown, Heather, Emily Guskin, and Amy Mitchell. “Arab-American Media: Bringing News to a Diverse Community: The Role of Social Media in the Arab Uprisings.” Pew Research Center, November 28, 2012. http://www.journalism.org/2012/11/28/role-social-media-arab-uprisings/.

Bump, Phillip. “What We Know about the Trump Tower Meeting.” *Washington Post*, August 7, 2018. https://www.washingtonpost.com/news/politics/wp/2018/08/07/what-we-know-about-the-trump-tower-meeting/.

Bureau of Public Affairs. *Soviet ‘Active Measures’ Forgery, Disinformation, Political Operations*. Washington, DC: Department of State, 1981. https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf.

Calamur, Krishnadev. “Putin Says ‘Patriotic Hackers’ May Have Targeted U.S. Election.” *The Atlantic*, June 1, 2017. https://www.theatlantic.com/news/archive/2017/06/putin-russia-us-election/528825/.

———. “Some of the People Trump Has Blamed for Russia’s 2016 Election Hack.” *The Atlantic*, July 18, 2018. https://www.theatlantic.com/international/archive/2018/07/trump-russia-hack/565445/.

Caruso-Cabrera, Michelle. “France’s Election Laws Mean near Silence on Massive Campaign Hack.” CNBC News, May 6, 2017. https://www.cnbc.com/2017/05/06/frances-election-laws-mean-near-silence-on-massive-campaign-hack.html.

Page 3174 of 3957

Carynnyk, Marco. “The Famine the ‘Times’ Couldn’t Find.” *Commentary Magazine*, November 1, 1983.

Chait, Jonathan. “Trump Determined to Get Vaccine before Election, Overrules FDA Guidelines.” *New York Magazine: Intelligencer*, October 5, 2020. https://nymag.com/intelligencer/2020/10/trump-vaccine-overrules-fda-election-coronavirus-science.html.

Charles, Douglas M. “Trump and Nunes Torch Tradition of Trust between Congress and FBI.” The Conversation, February 3, 2018. http://theconversation.com/trump-and-nunes-torch-tradition-of-trust-between-congress-and-fbi-91140.

Chen, Adrian. “The Agency.” *New York Times*, sec. Magazine, June 2, 2015. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Cheney, Kyle. “Comey Offers to Testify in Public about GOP’s FBI Bias Claims.” *Politico*, October 1, 2018. https://politi.co/2DK4Aj9.

Christian, Joshua D. “Russian Cyber Operations to Destabilize NATO.” Master’s thesis, Naval Postgraduate School, 2020.

Clark, Dartunorro, Michael Kosnar, Dareh Gregorian, and Tom Winter. “All Four Roger Stone Prosecutors Resign from Case after DOJ Backpedals on Sentencing Recommendation.” NBC News, February 11, 2020. https://www.nbcnews.com/politics/politics-news/doj-backpedalling-sentencing-recommendation-trump-ally-roger-stone-n1134961.

Clarke, Richard. “Counterterrorism Expert Richard Clarke on Trump’s Relations with Intelligence Agencies.” NPR, February 17, 2017. http://www.npr.org/2017/02/17/515728608/counterterrorism-expert-richard-clarke-on-trumps-relations-with-intelligence-age.

Comey, James B. *A Higher Loyalty: Truth, Lies, and Leadership*. 1st ed. New York: Flatiron Books, 2018.

———. “Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton’s Use of a Personal E-Mail System.” Press Release, Federal Bureau of Investigation, July 5, 2016. https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system.

Conger, Kate, and Mike Isaac. “In Reversal, Twitter Is No Longer Blocking New York Post Article.” *New York Times*, sec. Technology, October 16, 2020. https://www.nytimes.com/2020/10/16/technology/twitter-new-york-post.html.

Conquest, Robert. *The Harvest of Sorrow: Soviet Collectivization and the Terror-Famine*. New York, NY: Oxford University Press, 1987.

Page 3175 of 3957

Corera, Gordon. “Bulgaria Warns of Russian Attempts to Divide Europe.” BBC News, sec. Europe, November 4, 2016. https://www.bbc.com/news/world-europe-37867591.

———. “How France’s TV5 Was Almost Destroyed by ‘Russian Hackers.’” BBC News, sec. Technology, October 10, 2016. https://www.bbc.com/news/technology-37590375.

Courtney Weaver, Kerin Hope, and Sam Jones. “Alarm Bells Ring over Syriza’s Russian Links.” *Financial Times*, January 28, 2015. https://www.ft.com/content/a87747de-a713-11e4-b6bd-00144feab7de.

Cull, Nicholas J., Vasily Gatov, Peter Pomerantsev, Anne Applebaum, and Alistair Shawcross. *Soviet Subversion, Disinformation and Propaganda: How the West Fought against It: An Analytic History, with Lessons for the Present*. London: London School of Economics and Political Science, 2017. https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf.

Cyberspace Solarium Commission. *Report*. Arlington, VA: Cyberspace Solarium Commission, 2020. https://www.solarium.gov/report.

de Borchgrave, Arnaud. “The KGB’s Bead on the Media.” *Washington Post*, April 14, 1981. https://www.washingtonpost.com/archive/politics/1981/04/14/the-kgbs-bead-on-the-media/a58625f1-6959-470b-8afe-15ed92949304/.

Dearstyne, Bruce W. “The Russians Tried Once before to Meddle in a U.S. Presidential Election.” History News Network: George Washington University Columbian College of Arts and Sciences, December 29, 2016. https://historynewsnetwork.org/article/164769.

Defense Intelligence Agency. *Russia Military Power: Building a Military to Support Great Power Aspirations*. Washington, DC: Defense Intelligence Agency, 2017. https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf?ver=2017-06-28-144235-937.

Demirjian, Karoun, and Devlin Barrett. “How a Dubious Russian Document Influenced the FBI’s Handling of the Clinton Probe.” *Washington Post*, May 24, 2017. https://www.washingtonpost.com/world/national-security/how-a-dubious-russian-document-influenced-the-fbis-handling-of-the-clinton-probe/2017/05/24/f375c07c-3a95-11e7-9e48-c4f199710b69_story.html.

Page 3176 of 3957

Department of Justice. *Indictment: United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morganchev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev, Defendants*. Washington, DC: Department of Justice, 2018. https://www.justice.gov/file/1080281/download.

———. *Indictment: United States of America v. Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valaryevich Ochichenko, and Petr Nikolayevich Pliskin, Defendants*. Washington, DC: Department of Justice, 2020. https://int.nyt.com/data/documenttools/russian-cyberattacks-indictments/144ea8fe6680730c/full.pdf.

Department of State. *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–1987*. Washington, DC: Department of State, 1987. Proquest.

Deutsche Welle. "France Warns Russia against Meddling in Presidential Election." February 16, 2017. https://www.dw.com/en/france-warns-russia-against-meddling-in-presidential-election/a-37572358.

Dewey, Caitlin. "Hunting for Paid Russian Trolls in the Washington Post Comments Section." *Washington Post*, June 4, 2014. https://www.washingtonpost.com/news/the-intersect/wp/2014/06/04/hunting-for-paid-russian-trolls-in-the-washington-post-comments-section/.

Dewey, Taylor, Juliane Kaden, Miriam Marks, Shun Matsushima, and Beijing Zhu. *The Impact of Social Media on Social Unrest in the Arab Spring*. Stanford, CA: Stanford Public Policy Program, 2012. https://publicpolicy.stanford.edu/publications/impact-social-media-social-unrest-arab-spring.

Dilanian, Ken. "Feds Examining Whether Alleged Hunter Biden Emails Are Linked to a Foreign Intel Operation." NBC News, October 15, 2020. https://www.nbcnews.com/politics/national-security/feds-examining-if-alleged-hunter-biden-emails-are-linked-foreign-n1243620.

Director of Intelligence. *The Soviets in India: Moscow's Major Penetration Program." Intelligence Assessment*. Washington, DC: Central Intelligence Agency, 1985. https://www.cia.gov/library/readingroom/docs/CIA-RDP86T00586R000400490007-7.pdf.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. *The Tactics & Tropes of the Internet Research Agency*. Austin, TX: New Knowledge, 2018.

Page 3177 of 3957

Dixon, Sean M. “Finding the Limit: The Strategic Potential of the Network-Based Actor.” Master’s thesis, Naval Postgraduate School, 2016.

Dobrynin, Anatoly. *In Confidence: Moscow’s Ambassador to America’s Six Cold War Presidents (1962–1986)*. 1st ed. New York: Times Books, Random House, 1995.

Donadio, Rachel. “Why the Macron Hacking Attack Landed with a Thud in France.” *New York Times*, sec. World, December 22, 2017. https://www.nytimes.com/2017/05/08/world/europe/macron-hacking-attack-france.html.

Donaldson, Robert H., Joseph L. Nogee, and Vidya Nadkarni. *The Foreign Policy of Russia: Changing Systems, Enduring Interests*. 5th ed. Armonk, New York: M.E. Sharpe, 2014.

Dutch Safety Board. “MH17 Crash, 17 July 2014.” October 13, 2015. https://www.onderzoeksraad.nl/en/page/3546/crash-mh17-17-july-2014.

Economist, The. “Shadow Puppets: Russian Meddling in Europe.” April 15, 2017.

Elder, Miriam. “Emails Give Insight into Kremlin Youth Group’s Priorities, Means and Concerns.” *The Guardian*, February 7, 2012. https://www.theguardian.com/world/2012/feb/07/nashi-emails-insight-kremlin-groups-priorities.

Elliot, Chris. “The Readers’ Editor On… The Pro-Russia Trolls below the Line on Ukraine Stories.” *The Guardian*, May 4, 2014. https://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online.

Emmott, Robin. “Spain Sees Russian Interference in Catalonia Separatist Vote.” *Reuters*, November 13, 2017. https://www.reuters.com/article/us-spain-politics-catalonia-russia-idUSKBN1DD20Y.

Entous, Adam, Elizabeth Dwoskin, and Craig Timberg. “Obama Tried to Give Zuckerberg a Wake-up Call over Fake News on Facebook.” *Washington Post*, September 24, 2017. https://www.washingtonpost.com/business/economy/obama-tried-to-give-zuckerberg-a-wake-up-call-over-fake-news-on-facebook/2017/09/24/15d19b12-ddac-4ad5-ac6e-ef909e1c1284_story.html.

Erlanger, Steven. “Russia’s RT Network: Is It More BBC or KGB?.” *New York Times*, sec. World, March 8, 2017. https://www.nytimes.com/2017/03/08/world/europe/russias-rt-network-is-it-more-bbc-or-kgb.html.

Page 3178 of 3957

Fakiolas, Tassos E., and Efstathios T. Fakiolas. “Domestic Sources of Russia’s Resurgence as a Global Great Power.” *Journal of International and Area Studies* 16, no. 2 (December 1, 2009): 91–106.

Fearnow, Benjamin. “Timeline of the Tulsi Gabbard, Hillary Clinton Spat: Why the Two Democrats Fought.” *Newsweek*, November 20, 2019. https://www.newsweek.com/timeline-tulsi-gabbard-hillary-clinton-russian-asset-spat-why-two-democrats-fought-1473084.

FEMA. “National Level Exercise 2020.” *Federal Emergency Management Agency* (blog). July 23, 2020. https://www.fema.gov/emergency-managers/planning-exercises/nle/2020.

Foster, Peter, and Matthew Holehouse. “Russia Accused of Clandestine Funding of European Parties as U.S. Conducts Major Review of Vladimir Putin’s Strategy.” *The Sunday Telegraph*, January 16, 2016. http://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html.

Fox, Amos C., and Andrew J. Rossow. “Assessing Russian Hybrid Warfare: A Successful Tool for Limited War.” *Small Wars Journal* 12, no. 1 (August 8, 2016).

Frazin, Rachel. “Trump Knocks Mueller over Russia Probe: ‘18 Angry Democrats’ and ‘0 Collusion.” The Hill, April 19, 2019. https://thehill.com/homenews/administration/439855-trump-knocks-mueller-over-russia-probe-18-angry-democrats-and-0.

Galkins, Kaspars. “NATO and Hybrid Conflict Unresolved Issues from the Past or Unresolvable Threats of the Present.” Master’s thesis, Naval Postgraduate School, 2012.

Gamache, Ray. *Gareth Jones: Eyewitness to the Holodomor*. Cardiff, Wales: Welsh Academic Press, 2016.

Garmazhapova, Aleksandra. “Gdye zhivut trolli. Kak rabotayut internet-provokatory v Sankt-Peterburge i kto Imi zapravlyayet [Where the trolls live: How internet provocateurs work in St. Petersburg and who leads them].” Novaya Gazeta [New Gazette], August 9, 2013. https://www.novayagazeta.ru/articles/2013/09/09/56265-gde-zhivut-trolli-kak-rabotayut-internet-provokatory-v-sankt-peterburge-i-kto-imi-zapravlyaet.

Gatehouse, Gabriel. “Who’s Funding France’s Far Right?.” BBC News, sec. Europe, April 3, 2017. http://www.bbc.com/news/world-europe-39478066.

Page 3179 of 3957

Gearan, Anne, Philip Rucker, and Abby Phillip. “DNC Chairwoman Will Resign in Aftermath of Committee Email Controversy.” *Washington Post*, sec. Politics, July 24, 2016. https://www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html.

Goodman, Marc. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. First Anchor Books Edition. New York: Anchor Books, 2016.

Gorchinskaya, Katya, Olga Rudenko, and William Schreiber. “Authorities: Hackers Foiled in Bid to Rig Ukraine Presidential Election Results.” *Kyiv Post*, May 25, 2014. https://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html.

Graves, Lucia. “Ron Paul Is Putin’s New Best Friend.” *The Atlantic*, July 21, 2014. https://www.theatlantic.com/politics/archive/2014/07/ron-paul-is-putins-new-best-friend/439533/.

Greenberg, Andy. “Hacked Macron Emails Leak Online Ahead of French Presidential Runoff Election.” Wired, May 5, 2017. https://www.wired.com/2017/05/macron-email-hack-french-election/.

———. “Russia’s Cyberwar on Ukraine Is a Blueprint for What’s to Come.” Wired, June 20, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.

Gribble, Richard. “United States Recognition of Soviet Russia: 1917–1933—Church and State Responses.” *American Catholic Studies* 119, no. 4 (December 1, 2008): 21–51.

Grimes, David Robert. “Russian Fake News Is Not New: Soviet AIDS Propaganda Cost Countless Lives.” *The Guardian*, sec. Science, June 14, 2017. https://www.theguardian.com/science/blog/2017/jun/14/russian-fake-news-is-not-new-soviet-aids-propaganda-cost-countless-lives.

Gunaratna, Shanika. “With Trump’s Election, Facebook Wrestles with the Power of Fake News.” CBS News, November 11, 2016. https://www.cbsnews.com/news/with-trumps-election-facebook-wrestles-with-broader-impact-of-fake-news/.

Hackett, Robert. “Sanctions: America’s Best New Weapon against Cyber Crime.” *Fortune*, April 2, 2015. http://fortune.com/2015/04/02/us-cyber-crime-sanctions/.

Hacquebord, Felix. “Two Years of Pawn Storm: Examining an Increasingly Relevant Threat.” Trend Micro TrendLabs, April 25, 2017. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm.

Page 3180 of 3957

Halpin, Tony. “Journalists from Novaya Gazeta Are ‘Assassination Targets.’” *The Times*, January 23, 2009. https://www.thetimes.co.uk/article/journalists-from-novaya-gazeta-are-assassination-targets-cjbv5nzp2sg.

Harding, Luke. “Barack Obama Urges Russia Not to Interfere in Neighbouring States.” *The Guardian*, sec. World news, July 7, 2009. https://www.theguardian.com/world/2009/jul/07/obama-russia-first-trip.

Harris, Shane, Ellen Nakashima, Greg Miller, and Josh Dawsey. “White House Was Warned Giuliani Was Target of Russian Intelligence Operation to Feed Misinformation to Trump.” *Washington Post*, October 15, 2020. https://www.washingtonpost.com/national-security/giuliani-biden-ukraine-russian-disinformation/2020/10/15/43158900-0ef5-11eb-b1e8-16b59b92b36d_story.html.

Helderman, Rosalind S., and Tom Hamburger. “Trump Adviser Flynn Paid by Multiple Russia-Related Entities, New Records Show.” *Washington Post*, sec. Politics, March 16, 2017. https://www.washingtonpost.com/politics/new-details-released-on-russia-related-payments-to-flynn-before-he-joined-trump-campaign/2017/03/16/52a4205a-0a55-11e7-a15f-a58d4a988474_story.html.

Heller, Jacob. “Rumors and Realities: Making Sense of HIV/AIDS Conspiracy Narratives and Contemporary Legends.” *American Journal of Public Health* 105, no. 1 (November 13, 2014): e43–e50. https://doi.org/10.2105/AJPH.2014.302284.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. Santa Monica, CA: RAND, 2018. https://www.rand.org/pubs/research_reports/RR2237.html.

Hendry, Erica R. “The Many Different Ways Trump Has Described Putin and Russian Election Interference.” PBS NewsHour, July 16, 2018. https://www.pbs.org/newshour/politics/the-many-different-ways-trump-has-described-putin-and-russian-election-interference.

Higgins, Andrew. “Intent on Unsettling E.U., Russia Taps Foot Soldiers from the Fringe.” *New York Times*, sec. Europe, December 24, 2016. https://www.nytimes.com/2016/12/24/world/europe/intent-on-unsettling-eu-russia-taps-foot-soldiers-from-the-fringe.html.

Holland, Adam. “RT “Covers” the Shooting down of MH17.” July 18, 2014, *The Interpreter*. https://www.interpretermag.com/rt-covers-the-shooting-down-of-mh17/.

Page 3181 of 3957

Holland, Max. “The Propagation and Power of Communist Security Services Dezinformatsiya.” *International Journal of Intelligence and CounterIntelligence* 19, no. 1 (January 1, 2006): 1–31. https://doi.org/10.1080/08850600500332342; Andrew and Mitrokhin, *The World Was Going Our Way*, 318.

House Committee on Oversight and Reform. “Cummings Releases New Documents Confirming that Flynn Received Funds from Instrument of Russian Government.” March 16, 2017. https://oversight.house.gov/news/press-releases/cummings-releases-new-documents-confirming-that-flynn-received-funds-from.

Illing, Sean. “Division and Tension at the DNC: The Democrats’ Night of Unity Is Marred by Dissent.” Salon, July 26, 2016. https://www.salon.com/2016/07/26/division_and_tension_at_the_dnc_the_democrats_night_of_unity_is_marred_by_dissent/.

Iosifidis, Petros, and Nicholas Nicoli. “The Battle to End Fake News: A Qualitative Content Analysis of Facebook Announcements on How It Combats Disinformation.” *International Communication Gazette* 82, no. 1 (February 1, 2020): 60–81. https://doi.org/10.1177/1748048519880729.

Isaac, Mike, and Daisuke Wakabayashi. “Russian Influence Reached 126 Million through Facebook Alone.” *New York Times*, sec. Technology, October 31, 2017. https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

Isikoff, Michael, and David Corn. *Russian Roulette: The Inside Story of Putin’s War on America and The Election of Donald Trump*. 1st ed. New York: Twelve, 2018.

Jackson, David, and Kevin Johnson. “President Trump Accuses Special Counsel Robert Mueller of McCarthyism, Trying to Coerce Witnesses.” *USA Today*, November 28, 2018. https://www.usatoday.com/story/news/politics/2018/11/28/donald-trump-robert-mueller-mccarthy/2135863002/.

Jalonick, Mary Claire. “Comey Faces off with GOP over Clinton Emails, Alleged Bias.” *Associated Press*, December 7, 2018. https://apnews.com/article/734284dd1aa746c19bf209770ae1ce54.

Jarábik, Balázs. “Putin’s Budapest Bargain Is Built on Shaky Ground.” Carnegie Endowment for International Peace, August 28, 2017. http://carnegieendowment.org/2017/08/28/putin-s-budapest-bargain-is-built-on-shaky-ground-pub-72939.

Jarrett, Gregg. *Russia Hoax: The Illicit Scheme to Clear Hillary Clinton and Frame Donald Trump*. Northampton, MA: Broadside Books, 2018.

Javers, Eamon. “FBI’s Comey Opposed Naming Russians, Citing Election Timing: Source.” CNBC News, October 31, 2016. https://www.cnbc.com/2016/10/31/fbis-comey-opposed-naming-russians-citing-election-timing-source.html.

Page 3182 of 3957

Johnson, Martin. “Jill Stein: ‘I Am Not a Russian Spy.” The Hill, October 19, 2019. https://thehill.com/homenews/campaign/466594-jill-stein-i-am-not-a-russian-spy.

Kasparov, Garry, and Mig Greengard. *Winter Is Coming: Why Vladimir Putin and the Enemies of the Free World Must Be Stopped*. 1st ed. New York: PublicAffairs, 2015.

Kean, Thomas H., and Lee Hamilton and U.S. National Commission on Terrorist Attacks upon the United States. *9/11 Commission Report: The Official Report of the 9/11 Commission and Related Publications*. Washington, DC: Government Printing Office, 2004. http://www.gpoaccess.gov/911/index.html.

Keeley, Graham. “Russia Meddled in Catalonia Independence Referendum, Says German Intelligence Boss.” *The Times*, sec. World, May 15, 2018. https://www.thetimes.co.uk/article/russia-meddled-in-catalonia-vote-p6g5nttpm.

Kessler, Glenn. “Tulsi Gabbard Misquotes Hillary Clinton’s Jab at Her.” *Washington Post*, October 31, 2019. https://www.washingtonpost.com/politics/2019/10/31/tulsi-gabbard-misquotes-hillary-clintons-jab-her/.

Koppel, Ted. *Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath*. 1st ed. New York: Crown Publishers, 2015.

Kragh, Martin, and Sebastian Åsberg. “Russia’s Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case.” *Journal of Strategic Studies* 40, no. 6 (September 19, 2017): 773–816. https://doi.org/10.1080/01402390.2016.1273830.

Kreiss, Daniel, and Shannon C. McGregor. “Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google with Campaigns during the 2016 U.S. Presidential Cycle.” *Political Communication* 35, no. 2 (April 3, 2018): 155–77. https://doi.org/10.1080/10584609.2017.1364814.

Kreps, Sarah, Sandip Prasad, John S. Brownstein, Yulin Hswen, Brian T. Garibaldi, Baobao Zhang, and Douglas L. Kriner. “Factors Associated with U.S. Adults’ Likelihood of Accepting COVID-19 Vaccination.” *Journal of the American Medical Association Network Open* 3, no. 10 (October 20, 2020). https://doi.org/10.1001/jamanetworkopen.2020.25594.

Kristek, Michael R. “The Nature of Russia’s Threat to NATO’s Enhanced Forward Presence in the Baltic States.” Master’s thesis, Naval Postgraduate School, 2017.

Krushelnycky, Askold. “Ukrainians Want Pro-Stalin Writer Stripped of Pulitzer.” *The Guardian*, sec. World News, May 4, 2003. http://www.theguardian.com/world/2003/may/04/russia.usa.

Page 3183 of 3957

Kux, Dennis. “Soviet Active Measures and Disinformation: Overview and Assessment.” *Parameters, Journal of the U.S. Army War College* 15, no. 4 (December 1, 1985): 19–28.

LaFraniere, Sharon, and Zach Montague. “Roger Stone Is Convicted of Impeding Investigators in a Bid to Protect Trump.” *New York Times*, sec. U.S., November 15, 2019. https://www.nytimes.com/2019/11/15/us/politics/roger-stone-trial-guilty.html.

Landler, Mark, and Eric Lichtblau. “Jeff Sessions Recuses Himself from Russia Inquiry.” *New York Times*, sec. U.S., March 2, 2017. https://www.nytimes.com/2017/03/02/us/politics/jeff-sessions-russia-trump-investigation-democrats.html.

Lapowsky, Issie. “Did Trump’s Data Team Help Russians? Facebook Might Have the Answer.” Wired, July 14, 2017. https://www.wired.com/story/trump-russia-data-parscale-facebook/.

———. “Tumblr IDs 84 Accounts that Spread Propaganda.” Wired, March 23, 2018. https://www.wired.com/story/tumblr-russia-trolls-propaganda/.

Laqueur, Walter. *Putinism: Russia and Its Future with the West*. 1st ed. New York: Thomas Dunne Books, 2015.

Larson, Erik. “Flynn Prosecutor Steps Down as Case Is Reportedly Being Dropped.” *Bloomberg*, May 7, 2020. https://www.bloomberg.com/news/articles/2020-05-07/flynn-prosecutor-van-grack-steps-down-from-criminal-case.

Laruelle, Marlene. “Russia’s Bedfellowing Policy and the European Far Right.” *Russian Analytical Digest*, no. 167 (May 6, 2015): 3–12.

Lawfare. “The Macron Leaks: Are They Real, and Is It Russia?.” May 8, 2017. https://www.lawfareblog.com/macron-leaks-are-they-real-and-it-russia.

Lawyers Defending American Democracy. “Open Letter Supporting the 100,000 Lawyers, Agents, and Staff Members of the U. S. Department of Justice.” *Lawyers Defending American Democracy* (blog). Accessed October 19, 2020. https://lawyersdefendingdemocracy.org/open-letter-supporting-the-us-doj/.

Leask, David. “SNP Claims Russia Is Likely to Have Interfered in Referendum.” *The Herald*, December 14, 2017. https://www.heraldscotland.com/news/15771388.yes-leaders-dont-be-naive-about-russian-online-meddling-in-independence/.

Lederman, Josh. “Putin: Russia Will ‘Never’ Extradite Citizens Accused by U.S.” *Associated Press*, sec. United States, March 4, 2018. https://apnews.com/article/c5180bffb84d424ba11cf3384a665eb5.

Page 3184 of 3957

Lerer, Lisa. “What, Exactly, Is Tulsi Gabbard up to?.” *New York Times*, sec. U.S., October 12, 2019. https://www.nytimes.com/2019/10/12/us/politics/tulsi-gabbard.html.

Levintova, Hannah. “Russian Journalists Just Published a Bombshell Investigation about a Kremlin-Linked “Troll Factory.”” *Mother Jones*, October 18, 2017. https://www.motherjones.com/politics/2017/10/russian-journalists-just-published-a-bombshell-investigation-about-a-kremlin-linked-troll-factory/.

Lister, Tim, and Clare Sebastian. “Stoking Islamophobia and Secession in Texas—From an Office in Russia.” CNN, October 6, 2017. https://www.cnn.com/2017/10/05/politics/heart-of-texas-russia-event/index.html.

Longman, Martin. “Did the Russians Mess with the Voter Rolls?.” *Washington Monthly*, June 1, 2018. https://washingtonmonthly.com/2018/06/01/did-the-russians-mess-with-the-voter-rolls/.

Lough, Richard, Eric Auchard, and Ingrid Melander. “WikiLeaks Publishes Searchable Archive of Macron Campaign Emails.” *Reuters*, July 31, 2017. https://www.reuters.com/article/us-france-politics-wikileaks-idUSKBN1AG1TZ.

Lytvynenko, Jane. “InfoWars Has Republished More than 1,000 Articles from RT without Permission.” BuzzFeed News, November 8, 2017. https://www.buzzfeednews.com/article/janelytvynenko/infowars-is-running-rt-content.

Martelle, Scott. *The Fear within: Spies, Commies, and American Democracy on Trial*. New Brunswick: Rutgers University Press, 2011. Proquest.

Martin, John Bartlow. *Adlai Stevenson and the World: The Life of Adlai E. Stevenson*. Garden City, NY: Anchor Books, 1977.

Mastriano, Douglas. “Putin—The Masked Nemesis of the Strategy of Ambiguity.” *Defense & Security Analysis* 33, no. 1 (January 20, 2017): 68–76. https://doi.org/10.1080/14751798.2016.1272175.

Mazzetti, Mark, and Matthew Rosenberg. “Michael Flynn Misled Pentagon about Russia Ties, Letter Says.” *New York Times*, May 22, 2017. https://www.nytimes.com/2017/05/22/us/politics/michael-flynn-fifth-amendment-russia-senate.html.

Mazzetti, Mark, and Michael S. Schmidt. “Mueller Objected to Barr’s Description of Russia Investigation’s Findings on Trump.” *New York Times*, sec. U.S., April 30, 2019. https://www.nytimes.com/2019/04/30/us/politics/mueller-barr.html.

Page 3185 of 3957

McCauley, Kevin N. *Russian Influence Campaigns against the West: From the Cold War to Putin*. North Charleston, SC: CreateSpace Independent Publishing Platform, 2016.

McDonald, Bryan. "McCarthyism 2.0: Real Skill of U.S. 'Disinformation Experts' Is Spreading Disinformation." RT International, August 1, 2018. https://www.rt.com/op-ed/434846-twitter-russia-disinformation-mccarthyism/.

McFadden, Cynthia, William Arkin, and Kevin Monahan. "Russians Penetrated U.S. Voter Systems, Top Official Says." NBC News, February 7, 2018. https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721.

McFadden, Cynthia, William Arkin, Josh Meyer, and Ken Dilanian. "Red Alert? Hackers Target Election Systems in 20 States." NBC News, September 29, 2016. https://www.nbcnews.com/news/us-news/red-alert-election-systems-20-states-targeted-hackers-n657036.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." BBC News, sec. Europe, April 27, 2017. https://www.bbc.com/news/39655415.

Mearsheimer, John J. "Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions that Provoked Putin." *Foreign Affairs*, September 30, 2014.

Memoli, Michael A. "Trump National Security Advisor Michael Flynn Resigns over Contacts with Russia." *Los Angeles Times*, February 13, 2017. https://www.latimes.com/politics/la-na-pol-trump-flynn-20170213-story.html.

Mena, Paul. "Cleaning up Social Media: The Effect of Warning Labels on Likelihood of Sharing False News on Facebook." *Policy & Internet* 12, no. 2 (June 1, 2020): 165–83. https://doi.org/10.1002/poi3.214.

Mettler, Katie. "Jesse Ventura's New Russian State TV Show: 'I Am Working for the Enemy of Mainstream Media Now." *Washington Post*, June 8, 2017. https://www.washingtonpost.com/news/morning-mix/wp/2017/06/08/jesse-venturas-new-russian-state-tv-show-i-am-working-for-the-enemy-of-mainstream-media-now/.

Meyer, David. "Russia Blamed for 'Costliest Cyberattack in History." *Fortune*, February 16, 2018. http://fortune.com/2018/02/16/russia-notpetya-cyberattack-damage/.

Miazhevich, Galina. "Nation Branding in the Post-Broadcast Era: The Case of RT." *European Journal of Cultural Studies* 21, no. 5 (October 1, 2018): 575–93. https://doi.org/10.1177/1367549417751228.

Page 3186 of 3957

Michel, Casey. “America’s Neo-Nazis Don’t Look to Germany for Inspiration. They Look to Russia.” *Washington Post*, August 22, 2017. https://www.washingtonpost.com/news/democracy-post/wp/2017/08/22/americas-neo-nazis-dont-look-to-germany-for-inspiration-they-look-to-russia/.

———. “Russia Wants Texas and Puerto Rico to Secede.” *The Daily Beast*, sec. world, September 24, 2015. https://www.thedailybeast.com/articles/2015/09/24/russia-wants-texas-and-puerto-rico-to-secede.

———. “The Kremlin’s California Dream.” *Slate*, May 4, 2017. http://www.slate.com/articles/news_and_politics/foreigners/2017/05/why_russia_cultivates_fringe_groups_on_the_far_right_and_far_left.html.

———. “The Pro-Kremlin Talking Points of Jill Stein.” *ThinkProgress* (blog). December 19, 2017. https://archive.thinkprogress.org/jill-stein-campaign-russia-ecf424ac3b7e/.

Miller, Greg, Ellen Nakashima, and Adam Entous. “Obama’s Secret Struggle to Punish Russia for Putin’s Election Assault.” *Washington Post*, June 23, 2017. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/.

Miller, Susan, and Jordan Culver. “‘It’s Not Over’: Trump Supporters Flock to State Capitols after Biden Victory Is Announced.” USA Today, November 7, 2020. https://www.usatoday.com/story/news/nation/2020/11/07/election-protests-updates-trump-supporters-state-capitols-biden-win/6203271002/.

Mitchell, Lincoln. “Ron Paul’s Appearances on Kremlin TV Could Damage His Son’s Presidential Aspirations.” *Observer* (blog). November 17, 2014. https://observer.com/2014/11/ron-pauls-appearances-on-kremlin-tv-could-damage-his-sons-presidential-aspirations/.

Mohan, Vasu, and Alan Wall. “Foreign Electoral Interference: Past, Present, and Future.” *Georgetown Journal of International Affairs; Washington* 20 (September 1, 2019): 110–19.

Morris, Emma-Jo, and Gabrielle Fonrouge. “Smoking-Gun Email Reveals How Hunter Biden Introduced Ukrainian Businessman to VP Dad.” *New York Post*, October 14, 2020. https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/.

Mueller, Robert S. III. *Report on the Investigation into Russian Interference in the 2016 Election Vol. I*. Washington, DC: Department of Justice, 2019.

Mulligan, Stephen P., Wilson C. Freeman, and Chris D. Linebaugh. *Data Protection Law: An Overview*. CRS Report No. R45631. Washington, DC: Congressional Research Service, 2019.

Page 3187 of 3957

Murray, Sara, and Kate Sullivan. “Text Messages Show Roger Stone Discussing WikiLeaks Plans Days before Hack.” CNN, November 26, 2018. https://www.cnn.com/2018/11/14/politics/text-messages-roger-stone-wikileaks-hack/index.html.

Myagkov, Mikhail, Peter C. Ordeshook, and Dimitry Shakin. “Fraud or Fairytales: Russia and Ukraine’s Electoral Experience.” *Post-Soviet Affairs* 21, no. 2 (January 1, 2005): 91–131. https://doi.org/10.2747/1060-586X.21.2.91.

Myagkov, Mikhail G., Peter C. Ordeshook, and Dimitri Shakin. *The Forensics of Election Fraud: Russia and Ukraine*. Cambridge, New York: Cambridge University Press, 2009.

Myles-Primakoff, Justin, and Justin Sherman. “Russia’s Internet Freedom Shrinks as Kremlin Seizes Control of Homegrown Tech.” *Foreign Policy*, October 26, 2020. https://foreignpolicy.com/2020/10/26/russia-internet-freedom-kremlin-tech/.

Nakamura, David, and Greg Miller. “Trump, CIA on Collision Course over Russia’s Role in U.S. Election.” *Washington Post*, December 10, 2016. https://www.washingtonpost.com/politics/trump-cia-on-collision-course-over-russias-role-in-us-election/2016/12/10/ad01556c-bf01-11e6-91ee-1adddfe36cbe_story.html.

Nakashima, Ellen. “Russian Hackers Targeted Arizona Election System.” *Washington Post*, July 29, 2016. https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html.

———. “Russian Military Was behind ‘NotPetya’ Cyberattack in Ukraine, CIA Concludes.” *Washington Post*, January 12, 2018. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

Nance, Malcolm. *The Plot to Hack America: How Putin’s Cyberspies and WikiLeaks Tried to Steal the 2016 Election*. New York: Skyhorse Publishing, 2016.

Nance, Malcolm W. *The Plot to Destroy Democracy: How Putin and His Spies Are Undermining America and Dismantling the West*. 1st ed. New York: Hachette Books, 2018. Kindle.

Narayanan, Vidya, Philip N. Howard, Bence Kollanyi, and Mona Elwash. *Russian Involvement and Junk News during Brexit*. Computational Propaganda Project. Oxford: University of Oxford, 2017.

Page 3188 of 3957

New York Times. “Lawyer Says Texan Told Him Oswald Had Aid in ‘63 Plot.” Sec. Archives, April 3, 1977. https://www.nytimes.com/1977/04/03/archives/lawyer-says-texan-told-him-oswald-had-aid-in-63-plot.html; Andrew and Mitrokhin.

North Atlantic Treaty Organization. “NATO Opens New Centre of Excellence on Cyber Defence.” May 14, 2008. https://www.nato.int/docu/update/2008/05-may/e0514a.html.

———. “The North Atlantic Treaty.” April 4, 1949. http://www.nato.int/cps/en/natohq/official_texts_17120.htm.

Novinite Sofia News Agency. “Huge Hack Attack on Bulgaria Election Authorities ‘Not to Affect Vote Count.” October 27, 2015. https://www.novinite.com/articles/171533/Huge+Hack+Attack+on+Bulgaria+Election+Authorities+%27Not+to+Affect+Vote+Count%27.

O’Neill, Patrick Howell. “Researchers Link Macron Hack to APT28 with ‘Moderate Confidence.” Cyberscoop, May 11, 2017. https://www.cyberscoop.com/researchers-link-macron-hack-to-apt28-with-moderate-confidence/.

O’Sullivan, Donie, Drew Griffin, and Curt Devine. “In Attempt to Sow Fear, Russian Trolls Paid for Self-Defense Classes for African Americans.” CNNMoney, October 18, 2017. https://money.cnn.com/2017/10/18/media/black-fist-russia-self-defense-classes/index.html.

Obama, Barack. Executive Order 13694. “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.” Code of Federal Regulations, title 3 (2015). https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

———. Executive Order 13757. “Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.” Code of Federal Regulations, title 3 (2017). https://www.govinfo.gov/content/pkg/FR-2017-01-03/pdf/2016-31922.pdf.

Office of Public Affairs. “Appointment of Special Counsel.” Department of Justice, May 17, 2017. https://www.justice.gov/opa/pr/appointment-special-counsel.

Office of the Director of National Intelligence. *Assessing Russian Activities and Intentions in Recent U.S. Elections*. Washington, DC: Office of the Director of National Intelligence, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Page 3189 of 3957

Oliphant, Roland, and Cara McGoogan. “NATO Warns Cyber Attacks ‘Could Trigger Article 5’ As World Reels from Ukraine Hack.” *The Telegraph*, June 28, 2017. https://www.telegraph.co.uk/news/2017/06/28/nato-assisting-ukrainian-cyber-defences-ransom-ware-attack-cripples/.

Paget, Antonia. “Russia Today Host Condemns Ukraine ‘Occupation.” *The Times*, March 4, 2014. https://www.thetimes.co.uk/article/russia-today-host-condemns-ukraine-occupation-rgmqv036jcj.

Parker, Ashley, and David E. Sanger. “Donald Trump Calls on Russia to Find Hillary Clinton’s Missing Emails.” *New York Times*, sec. U.S., July 27, 2016. https://www.nytimes.com/2016/07/28/us/politics/donald-trump-russia-clinton-emails.html.

Parkinson, Joe, and Georgi Kantchev. “Document: Russia Uses Rigged Polls, Fake News to Sway Foreign Elections.” *Wall Street Journal*, sec. World. March 23, 2017. https://www.wsj.com/articles/how-does-russia-meddle-in-elections-look-at-bulgaria-1490282352.

Penzenstadler, Nick, Brad Heath, and Jessica Guynn. “We Read Every One of the 3,517 Facebook Ads Bought by Russians. Here’s What We Found.” *USA Today*, May 11, 2018. https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/.

Perkins, Alexander M. “Soviet Active Measures Reborn for the 21st Century: What Is to Be Done?” Master’s thesis, Naval Postgraduate School, 2018.

Perlroth, Nicole, and David E. Sanger. “Times’s Moscow Bureau Hit by Attempted Hacking.” *New York Times*, sec. Technology, August 24, 2016. https://www.nytimes.com/2016/08/24/technology/new-york-timess-moscow-bureau-was-targeted-by-hackers.html.

Permanent Select Committee on Intelligence. “Social Media Advertisements, 2016, Quarter 2, 2016-05: P(1)0000410.” U.S. House of Representatives. Accessed December 6, 2020. https://intelligence.house.gov/social-media-content/social-media-advertisements.htm.

———. “Social Media Advertisements, 2016, Quarter 4, 2016-10: P(1)0004496.” U.S. House of Representatives. Accessed December 6, 2020. https://intelligence.house.gov/social-media-content/social-media-advertisements.htm.

———. “Social Media Advertisements, 2016, Quarter 4, 2016-10: P(1)0005278.” U.S. House or Representatives. Accessed December 6, 2020. https://intelligence.house.gov/social-media-content/social-media-advertisements.htm.

Page 3190 of 3957

Person, Robert. “Balance of Threat: The Domestic Insecurity of Vladimir Putin.” *Journal of Eurasian Studies* 8, no. 1 (January 1, 2017): 44–59. https://doi.org/10.1016/j.euras.2016.11.001.

Plowright, Adam. “France and Macron Have Buried Allegations of Russian Meddling.” *Washington Post*, May 23, 2018. https://www.washingtonpost.com/news/global-opinions/wp/2018/05/23/france-and-macron-have-buried-allegations-of-russian-meddling/.

Plunkett, John. “Russia Today Reporter Resigns in Protest at MH17 Coverage.” *The Guardian*, sec. Media, July 18, 2014. http://www.theguardian.com/media/2014/jul/18/mh17-russia-today-reporter-resigns-sara-firth-kremlin-malaysia.

Political Capital Institute. *The Russian Connection: The Spread of Pro-Russian Policies on the European Far Right*. Budapest, Hungary: Political Capital Policy Research and Consulting Institute, 2014. http://www.riskandforecast.com/useruploads/files/pc_flash_report_russian_connection.pdf.

Politico Europe. “Catalan Referendum Stokes Fears of Russian Influence.” September 29, 2017. https://www.politico.eu/article/russia-catalonia-referendum-fake-news-misinformation/.

Polyakova, Alina, Laruelle, Marlene, Meister, Stefan, and Barnett, Neil. *The Kremlin’s Trojan Horses: Russian Influence in France, Germany, and the United Kingdom*. 3rd ed. Washington, DC: Atlantic Council, 2016. https://www.atlanticcouncil.org/in-depth-research-reports/report/kremlin-trojan-horses/.

Pomerantsev, Peter. “Yes, Russia Matters: Putin’s Guerrilla Strategy.” *World Affairs* 177, no. 3 (September 30, 2014): 16–23.

Priess, David. “The ‘Time of Troubles’ Is Back for America’s Spies.” *Foreign Policy*, July 26, 2018. https://foreignpolicy.com/2018/07/26/the-time-of-troubles-is-back-for-americas-intelligence-community/.

Putin, Vladimir. “Address by President of the Russian Federation.” President Rosiyi [President of Russia], March 18, 2014. http://en.kremlin.ru/events/president/news/20603.

Page 3191 of 3957

———. “Predsedatel Pravitelstva Rossiyskoy Federatsiy Vladimir Putin provel zasedaniye Koordinatsionnovo soveta Obshcherossiyskovo narodnovo fronta” [Prime Minister of the Russian Federation Vladimir Putin led the Coordination Council of the All-Russia People’s Front], Pravitel’stvo Rossiyskoy Federatsii [Office of the Prime Minister of the Russian Federation news release], December 8, 2011. https://web.archive.org/web/20120607083034/http://premier.gov.ru/events/news/17330/.

———. “Telekanal Russia Today nachal veshchaniye v Argentine [Russia Today TV channel began broadcast in Argentina].” Prezident Rossii [Office of the President of Russia], October 9, 2014. http://kremlin.ru/events/president/news/46762

Radio France Internationale. “France Warns Russia against Interfering in Elections.” February 16, 2017. http://en.rfi.fr/france/20170216-france-warns-russia-against-interfering-elections.

Ramsay, Gordon, and Sam Robertshaw. *Weaponising News: RT, Sputnik and Targeted Disinformation*. London, England: King’s College, 2019. https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf.

Rasmussen, Earl. “How the U.S. Stifles Free Speech: Reviving McCarthyism & Nurturing Orwellian Society.” RT International, May 10, 2018. https://www.rt.com/op-ed/426351-us-free-speech-mccarthyism/.

Ratner, Gershon (Gary), Roy L. Austin, Dori Bernstein, Charles Both, John Brittain, Katherine S. Broderick, Paul Butler, et al. “Ethics Complaint Re: Professional Responsibility Investigation of William P. Barr.” July 23, 2020. Lawyers Defending America Democracy. https://lawyersdefendingdemocracy.org/reprofessional-responsibility-investigation-of-william-p-barr/.

“Recognition of the Soviet Union, 1933.” In *Milestones in the History of U.S. Foreign Relations: 1921–1936*. Department of State Office of the Historian, 2009. https://history.state.gov/milestones/1921-1936/ussr.

Reevell, Patrick. “Texas, California Separatists Attend Kremlin-Funded Conference.” ABC News, September 27, 2016. https://abcnews.go.com/International/texas-california-separatists-attend-pro-kremlin-conference/story?id=42395066.

Reuters Staff. “Socialist Ally Rumen Radev Wins Bulgaria Presidency: Exit Polls.” *Reuters*, November 13, 2016. https://www.reuters.com/article/us-bulgaria-election-exitpoll-idUSKBN1380Q7.

Rezunkov, Viktor. “Oni lyubyat Putina 12 chasov podryad [They love Putin 12 hours straight].” Radio Svoboda [Radio Liberty].” March 14, 2015. https://www.svoboda.org/a/26899521.html.

Page 3192 of 3957

Ribeiro, Filipe N., Koustuv Saha, Mahmoudreza Babaei, Lucas Henrique, Johnnatan Messias, Fabricio Benevenuto, Oana Goga, Krishna P. Gummadi, and Elissa M. Redmiles. "On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook." In *Proceedings of the Conference on Fairness, Accountability, and Transparency—FAT* '19*, 140–49, January 29, 2019. https://doi.org/10.1145/3287560.3287580.

Riechmann, Deb. "Retrieved Papers Shed Light on Communist Activities in U.S." *The Billings Gazette*, January 30, 2001. http://billingsgazette.com/news/world/retrieved-papers-shed-light-on-communist-activities-in-u-s/article_bd5e5ca5-38b7-5dcd-b645-b203cbaa0445.html.

Roberts, Kari. "Understanding Putin: The Politics of Identity and Geopolitics in Russian Foreign Policy Discourse." *International Journal: Canada's Journal of Global Policy Analysis* 72, no. 1 (March 1, 2017): 28–55. https://doi.org/10.1177/0020702017692609.

Roberts, Molly. "Jill Stein Isn't Doing the Left Any Favors." *Washington Post*, May 2, 2018. https://www.washingtonpost.com/blogs/post-partisan/wp/2018/05/02/jill-steins-attitude-toward-the-russia-investigation-isnt-doing-the-left-any-favors/.

Robertson, Katie. "New York Post Published Hunter Biden Report Amid Newsroom Doubts." *The New York Times*, sec. Business, October 18, 2020. https://www.nytimes.com/2020/10/18/business/media/new-york-post-hunter-biden.html.

Roose, Kevin. "Facebook and Twitter Dodge a 2016 Repeat, and Ignite a 2020 Firestorm." *New York Times*, sec. Technology, October 15, 2020. https://www.nytimes.com/2020/10/15/technology/facebook-twitter-nypost-hunter-biden.htm;

Rosen, Guy. "Facebook Publishes Enforcement Numbers for the First Time." *Facebook Newsroom* (blog). May 15, 2018. https://newsroom.fb.com/news/2018/05/enforcement-numbers/.

Rosenberg, Matthew. "U.S. Intelligence Community Reacts with Fury to Trump's Rebuke." *New York Times*, sec. U.S., July 17, 2018. https://www.nytimes.com/2018/07/16/us/politics/us-intel-community-reacts-with-fury-to-trumps-rebuke.html.

RT. "'Atone!' Democrats Blame Jill Stein Voters for Trump's Chance to Appoint a 3rd Supreme Court Justice." September 26, 2020. https://www.rt.com/usa/501803-jill-stein-bill-maher-supreme-court-trump/.

———. "Green Party Candidates to Face Off in Debate Hosted by RT (Watch Live)." May 9, 2016. https://www.rt.com/usa/342395-green-party-rt-debate/.

Page 3193 of 3957

———. “Jill Stein Offers Third Party Perspective on Final Debate.” October 20, 2016. https://www.rt.com/usa/363379-jill-stein-debates-live/.

Saari, Sinikukka. “Putin’s Eurasian Union Initiative: Are the Premises of Russia’s Post-Soviet Policy Changing?.” *Swedish Institute of International Affairs UI Brief*, no. 9 (November 1, 2011). https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/putins-eurasian-union-initiative-are-the-premises-of-russias-post-soviet-policy-changing-min.pdf.

Safire, William. “The Cold War’s Hot Kitchen.” *New York Times*, sec. Opinion, July 23, 2009. https://www.nytimes.com/2009/07/24/opinion/24safire.html.

Sakwa, Richard. “‘New Cold War’ or Twenty Years’ Crisis? Russia and International Politics.” *International Affairs* 84, no. 2 (March 1, 2008): 241–67. https://doi.org/10.1111/j.1468-2346.2008.00702.x.

Samuel, Henry. “Marine Le Pen’s Links to Russia under U.S. Scrutiny.” *The Telegraph*, December 21, 2016. http://www.telegraph.co.uk/news/2016/12/21/marine-le-pens-russian-links-us-scrutiny/.

Sanger, David E., and Katie Benner. “U.S. Accuses North Korea of Plot to Hurt Economy as Spy Is Charged in Sony Hack.” *New York Times*, August 6, 2018. https://www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html.

Sanz, Catherine, and Catherine Thorbecke. “What Social Media Giants Are Doing to Counter Misinformation This Election.” ABC News, October 18, 2020. https://abcnews.go.com/Technology/social-media-giants-counter-misinformation-election/story?id=73563997.

Schoen, Fletcher, and Christopher J. Lamb. “Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference.” *Institute for National Strategic Studies: Strategic Perspectives*, no. 11 (June 1, 2012): 1–168.

Schrecker, Ellen. “McCarthyism: Political Repression and the Fear of Communism.” *Social Research* 71, no. 4 (December 1, 2004): 1041–86.

Seddon, Max. “Documents Show How Russia’s Troll Army Hit America.” Buzzfeed News, June 2, 2014. https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america.

Seddon, Max, and James Politi. “Putin’s Party Signs Deal with Italy’s Far-Right Lega Nord.” *Financial Times*, March 6, 2017. https://www.ft.com/content/0d33d22c-0280-11e7-ace0-1ce02ef0def9; Laqueur, *Putinism*.

Page 3194 of 3957

Shekhovtsov, Anton. *Russia and the Western Far Right: Tango Noir*. Abingdon, United Kingdom: Routledge, 2017. Kindle.

Shepherd, Katie. "Tensions over Restrictions Spark Violence and Defiance among Protesters as Trump Pushes States to Reopen." *Washington Post*, May 13, 2020. https://www.washingtonpost.com/nation/2020/05/13/protest-violence-coronavirus/.

Sherman, Justin. "Russia Is Trying Something New to Isolate Its Internet from the Rest of the World." *Slate Magazine*, September 25, 2020. https://slate.com/technology/2020/09/russia-internet-encryption-protocol-ban.html.

Shih, Adrienne. "FBI Director James Comey: 'You Can Call Us Wrong, But Don't Call Us Weasels." CNN, September 26, 2016. https://www.cnn.com/2016/09/28/politics/james-comey-congress-hearing-weasel/index.html.

Shimer, David. *Rigged: America, Russia and One Hundred Years of Covert Electoral Interference*. New York: Knopf, 2020.

Shore, Marci. *The Ukrainian Night: An Intimate History of Revolution*. New Haven, CT: Yale University Press, 2018. Kindle.

Shultz, Richard H., and Roy Godson. *Dezinformatsia: Active Measures in Soviet Strategy*. Washington, DC: Pergamon-Brassey's, 1984.

Snell, Robert, and Melissa Nann Burke. "Plans to Kidnap Whitmer, Overthrow Government Spoiled, Officials Say." *Detroit News*, October 8, 2020. https://www.detroitnews.com/story/news/local/michigan/2020/10/08/feds-thwart-militia-plot-kidnap-michigan-gov-gretchen-whitmer/5922301002/.

Socor, Vladimir. "Russia Orchestrates Gagauz Election in Moldova, Ponders the Next Steps." NGO Publication, *Jamestown Foundation* 12, no. 59 (March 15, 2015). https://jamestown.org/program/russia-orchestrates-gagauz-election-in-moldova-ponders-the-next-steps/.

Sonne, Paul. "A Russian Bank Gave Marine Le Pen's Party a Loan. Then Weird Things Began Happening." *Washington Post*, December 27, 2018. https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html.

Soshnikov, Andrey. "Stolitsa politicheskovo trollinga, [Capital of political trolling]" moy rayon [my neighborhood], March 11, 2015. https://mr-7.ru/articles/112478/.

Page 3195 of 3957

Sputnik International. “Ex-French Economy Minister Macron Could Be ‘U.S. Agent’ Lobbying Banks’ Interests.” February 4, 2017. https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq/.

Stapleton, AnneClaire. “No, You Can’t Vote by Text Message.” CNN, November 7, 2016. https://www.cnn.com/2016/11/07/politics/vote-by-text-message-fake-news/index.html.

Stein, Jill. “Hillary Clinton Called Me a ‘Russian Asset.’ The Establishment Is Losing Its Grip.” *The Guardian*, sec. Opinion, October 24, 2019. https://www.theguardian.com/commentisfree/2019/oct/24/hillary-clinton-called-me-a-russian-asset-the-establishment-is-losing-their-grip.

Stelzenmüller, Constanze. “The Impact of Russian Interference on Germany’s 2017 Elections.” Brookings. https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

Stone, Peter, and Greg Gordan. “Trump-Russia Investigators Probe Jared Kushner-Run Digital Operation.” McClatchey DC Bureau, July 12, 2017. https://www.mcclatchydc.com/news/nation-world/national/article160803619.html.

Styles, William. “The World Federation of Scientific Workers, A Case Study of a Soviet Front Organisation: 1946–1964.” *Intelligence and National Security* 33, no. 1 (January 2, 2018): 116–29. https://doi.org/10.1080/02684527.2017.1323479; Shultz and Godson, *Dezinformatsia*, 112–131.

Szabolcs, Dezső, and Panyi András. “Russian Diplomats Exercised with Hungarian Cop Killer’s Far-Right Gang.” Index, October 28, 2016. http://index.hu/belfold/2016/10/28/russian_diplomats_exercised_with_hungarian_cop_killer_s_far-right_gang/

Tanfani, Joseph. “Comey Strongly Defends Decision to Reopen FBI Probe into Clinton Emails 11 Days before the Election.” *Los Angeles Times*, May 3, 2017. https://www.latimes.com/politics/washington/la-na-essential-washington-updates-comey-says-the-late-disclosure-of-1493824301-htmlstory.html.

Taylor, Adam. “This Kremlin Leader Bragged about Tipping a U.S. Presidential Election.” *Washington Post*, January 6, 2017. https://www.washingtonpost.com/news/worldviews/wp/2017/01/06/this-kremlin-leader-bragged-about-tipping-a-u-s-presidential-election/.

Taylor, Derrick Bryson. “George Floyd Protests: A Timeline.” *New York Times*, sec. U.S., July 10, 2020. https://www.nytimes.com/article/george-floyd-protests-timeline.html.

Page 3196 of 3957

Taylor, S. J. *Stalin's Apologist: Walter Duranty, The New York Times's Man in Moscow*. New York: Oxford University Press, 1990.

Thompson, Isobel. "Did Russia Hack the Brexit Vote?." *Vanity Fair*, April 12, 2017. http://www.vanityfair.com/news/2017/04/did-russia-hack-the-brexit-vote.

Timberg, Craig, and Isaac Stanley-Becker. "QAnon Learns to Survive—And Even Thrive—After Silicon Valley's Crackdown." *Washington Post*, October 28, 2020. https://www.washingtonpost.com/technology/2020/10/28/qanon-crackdown-election/.

TMZ. "Jesse Ventura Considering Running for President, 'Trump Will Not Have a Chance!." November 28, 2018. https://www.tmz.com/2018/11/28/jesse-ventura-running-president-trump-wrestlemania/.

Tóth, Csaba. "Pro-Russian Jobbik 'Election Observers' Banned from Ukraine." *The Budapest Beacon*, November 4, 2014. https://budapestbeacon.com/pro-russian-jobbik-election-observers-banned-ukraine/.

Treisman, Daniel. "Why Putin Took Crimea." *Foreign Affairs*, April 18, 2016. https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-putin-took-crimea.

Tucker, Eric. "The Comey Firing, As Retold by the Mueller Report." *Associated Press*, sec. Criminal investigations, April 23, 2019. https://apnews.com/article/4ff1ecb621884a728b25e62661257ef0.

Tucker, Eric, and Chad Day. "Watchdog Finds Comey 'Insubordinate,' Not Biased in Clinton Email Investigation." *Chicago Tribune*, June 14, 2018. https://www.chicagotribune.com/news/nationworld/ct-clinton-email-case-20180613-story.html.

Tucker, Eric, and Jonathan Lemire. "Trump, GOP Launch Broad Attack on Russia Probe Foundations." *Associated Press*, May 13, 2020. https://apnews.com/article/ebcd45c5d89ac3cf8cc61ed3d6e1ac1a.

Tumblr. "Public Record of Usernames Linked to State-Sponsored Disinformation Campaigns." *Tumblr Help Center* (blog). November 16, 2018. http://tumblr.zendesk.com/hc/en-us/articles/360002280214-Public-record-of-usernames-linked-to-state-sponsored-disinformation-campaigns.

Twitter News Desk. "Twitter's Focus Is on a Healthy Public Conversation." *Elections Integrity* (blog). October 17, 2018. https://about.twitter.com/en_us/values/elections-integrity.html.

Page 3197 of 3957

U.S. Congress. House of Representatives. *House Committee on Armed Services. Countering Adversarial Propaganda: Charting an Effective Course in the Contested Information Environment: Hearing before the Subcommittee on Emerging Threats and Capabilities*. Hrg. 59, serial 97-493. 114th Cong., 1st sess., 2015.

———. *House Committee on Foreign Affairs, Confronting Russia's Weaponization of Information: Hearing before the Committee on Foreign Affairs*. Serial 114-37. 114th Cong., 1st sess., 2015.

———. Permanent Select Committee on Intelligence. "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements." Accessed September 30, 2020. https://intelligence.house.gov/social-media-content/default.aspx.

U.S. Congress. Senate. *Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 5: Counterintelligence Threats and Vulnerabilities*. S. Rep. 116-XX. 116th Cong. 1st sess., 2020. https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf.

———. *Committee on the Judiciary, Extremist Content and Russian Disinformation Online: Working with Tech to Find Solution*. 105th Cong. 1st sess., 2017. https://www.judiciary.senate.gov/meetings/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions.

———. *Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts against Election Infrastructure with Additional Views*. S. Rep. 116-XX. 116th Cong., 1st sess., 2018. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

———. *Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia's Use of Social Media with Additional Views*. S. Rep. 116-XX. 116th Cong., 1st sess., 2018. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

Ukrayins'ka Pravda [Ukrainian Truth]. "SBU likviduvala virus, shcho mav znyshchyty rezul'taty vyboriv [SBU eliminates virus that was meant to destroy election results]." May 23, 2014. https://www.pravda.com.ua/news/2014/05/23/7026217/.

United Press International. "Two Diplomatic Cables Called KGB Forgeries." July 14, 1983. https://www.upi.com/Archives/1983/07/14/Two-diplomatic-cables-called-KGB-forgeries/2457427003200/.

Page 3198 of 3957

University of Chicago Harris School of Public Policy and Associated Press-NORC Center for Public Affairs Research. *Americans Split on Relationship with Russia*. Chicago, IL: University of Chicago Harris School of Public Policy, 2020. https://apnorc.org/wp-content/uploads/2020/10/topline_release1.pdf.

van Herpen, Marcel. *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy*. Lanham: Rowman & Littlefield, 2016.

Vassilev, Ilian. "Thinking the Unthinkable—Bulgaria's Silent Exit from NATO and the EU." *Bulgaria Analytica* (blog). February 28, 2017. https://bulgariaanalytica.org/en/2017/02/28/thinking-the-unthinkable-bulgarias-silent-exit-from-nato-and-the-eu/.

Wahl, Elizabeth. "I Was Putin's Pawn." *Politico Magazine*, March 21, 2014. https://www.politico.com/magazine/story/2014/03/liz-wahl-quit-russia-today-putins-pawn-104888.html.

Walker, Robert E. "Combating Strategic Weapons of Influence on Social Media." Master's thesis, Naval Postgraduate School, 2019. https://www.hsdl.org/?view&did=828243.

Washington Post Staff. "Read the Full Testimony of FBI Director James Comey in Which He Discusses Clinton Email Investigation." *Washington Post*, May 3, 2017. https://www.washingtonpost.com/news/post-politics/wp/2017/05/03/read-the-full-testimony-of-fbi-director-james-comey-in-which-he-discusses-clinton-email-investigation/.

Watts, Duncan J., and David M. Rothschild. "Don't Blame the Election on Fake News. Blame It on the Media." *Columbia Journalism Review*, December 5, 2017. https://www.cjr.org/analysis/fake-news-media-election-trump.php.

Windrem, Robert. "Guess Who Came to Dinner with Flynn and Putin." NBC News, April 18, 2017. https://www.nbcnews.com/news/world/guess-who-came-dinner-flynn-putin-n742696.

———. "Mike Flynn's RT Headache Won't Go Away." NBC News, April 27, 2017. https://www.nbcnews.com/news/us-news/mike-flynn-s-rt-headache-won-t-go-away-n752216.

———. "Russians Launched Pro-Jill Stein Social Media Blitz to Help Trump, Reports Say." NBC News, December 22, 2018. https://www.nbcnews.com/politics/national-security/russians-launched-pro-jill-stein-social-media-blitz-help-trump-n951166.

———. "Senate Russia Investigators Are Interested in Jill Stein." NBC News, December 19, 2017. https://www.nbcnews.com/news/us-news/why-are-senate-russia-investigators-interested-jill-stein-n831261.

Page 3199 of 3957

World Council of Peace. *World Peace Movement: Resolutions and Documents*. Vienna, Austria: Secretariat of the World Council of Peace, 1955.

Wu, Nicholas. "What's the Dispute between Hillary Clinton and Tulsi Gabbard about?." *USA Today*, October 24, 2019. https://www.usatoday.com/story/news/politics/elections/2019/10/24/what-feud-between-tulsi-gabbard-and-hillary-clinton-about/4082268002/.

Zengerle, Patricia, and Warren Strobel. "FBI Head Denies Trump Wiretap Claim, Confirms Russia Election Probe." *Reuters*, March 20, 2017. https://www.reuters.com/article/usa-trump-russia-idUSL2N1GX1L8.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. 1st ed. New York: Crown Publishers, 2014.

———. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

Ziegler, Charles E. "International Dimensions of Electoral Processes: Russia, the USA, and the 2016 Elections." *International Politics; Basingstoke* 55, no. 5 (September 1, 2018): 557–74. http://dx.doi.org.libproxy.nps.edu/10.1057/s41311-017-0113-1.

Zubok, Vladislav, and Konstantin Pleshakov. *Inside the Kremlin's Cold War: From Stalin to Khrushchev*. Cambridge, MA: Harvard University Press, 1996.

Page 3200 of 3957

THIS PAGE INTENTIONALLY LEFT BLANK

Page 3201 of 3957

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

USAWC STRATEGY RESEARCH PROJECT

THE EVOLUTION OF STRATEGIC INFLUENCE

by

LTC SUSAN L. GOUGH
UNITED STATES ARMY

Professor Frank Jones
Project Adviser

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
07 APR 2003		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Evolution of Strategic Influence	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Susan Gough;	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050,	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**60**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Page 3205 of 3957

ABSTRACT

AUTHOR: LTC Susan L. Gough

TITLE: The Evolution of Strategic Influence

FORMAT: Strategy Research Project

DATE: 7 April 2003 PAGES: 60 CLASSIFICATION: Unclassified

This paper will examine the evolution of how the U.S. Government and the Department of Defense have organized to conduct strategic influence as an instrument of national power, from the Psychological Warfare Division of World War II, through the Psychological Strategy Board and Operations Coordinating Board of the early Cold War, through the Vietnam years to today. Are they organized effectively today to meet the asymmetric threats of the 21st Century?

Page 3206 of 3957

Page 3207 of 3957

TABLE OF CONTENTS

ABSTRACT……iii

THE EVOLUTION OF STRATEGIC INFLUENCE……1

WORLD WAR II ……3

EARLY COLD WAR ……6

TRUMAN……7

EISENHOWER……12

MIDDLE COLD WAR ……15

REAGAN AND BEYOND……20

STRATEGIC INFLUENCE TODAY ……28

THE WAY AHEAD ……33

ENDNOTES……39

BIBLIOGRAPHY……49

Page 3208 of 3957

Page 3209 of 3957

THE EVOLUTION OF STRATEGIC INFLUENCE

> It is the significant actions taken by government in and of themselves, the appropriate and most desirable arrangements of such actions, and the manner and emphasis of the publication of such actions to the world, that advance the struggle for men's minds and create a desirable climate of world opinion.
>
> —Robert Cutler

In the aftermath of the terrorist attacks on America in September 2001, both the American people and the U.S. Government tried to understand why some people could hate the United States so much that they would perpetrate such acts. Time and investigation into the motivations behind the terrorist acts have revealed that simply destroying terrorist organizations will not alter the conditions or mindsets that fostered such actions.

America has again entered a war of ideas, of hearts and minds - a war of ideologies as potent and potentially dangerous as the Cold War. Failure to succeed could have equally dire consequences as any envisioned in the struggle against the Soviet Union and Communism. Like the Cold War, this is a global war. Like the Cold War, the War on Terrorism needs to contain the wellsprings of Anti-Americanism to prevent further spreading, and then to erode and eventually eliminate those wellsprings. As before, this new war for the minds of men includes our friends, allies and neutral audiences, as well as hostile ones. Despite its lone superpower status, the United States will need the support of other nations to succeed on a long-term, global scale.

Since September 11, the Bush Administration has wrestled with how to organize and conduct a campaign to influence world audiences on a global scale – how to organize for strategic influence. In this paper, strategic influence is broadly defined as the deliberate, conscious coordination or integration of all government informational activities designed to influence opinions, attitudes, and behavior of foreign groups in ways that will promote U.S. national objectives, combined with other elements of national power to achieve maximum psychological effect.

Every act of government has a psychological impact. The movement of a carrier battle group from one end of the Mediterranean Sea to the other, for example, has a direct psychological impact on the countries in the area it departed and the countries near its new location. It may also indirectly influence other audiences around the world. The movement of the carrier becomes part of a strategic influence campaign when its movement was deliberately

directed and timed with White House and Department of Defense (DoD) press conferences, with State Department diplomatic endeavors, and with other government actions to magnify the psychological effect.

Strategic influence is nothing new; the United States has conducted strategic influence campaigns since its inception. The history of strategic influence in the United States has been a roller coaster, with ups and downs and occasional unexpected turns in new directions. And like a roller coaster, we always seem to end up back where we started. This oscillating approach has been a result of a peculiarly American outlook that using persuasion and influence at the national level is somehow unethical and inconsistent with a democracy, that using "psychological tricks" is "dirty" and immoral, and that it's completely unnecessary: there is no need to overtly persuade; the United States should just factually show the world who we are, and everyone will automatically recognize how wonderful we are and want to emulate us. The successful propaganda efforts of U.S. enemies also contributed to the American distaste in many circles for strategic influence. Anything that smacked of propaganda or psychological warfare became something that only the "bad guys" did: first the Nazis, then the Soviets. Fortunately, despite this attitude and resistance, most U.S. administrations in the latter half of the 20th Century recognized both the value and need for strategic influence.

Strategic influence and its elements have been known by many names: foreign information program, international information activities, political warfare, propaganda, psychological warfare, psychological operations, public information, public affairs, public diplomacy, international military information, information operations, influence operations, and perception management, to name just a few. Further, strategic influence has always had both overt and covert components.

Today, key informational components of strategic influence include public affairs, political warfare, political advocacy, public diplomacy and psychological operations. While each of the components contains a persuasive element to some degree, by themselves they do not constitute strategic influence. Public diplomacy by itself is not strategic influence. Psychological operations are not strategic influence. None of these components can be conducted in isolation in the 21st Century. Strategic influence constitutes the orchestrated combination of them all.

There is an accepted belief that history repeats itself, and that the mistakes of history will be repeated if we don't learn them. As the Bush Administration continues to prosecute the War on Terrorism, what can history teach us about organizing for strategic influence? How has the U.S. Government organized in the past to coordinate and conduct strategic influence? What

has been the DoD organization for and role in strategic influence? In a world where information, both true and false, is available worldwide, twenty-four hours a day, where events are broadcast worldwide virtually instantaneously, is the United States organized effectively to win the strategic influence battle of the War on Terrorism?

WORLD WAR II

The real crucible for the evolution of U.S. strategic influence was World War II. While there had been a successful foray into propaganda during World War I, that experience was fleeting. U.S. propaganda in World War I had no lasting impact on the people involved, the U.S. Government, or the War Department. World War II, however, laid the foundation for the future for strategic influence. While many people still had doubts about the efficacy of propaganda and psychological warfare, few had been unexposed to it. Propaganda was everywhere: on the home front, in local, national and international news, and across the battlefields. Names synonymous with early U.S. Government and DoD efforts in strategic influence had their seminal experiences in psychological warfare in World War II – Robert McClure, Robert Cutler, and Gordon Gray, to name just a few. And the impressions and experience of these and other World War II veterans directly affected the U.S. Government's approach to strategic influence through at least 1960.

At the outbreak of World War II, neither the U.S. Government nor the War Department had an organized capability to conduct psychological warfare. There were no committees trying to coordinate amongst the departments. No departments or agencies had offices or personnel dedicated to propaganda. The Army had no psychological operations units, and had not had a psychological warfare office on the staff since 1918.[1]

In early 1941, Colonel William B. Donovan conducted a fact-finding trip to the Middle East and Great Britain. Donovan was particularly impressed by Britain's system of coordinating and combining intelligence, counterintelligence, psychological warfare and unorthodox methods of sabotage, subversion and guerrilla warfare to achieve objectives. Upon his return, Donovan recommended that the U.S. establish a single agency to coordinate and control these same elements for the U.S. Government.

Donovan's recommendations, combined with the growing Nazi threat, apparently received support within the Roosevelt Administration. On 11 July 1941, President Franklin D. Roosevelt established the office of the Coordinator of Information (COI), with Donovan as its first director. COI had two divisions, Research & Analysis and the Foreign Information Service

Page 3212 of 3957

(FIS), plus sections for special intelligence and sabotage. FIS had the information piece, with a mission to explain U.S. policy everywhere except Latin America.[2]

Thus the initial seed for strategic influence was sowed. But conjoined to that seed from its inception was a disease that continues to plague strategic influence today: internecine and interagency rivalry, misperceptions, misinformation, and "turf" battles over control, frequently leading to deliberate roadblocks. Not everyone was happy with COI; too few people understood either psychological warfare or the infant "special operations."

Less than a year later, on 11 June 1942, Roosevelt dissolved the COI, replacing it with two new organizations: the Office of War Information (OWI), responsible for the psychological warfare function, and the Office of Strategic Services (OSS), responsible for special operations. Roosevelt created OWI due to a need to consolidate wartime information and psychological warfare activities in one agency and to better coordinate with the increasing number of agencies involved in propaganda. Roosevelt also desired to separate wartime propaganda from strategic intelligence and special operations. Over the next several months, additional presidential directives clarified the lines of responsibility between OWI and OSS. OWI had responsibility for domestic and overt psychological warfare, while OSS had the mission to conduct covert operations, including covert psychological warfare. Interestingly, the last such directive, in March 1943, directed that OWI coordinate its activities with the military services, but did not direct that OSS do the same.[3]

The War Department also began examining psychological warfare. In June 1941, John J. McCloy, the Assistant Secretary of War, formed a Special Study Group within G-2 to plan for future psychological warfare operations. This office eventually evolved into the Psychological Warfare Branch (PWB), G-2.[4]

Over the next year, a multitude of committees and groups were established to wrestle with psychological warfare issues: the Joint Chiefs of Staff (JCS) established a Joint Psychological Warfare Committee and a Joint Psychological Warfare Advisory Subcommittee; OSS established a Supporting Committee on Psychological Warfare; and Donovan chaired a Joint Psychological Warfare Advisory Committee that was chartered to coordinate psychological warfare activities with other government and civilian agencies outside JCS purview, including OWI and the State Department.[5]

This multitude of groups actually proved counterproductive at this stage of the development of strategic influence. In December 1942, the War Department disbanded the PWB. Too many agencies complained about the difficulty of defining psychological warfare and the various interpretations caused conflict within the Department. Interagency "turf" battles in

the new arena hampered any coordinated, constructive effort. JCS subsequently abolished all of its psychological warfare committees and gave OSS responsibility for military psychological activities. In response, the Army eliminated its PWB.[6] More than a year before the U.S. launched Operation Overlord, the top levels of the military bureaucracy had no psychological warfare offices, because they could not agree on a definition or who should be responsible for what activities.

However, the military was not bereft of psychological warfare assets. The same JCS document which disbanded the PWB and committees also gave the military theater commanders control of psychological warfare within their areas. This direction implicitly gave theater commanders the authority to determine their own relationship with OWI and OSS.[7]

Both the Pacific and European theaters conducted operational and tactical psychological warfare, controlled by organizations at the theater level. The theater commands created Psychological Warfare Branches or Divisions, depending on their needs. General Eisenhower activated the largest of these, the PWB at Allied Forces Headquarters (PWB/AFHQ), in North Africa in November 1942. By February 1944, PWB/AFHQ had expanded to become the Psychological Warfare Division, Supreme Headquarters, Allied Expeditionary Force.[8] At the tactical level, the Army established a number of Mobile Radio Broadcasting Companies, armed with print presses, loudspeakers, typewriters, radios, public address systems and leaflet bombs. These units operated much as military tactical psychological operations units do today, forming small teams that deploy forward to directly support the combat units.[9]

In November 1943, after much discussion and still with lukewarm endorsements, the Army reversed its earlier decision and established a Propaganda Branch in G-2 in November 1943. The new branch had responsibility to coordinate propaganda functions for the War Department, to staff OWI plans through JCS, and to provide an Army representative to the JCS liaison with OWI.[10]

Following World War II, despite advice to the contrary and the efforts of those involved, Army psychological warfare staffs and units virtually disappeared during the post-war drawdown. OWI and OSS also disbanded. By the outbreak of the Korean War five years later, the Army had only one operational psychological warfare troop unit.[11]

Two notable exceptions remained. In the occupied territories, the theater military Psychological Warfare Divisions became Information Control Divisions (ICD). The ICDs focused on “consolidation psychological operations” – gaining the cooperation of the civilian and military populace in the occupied area, creating favorable public opinions for Allied objectives for

the areas, and controlling all information sources as well as the dissemination of information within the occupied territories.[12]

At the War Department and Army headquarters, the Psychological Warfare Branch moved in late 1946 from the G-2 to the Policy Section, Plans and Operations Division. This marked the first recognition that psychological operations are operational in nature, and while intelligence supports psychological operations, psychological activities are not an intelligence function. However, centralization of psychological warfare still eluded the War Department. Responsibilities for different aspects of psychological warfare rested with several different agencies within the Department. Not until the Office of the Chief of Psychological Warfare was established in January 1951 did the War Department achieve centralization of effort.[13]

At the end of World War II, while writing about his experiences as Supreme Commander, Allied Expeditionary Forces, General Eisenhower noted:

> "In this war, which was total in every sense of the word, we have seen many great changes in military science. It seems to me that not the least of these was the development of psychological warfare as a specific and effective weapon…I am convinced that the expenditure of men and money in wielding the spoken and written word was an important contributing factor…Without doubt, psychological warfare has proved its right to a place of dignity in our military arsenal."[14]

When Eisenhower became President, psychological warfare became far more than just a piece of the military arsenal.

THE EARLY COLD WAR

The early Cold War years were a "Golden Age" for strategic influence. Veterans populated every department and agency of the U.S. Government – veterans, who, while they may not have been directly involved in psychological warfare, had seen the value and impact of such activities, and wanted to keep and utilize that capability in the future. Many people in government also correctly read the early evidence that the Soviet Union had also recognized the impact of propaganda during World War II, and was quickly building what would become a fearsome propaganda machine. The perspective of the country changed, too, in the aftermath of World War II and the beginning of the "Nuclear Age" – no longer could isolationism rule; the U.S. had to become the leader of the free world. Information and influence on the international scene grew in importance, as did the means to disseminate information.

The need for enhanced coordination of national security policy at the top levels of the U.S. Government arrived on the coattails of World War II. In June 1945, James Forrestal, Secretary of the Navy, asked Ferdinand Eberstadt, vice chairman of the War Productions

Board, to conduct a study on what form of postwar organization should be established to provide for national security. Forrestal requested recommendations not just for better organizing the War and Navy Departments, but also how to better integrate the military services with other government departments and agencies for national security matters.[15]

In his report to Forrestal, Eberstadt recognized that a new organization for the military services and their integration with other departments was just one piece of a larger problem that needed to be solved. He discussed the growing necessity to integrate and provide direction for all the departments and agencies within the U.S. Government towards a common goal and a unity of effort. Eberstadt also believed that stronger ties should be created among the military services, departments and agencies for strategy, logistics, planning, scientific research, mobilization, and "between the gathering of information and intelligence and its dissemination and use."[16]

To accomplish the necessary integration and direction, Eberstadt recommended the creation of a National Security Council to be the cornerstone of a new national security organization. Among its duties and functions as the formulator and coordinator for national security policy, Eberstadt recommended, "the Council should also control the policies and activities of the organizations responsible for the conduct of psychological and economic warfare."[17] Strategic influence, then, has been a part of the National Security Council since its inception.

TRUMAN

Two years later, on 26 July 1947, President Truman signed the National Security Act, to "provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to national security."[18] The National Security Act enacted many of Eberstadt's recommendations, including both the creation of the National Security Council, to advise the President on the integration of domestic, foreign, and military policies relating to national security, and the creation of the Central Intelligence Agency (CIA).[19]

The National Security Council's first foray into a national information policy came in December 1947, with the signing of National Security Council Memorandum (NSC) 4/4A, "Coordination of Foreign Information Measures." The National Security Council hoped this directive would correct the lack of coordination in a weak U.S. propaganda campaign, to counter the well-coordinated and increasingly effective Soviet propaganda campaign. NSC 4 dealt with overt information policy. The memorandum designated the State Department as the primary

coordinator of U.S. information policy, and created the Interagency Foreign Information Organization (IFIO). NSC 4 also identified the CIA and the Army's Chief of Information, under the Deputy Chief of Staff, as key supporters of the national propaganda effort. NSC 4 included the Navy's Division of Public Information and the Air Force Troop Information and Education Division as potential players as well. The latter agency, and others similar to it, was included in information policy organizations throughout the Cold War because Cold War psychological warfare and counter-propaganda campaigns also included protecting and arming troops against hostile propaganda. NSC 4A, a classified annex, directed the CIA to initiate and conduct covert psychological operations to counteract Soviet propaganda.[20] Echoes of OWI and OSS can be clearly seen in this delineation of effort between overt and covert operations.

IFIO members included the Joint Chiefs of Staff (JCS), the Office of the Secretary of Defense (OSD), CIA and the National Security Resources Board.[21] The Assistant Secretary of State for Public Affairs headed the organization. IFIO did little until the Korean War. During that conflict, IFIO issued weekly directives that were to be used by member agencies as a basis for their propaganda activities overseas. IFIO's more lasting contribution came from its chairman, Edward Barrett, who first suggested the creation of a National Psychological Strategy Board in August 1950 to more effectively coordinate the national effort. For Barrett and the State Department, however, it was also a move to demilitarize the Government's psychological warfare activities.[22]

Congress also maintained a keen interest in national information and security policy. After a visit to Europe, where they had been inundated with hostile Soviet propaganda, Senator H. Alexander Smith and Representative Karl Mundt sponsored the Smith-Mundt Act. This Act, which passed with little difficulty on 16 January 1948, "breathed life into overseas information programs," and laid the groundwork for the future U.S. Information Agency (USIA). The Smith-Mundt Act provided funds "to spread America's message to the world" through a variety of media, including radio, print, film and exchange programs."[23] The Smith-Mundt Act also directed that any such information and programs "shall not be disseminated within the United States, its territories, or possessions."[24] Congressional and Department of Defense General Counsels have interpreted this statute to also apply to military psychological operations.

In response to the concerns and disagreements between DoD and the State Department over the implications of NSC 4/4A, President Truman signed NSC 10/2 on 18 June 1948. This directive created the Office of Special Projects, to carry out covert activities that had been assigned to the CIA, including covert psychological operations. The Office of Special Projects carried out plans as formulated by the Departments of State and Defense, but reported only to

Page 3217 of 3957

the CIA. This gave State and Defense some input into covert operations, but kept responsibility for it within the CIA. To maintain the secrecy and security of the covert operations, the name of the office changed shortly thereafter to the more ambiguous Office of Policy Coordination.[25] One of CIA's early ventures included the establishment and covert funding of U.S.-controlled overseas broadcasting stations, including Radio Free Europe and Radio Liberty.[26]

As the Cold War continued to build, some officials in the Truman Administration argued that the U.S. needed to do more than it was currently doing to influence the world situation. Based on recommendations from an ad hoc committee headed by Paul Nitze, Truman signed NSC 68 on 14 Apr 1950. NSC 68 called for an intense program of both overt and covert economic, political and psychological warfare to influence the political and psychological conditions in both the Free World and Soviet areas, with a particular aim to foster unrest in Soviet satellite countries."[27] NSC 68 was the hallmark of the American containment strategy of the Cold War.

While the Truman Administration prepared to fight both the Cold War and a potential World War III, North Korea attacked South Korea in the Fall of 1950 and precipitated a new type of war – "limited" war. The Soviet role in the origins of the Korean War galvanized the need for better coordination and planning of psychological warfare at the national level. The Soviets increasingly used propaganda and other unorthodox methods to increase their sphere of influence. The United States needed to find ways to counter Soviet influence that would not trigger nuclear war. Recognition arose that this was as much a battle of ideas, a battle for the hearts and minds of men, as it was a battle of tanks and artillery. Political and psychological warfare became key weapons in the U.S. arsenal.

At the Pentagon, the Army activated the Psychological Warfare Division (PWD), G-3, to handle Army's psychological warfare responsibilities in both Korea and the growing Cold War. Six months later, the PWD became the Office of the Chief of Psychological Warfare (OCPW). OCPW was not a section within the G-staff, but a special staff office with over 100 personnel and a direct access to the Chief of Staff. OCPW had responsibility for developing Army psychological and special operations plans, recommending policies for psychological warfare and special operations, and supervising the execution of Army programs in the field.[28]

Within the Korean theater, the military organized theater, operational and tactical level military psychological units much like the ones in World War II – with one key advancement. The 1st Radio Broadcasting and Leaflet Group (1st RB&L) was specifically designed to conduct strategic propaganda in direct support of military operations and to further long-term strategic aims. The 1st RB&L targeted not just enemy forces, but foreign populations in both friendly- and

Page 3218 of 3957

enemy-occupied areas.[29] It was the first military psychological operations troop unit to have a strategic psychological mission.

On 4 April 1951, President Truman created the Psychological Strategy Board (PSB) to develop, coordinate and evaluate the national psychological strategy effort, including the formulation and promulgation of national psychological objectives, policies and programs.[30] The PSB had three principal tasks: "(1) to provide more effective planning of psychological operations within the framework of approved national policies; (2) to coordinate the psychological operations of all departments and agencies of government; and (3) to evaluate the effectiveness of the national psychological effort."[31]

The creation of the PSB was the first time the U.S. Government attempted to organize a national psychological effort for influencing international audiences above the military theater/operational level. PSB members included the Under Secretary of State, the Deputy Secretary of Defense, and the Director of Central Intelligence; JCS provided a representative as the principal military adviser. PSB had a full-time Director, an Executive Secretariat, and a staff. The staff was organized into three offices, each under an Assistant Secretary: Plans and Policy, Coordination, and Review. The PSB also established panels, made up of representatives from each Office, and others agencies as needed. Panels were created as needed to handle one issue, and reported to the Offices and directly to the Board.[32] The PSB was not technically a part of the National Security Council structure. Rather, it was an independent organization, but was required to report to the NSC on its activities and its evaluation of national psychological efforts.[33] An important distinction - the PSB was intended as a coordinating organization and was not authorized to perform psychological operations.[34]

Truman's first PSB director was Gordon Gray, former Secretary of the Army.[35] Gray took a very broad view of PSB's responsibilities. None of the directives governing the PSB provided a specific definition for "psychological strategy" or "psychological operations". Gray interpreted PSB responsibilities as having cognizance over anything that had a psychological impact. Since virtually any act by a nation has such an impact, Gray eventually believed that PSB should have the lead on all foreign policy matters short of formal hostilities. A clash with State was inevitable. State firmly believed that PSB should be restricted to just coordinating information and propaganda, and not other aspects of foreign policy. Over time, other agencies and departments also became concerned that PSB was overstepping its boundaries and becoming almost a second National Security Council. This friction and broad interpretation of responsibilities eventually led to the PSB's downfall.[36]

Page 3219 of 3957

Gray's early priorities on taking charge, however, are still a model for today: development of a strategic plan, an estimate of the current situation, a statement of objectives, a plan for reaching national goals, and a clear delineation of responsibilities. Gray was also an early proponent of the need to improve understanding of the scientific aspects of psychological operations.[37]

Additional specific tasks and responsibilities for psychological operations were articulated in NSC 59/1, which covered overt propaganda efforts and established the Psychological Operations Coordinating Committee, and NSC 10/5, signed 21 October 1951, which expanded on NSC 10/2, reaffirming CIA responsibility for covert operations, including covert psychological operations, and calling for intensified covert action.[38] At this time, there were three key players in strategic influence: CIA, State and DoD. On 16 January 1952, State Department established the International Information Administration as its information arm that coordinated with PSB.[39]

In response to the establishment of the PSB and the additional psychological operations tasks specified in NSC Memorandums 10/2, 10/5 and 59/1, the Department of Defense (DoD) published DoD Directive C-5132.1 in April 1952, titled "Organization, Office of Psychological Policy." This directive established the Office of Psychological Policy, under the Assistant Secretary of Defense for International Security Affairs. The new office was headed by a Deputy for Psychological Policy, formally known in Defense parlance as the Deputy Assistant to the Assistant Secretary of Defense for International Affairs – Psychological Policy. DoD signaled the importance it gave this new office by specifying in the directive that the Deputy for Psychological Policy "shall have direct access to the DoD member of the PSB on matters pertaining to PSB and to the Assistant Secretary of Defense for International Security Affairs on other matters."[40]

The directive laid out DoD responsibilities, which included developing DoD positions on all PSB objectives, policies and programs; providing representation to the PSB and its panels, to the Consultant's Committee established by NSC 10/2, to any ad hoc committees established by NSC 10/5, and to the Psychological Operations Coordinating Committee established by NSC 59/1; and ensuring coordination with all DoD departments and agencies participating in any of these committees' activities.[41]

The role of DoD in peacetime psychological operations was not clear in DoD, let alone the other departments. The other departments tended to believe that, while DoD had a clear role in psychological warfare during hostilities, it didn't have much to do in peacetime. Some senior officials in DoD, though, felt that DoD capabilities could be utilized more effectively in

peacetime than the limited scope envisaged by other departments. DoD began to make a case for a larger role in psychological operations and planning its portion of the PSB's first status report, outlining the planning it had already done for wartime, when most of the U.S. propaganda machine would be subordinated to military goals. In the report, DoD also called for increased use of military assets for peacetime propaganda value.[43] In March 1952, the Army established the Psychological Warfare Center at Fort Bragg, North Carolina, to train both psychological operations and special operations personnel and units.[44] In late 1952, DoD further supplemented and expanded on its policy and roles regarding psychological operations with DoD Directive S-3140.1.

Two of the key purposes in DoD Dir S-3140.1 were establishing authority for using DoD capabilities to conduct psychological operations when not at war, and establishing a DoD Committee on Psychological Operations to more effectively coordinate and integrate DoD psychological operations efforts in the national psychological operations effort.[45] The directive also sought to increase senior official attention on psychological operations, and to enhance continuity, consistency, security and timeliness of psychological actions. To ensure that psychological operations received the necessary consideration at the top levels of the policy decision-making chain, DoD directed the Services Secretaries to assign functional responsibilities for psychological operations to Under Secretaries or Assistant Secretaries, and directed the Joint Chiefs of Staff to assign responsibility for military psychological matters to a general or flag officer. These officials, plus a representative from the DoD Office of Public Information, constituted the members of the new DoD Committee on Psychological Operations, headed by the Deputy for Psychological Policy. As with the earlier directive, DoD declared the significance of these new responsibilities by stipulating that the committee members "shall be specifically empowered to have necessary access to key personnel within their respective departments in all matters concerning psychological problems with which they are concerned."[46] The committee's purpose included securing the exploitation and integration of DoD potential in psychological operations and securing DoD viewpoints on psychological operations matters. The committee's initial task included developing and submitting an outline of the specific roles, objectives and capabilities of DoD to conduct psychological operations during the Cold War.[47]

EISENHOWER

The "Golden Age" for strategic influence continued under Eisenhower. Due to his wartime experience, Eisenhower came to the presidency with a clear idea on the uses and effectiveness of information and psychological warfare. He also had some very firm ideas about

the need for coordination at the highest level of government to win the battle against Communism. In a campaign speech in 1952, he spoke about the need to coordinate every significant act of government, to time and direct all the departments' actions, to produce the maximum effect.[48] In his second National Security Council directive, Eisenhower stated, "psychological operations are established instruments of national power."[49]

Early in 1953 Eisenhower established the President's Committee on International Information Activities (PCIIA), to examine in depth the nation's Cold War information policy. The committee was headed by William H. Jackson, a lawyer and former Deputy Director of the CIA, and included other notables in Eisenhower's Administration: Robert Cutler, Eisenhower's first National Security Adviser and a one-time member of the PSB; Gordon Gray, who would later become one of Eisenhower's National Security Advisers; John C. Hughes, one of Eisenhower's aides; and C.D. Jackson, a former member of the OWI who had worked with Eisenhower during World War II and Eisenhower's future PSB Director.[50]

The PCIIA report, published in June 1953, criticized the current state of information policy and the PSB in several areas. First, while the PSB had accomplished significant planning and provided guidance to the other agencies, it lacked the power and authority to effectively coordinate within an uncooperative interagency environment and to ensure implementation of its plans and policy guidance. Second, the PCIIA criticized the Truman Administration for conducting a defensive campaign against the Soviet regime, and urged Eisenhower to take the offensive in psychological warfare. And, third, they felt that the PSB had gone too far in developing an independently existing psychological strategy that was not integrated with overall national strategy. The name itself fostered a misconception that psychological strategy could be separated from every act the nation took.[51]

At this time, the National Security Council was an advisory board, not a coordinating agency. There were no interagency working groups, no policy coordinating committees as there are today. There was not even a National Security Adviser yet. PSB, at least while under Gray, had tried to fill that coordinating role, but without the proper authority, was unsuccessful.

Amongst PCIIA's recommendations, Eisenhower enacted three key ones that were to have a profound effect on national security policy-making and psychological warfare under his Administration: the creation of the Special Assistant to the President for National Security Affairs, the creation of the Operations Coordinating Board, with the subsequent abolition of the PSB, and the creation of the USIA.

Cutler, in a separate report to Eisenhower, first recommended that the President's Special Assistant for Cold War Planning become an adviser to the National Security Council,

Page 3222 of 3957

with the corresponding elimination of the PSB Director as an observer. Not long after, the Cold War Planning position became the President's Special Assistant for National Security Affairs, and Eisenhower chose Cutler as his first National Security Adviser.[52]

PCIIA strongly recommended replacing the PSB with the Operations Coordinating Board (OCB) to "coordinate and integrate psychological with national strategy and, more importantly, to act as the coordinating and integrating arm of the National Security Council for all aspects of the implementation of national security policy."[53] PCIIA clearly intended to fix some of PSB's problems, and signaled a change in the view of the National Security Council from advisory to coordinating. This was also the birth of the modern National Security Council interagency committee system.

Eisenhower established the OCB by Executive Order 10483 on 2 September 1953. Like the PSB, OCB was not originally within the NSC structure, but a separate agency that reported to it. The order also designated the Under Secretary of State as OCB chair. According to Cutler, the OCB would coordinate and "ride herd on" the performance and policies of all departments and agencies responsible for carrying out national security policy, and would be "constantly mindful" of the psychological implications of their actions.[54]

In January 1954, Eisenhower signed a National Security Council Memorandum that delineated the responsibilities for the departments and agencies participating in foreign information programs and psychological operations under his new National Security Council system. OCB responsibilities, with respect to psychological operations, included initiating new proposals for action, advising agencies on their operational planning responsibilities, coordinating the interdepartmental aspects of those plans, and orchestrating the timely execution of psychological operations to ensure their full contribution to the attainment of national security objectives.[55]

The third key recommendation of the PCIIA was the creation of the USIA. Truman had created the International Communications Agency to manage the activities under the Smith-Mundt Act.[56] Based upon the PCIIA report, Eisenhower created the USIA to perform the same work, but now as an autonomous agency reporting directly to the National Security Council. The USIA Director regularly attended National Security Council meetings as an observer.[57]

Eisenhower's directive gave USIA responsibility for coordination of policies, plans and operations for the national foreign information program. USIA also had responsibility for disseminating to other departments guidance concerning the official treatment of news in foreign information outlets. In another attempt to correct the PSB's problems, the memo also stipulated that such guidance was authoritative for all departments and agencies. The directive also drew

a line between USIA and DoD responsibilities: USIA had responsibility for the foreign information program only in areas that were not military theaters of operations or where U.S. troops were actually engaged in combat operations. Since this NSC Memorandum also reconfirmed CIA's responsibility for covert psychological operations in accordance with the applicable NSC directives (NSC 10 series), this relegated DoD to military psychological operations matters only, and an advisory role for the rest.[58]

This same directive also rescinded NSC 59/1, which had established the Psychological Operations Coordinating Committee (POCC), and established a new organization to provide OCB with a forum for carrying out its psychological operations responsibilities. Chaired by the Executive Secretary of OCB, other members included representatives from DoD, State, CIA, JCS, USIA, and the Foreign Operations Administration. The Service's psychological warfare chiefs established in DoD Directive S-3140.1 served as consultants. All of the members also provided personnel to be a full-time staff, with OCB providing administrative support.[59]

Throughout the rest of his time in office, Eisenhower continued to refine his mechanisms for coordinating national security policy and the national psychological operations effort. On 25 February 1957, Executive Order 10700 changed OCB's status from an independent coordinating board to actually part of the National Security Council structure. The Executive Order also changed the OCB chairman from State Department to whomever the president designated[60] – and Eisenhower's first choice was Gordon Gray.[61]

On 4 June 1958, Eisenhower signed NSC 5812/1, which dealt with wartime responsibilities for psychological operations. Recognizing that "no single department or agency having responsibility in the field of psychological operations can feasibly perform these operations for the entire Executive Branch," this directive specified the responsibilities of DoD, CIA, USIA and DoD under a variety of conditions. Eisenhower covered not just the general wartime responsibilities, but also which department or agency was in charge, depending on whether the target audience was friendly, neutral or hostile, and within or without the theater of operations. The directive also specified the workings of the coordination and flow of guidance from Washington to overseas and back.[62]

THE MIDDLE COLD WAR

The next two decades after Eisenhower's term constituted an "Ice Age" for strategic influence. The interagency structures and committees that Truman and Eisenhower built to coordinate strategic influence disappeared. The psychological warfare offices in DoD, JCS and

the Army dissolved, as did their coordinating committees. The few people on the staff who retained some responsibility, now lowly action officers rather than generals or Assistant Secretaries, lost direct access to the decision makers – an access that has never been regained. The military psychological troop units demobilized after the Korean War, except for one lone unit at Fort Bragg. Even before President Kennedy's assassination, the focus of the Psychological Warfare Center had changed to special operations – even the name had changed, to Special Warfare Center. As one writer put it, "The congenial climate for American psychological operations was polluted in the seventeen years that followed 1956; not until President Reagan's Westminster speech was there again much sunshine."[63]

Subsequent administrations still used information and psychological methods in the Cold War, but they no longer received top-level attention. The elements of strategic influence still existed, but were compartmentalized throughout the departments. CIA retained the covert operations mission. State Department conducted its traditional foreign diplomacy mission, and USIA had the overt foreign information mission. However, starting in the 1960s, the USIA shifted focus. The informative function, focusing on objective, factual reporting of news, gained emphasis, while attention on the persuasive function and the function of advising other departments on psychological implications declined.[64]

The various administrations during this period did not create any permanent overarching committees to coordinate psychological activities within the government. Departments and agencies were expected to coordinate with the others, but no one "ran the show". There was no national level effort to direct and coordinate the timing of acts to ensure maximum effect. Ad hoc committees sometimes appeared to fill the vacuum, but these were usually narrowly focused and of short duration.

Party politics played a key role in this change. Eisenhower carried over into his Administration people who had been key in Truman's Administration, such as Gordon Gray. Kennedy, much like modern presidents, brought in a whole new team. Kennedy also, both personally and as a Democrat, had a vastly different view of the role of the National Security Council and its organization.

Another key factor appears to be the loss of a voice of sufficient stature to influence the top levels of the government. This may have been due to a generational change and lack of direct experience. The Truman and Eisenhower Administrations had been filled with high-ranking World War II veterans who had worked together, or at least known one another, during the war, and who had had to consider the implications of psychological warfare at the theater level. Starting with Kennedy, World War II veterans in the Administration tended to have been

junior or field grade officers, with virtually no propaganda experience except at the receiving end. Truman and Eisenhower had many advocates for strategic influence; Kennedy and Johnson had few.

Prior to Kennedy taking office, Senator Henry M. Jackson headed a congressional inquiry into government methods for formulating national policy in the Cold War. Jackson's report was highly critical of Eisenhower's National Security Council system, deeming it a bloated paper mill that didn't accomplish much real work, and that exceeded what he envisioned as the proper role for the Council. Jackson viewed the National Security Council as a small forum of intimates for the President to explore intelligence and policy options; he believed it ill-suited for comprehensive coordinating and follow-through of responsibilities.[65]

Jackson recommended a complete reorganization of the National Security Council, starting with the abolishment of the OCB. He believed that State Department should not only have control over foreign information policy, but should also be the agent of coordination on all major policies toward other nations. In his view, OCB infringed on this basic responsibility. Jackson also saw no need for permanent interdepartmental committees. He believed that the lead agency should have responsibility for implementation of policies cutting across departmental lines, with possibly the assistance of an informal, temporary interdepartmental group.[66]

Jackson's views dovetailed completely with Kennedy's own views. Less than a month after taking office, Kennedy issued Executive Order 10920, abolishing the OCB. Over 45 interagency committees died with OCB. In the next few weeks, Kennedy continued to dismantle Eisenhower's system, abolishing another 40 interdepartmental groups. The National Security Council staff decreased significantly and lost much of its power.[67]

Kennedy did not completely abandon psychological warfare, due to the focus on counter-insurgency throughout his term. Kennedy issued a number of National Security Action Memorandums (NSAM) directing increased emphasis, spending and action in counter-insurgency. While psychological activities rarely received primacy, they were normally imbedded in many of these policy directives. Four in particular demonstrated that the Administration did not ignore information as an element of national power.

NSAM 3, issued 15 April 1961, directed the Bureau of Budget to study continued CIA funding of activities such as Radio Free Europe, and whether open government support would be better. Someone had raised the very valid concern that if the CIA cover were compromised, the program would lose credibility and therefore most of its effectiveness.[68]

NSAM 61, issued 14 July 1961, directed the State Department and USIA to use their means to support and disseminate an approved counter-theme to combat a Soviet propaganda theme called “peaceful coexistence”.[69]

NSAM 63, issued ten days later, directed the State Department, through the USIA, to provide foreign policy guidance to all international radio broadcasting and television stations controlled by U.S. Government agencies. These included DoD stations, such as the Armed Forces Radio and Television Service and the Voice of the United Nations Command in Korea. NSAM 63 also gave the USIA the authority to preempt any of these stations as needed for “special programs”.[70]

Kennedy did establish some interdepartmental groups, which he called “Special Groups”. On 18 January 1962, NSAM 124 established the Special Group (Counter-Insurgency). Special Group (CI) functions included insuring that all U.S. Government agencies recognized that subversive insurgency was a major form of politico-military conflict on a par with conventional war, and that such recognition was included in the “political, economic, intelligence, military aid and informational programs conducted overseas by State, Defense, [U.S. Agency for International Development], USIA and CIA.”[71]

During the Vietnam years, the U.S. Government and DoD again established a fairly robust psychological operations effort to support the war. But this effort was narrowly focused to that theater, primarily tactical in nature, and did not last once the war ended.[72]

A study on national coordination of psychological operations conducted by the Joint Staff in the early 1970s noted that an ad hoc committee approach had arisen to fill the void caused by both a lack of coordination and insufficient authority at high enough level providing guidance for psychological operations. One example cited was the Psychological Operations in Critical Areas Watch Committee (POCA). Another ad hoc group, the Interagency Working Group on Psychological Operations in Critical Areas, had formed POCA based upon a 1965 USIA study. The Joint Staff deemed POCA moribund at the time of its study, as POCA had had no meetings since May 1969, even though the memorandum of agreement establishing it was still valid.[73]

Military psychological operations units during the Vietnam years traveled the familiar roller coaster track. In the 1960s, the Army had just one psychological operations unit. At the height of the Vietnam War, the Army had a full Group operating in Vietnam, and other psychological operations units stationed in Fort Bragg, Germany, Panama and Okinawa. By the mid-1970s, all that remained in the active component was one Psychological Operations Group – undermanned and with poor, antiquated equipment.[74]

President Johnson's national security system was modeled after Truman[75], but regarding strategic influence resembled Kennedy's. USIA clearly had the lead on psychological warfare programs, and the emphasis was on Southeast Asia.[76] While Johnson strengthened the National Security Council and established interdepartmental working groups, none appear to have dealt directly with strategic influence or psychological operations. A few, limited-scope ad hoc bodies did appear: the Vietnam Psychological Operations Working Group, which had been dormant for over a year by 1967, and the Psychological Operations Pressure Operations Group, which appeared briefly during the latter stages of the Vietnam War.[77] Like Kennedy, Johnson believed that the State Department should have the lead in foreign policy. In March 1966, Johnson signed NSAM 341, which gave the Secretary of State authority and full responsibility for the overall direction, coordination and supervision of interdepartmental activities overseas.[78]

President Nixon reformed the National Security Council more along Eisenhower's lines. Regarding strategic influence, though, he did not resurrect anything similar to the Psychological Strategy Board or the Operations Coordinating Board. Nixon continued a multi-pronged approach with CIA, State, and USIA, responsible for covert psychological operations, public diplomacy and overt information programs, respectively. DoD continued to have responsibility for psychological operations only in military theaters of operations.

Nixon did issue a number of National Security Decision Memorandum (NSDMs) which had informational or psychological components: NSDM 3, "Direction, Coordination and Supervision of Interdepartmental Activities Overseas"; NSDM 7, "Direction, Coordination and Supervision of Interdepartmental Groups"; NSDM 19, "Washington Special Actions Group"; NSDM 23, "Vietnamese Special Studies Group"; and NSDM 40, "Responsibility for Conduct, Supervision and Coordination of Covert Action Operations". Only one dealt directly with psychological operations: NSDM 63, "Psychological Warfare Operations Against Vietnamese Communists".[79] This NSDM continued the national-level narrow strategic influence focus on the Vietnamese theater, as opposed to a global focus. Unfortunately, further information dealing specifically with these NSDMs or the establishment of any ad hoc interagency committees was unavailable or still classified.

The lack of attention at the upper levels of the government on strategic influence and the limited focus on Southeast Asia led to a reduction in effectiveness against Communist propaganda worldwide. Most U.S. efforts outside the Vietnam theater were negated by the virulent anti-Vietnam movement, and the highly effective Soviet and Communist psychological operations programs, which were both strategic and global.[80] At the time, both JCS and the Army strongly recommended the establishment of a permanent standing committee with

broadened responsibilities to coordinate implementation by all government agencies of the psychological aspects of decisions rendered by the National Security Council.[81] Their recommendations fell on deaf ears. As one writer put it, "During the Vietnam years, in spite of some notable successes with psychological and political techniques of counterinsurgency warfare, the US military and the government as a whole proved unable to devise and execute an overall strategy that took due account of the vital importance of the psychological-political dimension of the struggle."[82]

President Carter continued the separation of the elements of strategic influence among CIA, USIA, State Department and DoD. However, in his restructuring of the National Security Council system, he established two new committees that included information policy within their scope, but not as a primary focus. The Policy Review Committee developed national security policies in those areas that were the primary responsibility of one department but where the subject also had important implications for other departments. These areas included foreign policy issues with significant military or interagency aspects and defense policy issues having international implications. The Special Coordinating Committee handled sensitive intelligence activities and covert operations.[83]

REAGAN AND BEYOND

Under President Reagan, strategic influence experienced a rebirth, buoyed by his emphasis on foreign policy and determination to win the Cold War. During his terms in office, the press dubbed Reagan "the Great Communicator" for his ability to use his speeches to gain support for his policies. It is an equally apt term for what he accomplished for strategic influence.

Reagan's initial national security strategy contained four basic components: diplomatic, economic, military and informational.[84] This was the first time that information had been elevated from a supporting instrument to a top element of national strategy. This emphasis on information and the psychological component – on strategic influence – of national security strategy continued throughout his terms.

Three National Security Decision Directives (NSDDs) built the cornerstone of Reagan's strategic influence policy: NSDD 45, signed 15 July 1982; NSDD 77, 14 January 1983; and NSDD 130, 6 March 1984.

NSDD 45 revitalized the U.S. international broadcasting program, declaring it an important instrument of national security policy. It directed quantum improvements in the quality and capabilities of US-controlled broadcasting stations, such as Voice of America, Radio Free

Europe/Radio Liberty, and Radio in the American Sector of Berlin. The directive established Radio Marti, to garner and consolidate anti-Castro support in Cuba and among Cuban exiles in the U.S. Reagan specifically stipulated that the money and other resources required to implement his improvements were to be given the same priority as other programs deemed vital to the national security.[85] NSDD 45 also directed that State Department give high priority to the diplomatic requirements for modernizing and expanding these stations, with particular emphasis on obtaining international support to halt and deter Soviet jamming of the stations and to develop countermeasures to that jamming.[86] Reagan foresaw the future of space-borne platforms and initiated further research into direct broadcasting by satellite. Finally, NSDD 45 directed a study between State and DoD on closer integration and role of broadcasting facilities in crisis and war.[87]

NSDD 77 established a Special Planning Group (SPG) under the National Security Council to strengthen the organization, planning and coordination of the various aspects of public diplomacy related to national security. Chaired by the President's National Security Adviser, SPG members included the Secretaries of State and Defense, the Director, USIA, and the Assistant to the President for Communications, with other agencies invited as needed. The directive indicated the importance Reagan placed on strategic influence by listing department and agency principals as the primary members, although they could designate an alternate.[88]

NSDD 77 also established four interagency standing committees that reported to the SPG: the Public Affairs Committee, the International Information Committee, the International Political Committee, and the International Broadcasting Committee. The latter committee had responsibility for planning and coordinating international broadcasting activities pursuant to NSDD 45.[89]

NSDD 77 gave the Public Affairs Committee responsibility for the planning and coordination of major speeches on national security subjects, and for the planning and coordination of public affairs for foreign policy events and foreign and domestic issues with a national security dimension. The International Information Committee had responsibility for planning, coordinating and implementing international information activities in support of US national security interests. This committee dealt almost exclusively with USIA activities, and was chaired by the Director, USIA.[90]

The International Political Committee had a broader role than the other three. Headed by the State Department, it had responsibility for planning, coordinating and implementing international political activities in support of US national security interests. These activities included State Department's role in foreign aid, in training and organizational support for

democratization, and coordination and cooperation with non-government organizations and private voluntary organizations that supported democratization. NSDD 77 specifically directed the International Political Committee to develop means to increase the U.S. Government capability to promote democracy, "as enunciated in the President's speech in London, 8 Jun 82," known as the Westminster speech. The directive also directed the committee to develop and implement plans, programs and strategies to counter totalitarian ideologies and political action by the Soviets. Additionally, NSDD 77 gave the State Department some authority to direct other departments to implement political action strategies in support of objectives established by the International Political Committee.[91]

While Reagan was generally pleased with the progress made under NSDDs 45 and 77, he did not feel that the departments had gone far enough, nor that they were maintaining focus. On 6 March 1984 he signed NSDD 130 to re-emphasize and clarify his policy on strategic influence.[92]

NSDD 130 reiterated the importance of U.S. international information programs to national security, expanded Reagan's policies set out in NSDDs 45 and 77, and directed "sustained commitment over time to improving the quality and effectiveness of U.S. international information efforts" – including improving the level of resources devoted to international information activities and their coordination with other elements of national power. Areas highlighted for improvement included designing products for different cultural target audiences, further enhancing international radio broadcasting, and reconstituting a program for disseminating books and other publications abroad. NSDD 130 directed studies into more effective use of international television broadcasting, including the new audio and videocassette technologies, and into how to utilize new communications technologies to penetrate closed societies. NSDD 130 also addressed functional and personnel requirements, including development of career tracks and education programs.[93]

NSDD 130 also directed great changes and improvements for DoD. First, NSDD 130 directed DoD to give a high priority to the revitalization and full integration of PSYOP in military operations and planning. Second, Reagan directed DoD to participate in overt PSYOP programs in peacetime. Third, he tasked the SPG to lead the development of coordinated interagency international information plans that included utilizing DoD capabilities. Fourth, NSDD 130 directed all departments and agencies to develop special procedures to ensure policy consistency and timeliness in international information programs during crisis and war.[94]

When NSDD 130 was published, DoD undertook a major review and evaluation of military psyop capabilities. That review showed that DoD capabilities had significantly atrophied

Page 3231 of 3957

since the Vietnam War. DoD's solution to correct its deficiencies was the DoD Psychological Operations (PSYOP) Master Plan of 1985. This watershed document provided a comprehensive plan for the fundamental improvement of DoD PSYOP capabilities worldwide, across the spectrum of conflict.[95]

Throughout DoD, PSYOP offices were re-established or improved. DoD created a PSYOP directorate, the first such office on the staff in over 20 years. JCS upgraded its PSYOP staff element from a branch to a division. The Department of the Army Staff upgraded its PSYOP staff element from a one-man shop to a PSYOP and Civil Affairs division.[96] Both Active and Reserve PSYOP units experienced growth in personnel, more funding for training, exercises and operations, and received updated equipment.

One important directive of the Master Plan was the separation of PSYOP staff elements from special operations staff elements throughout DoD, including the military departments, the Joint Staff, Service staffs, unified and specified command staffs and their components. The DoD review had determined that the subordination of PSYOP personnel under special operations "de-linked" the PSYOP personnel from broad support of national policy and objectives and critical interagency coordination. The Plan also noted that PSYOP personnel in special operations staffs tended to work PSYOP issues only part-time, and the placement within special operations staffs contributed to a continuing lack of understanding within DoD of PSYOP. It also tended to reinforce the misperception by both military and civilian senior leaders that PSYOP focused primarily on special operations.[97]

The 1985 PSYOP Master Plan also called for the creation of a Joint PSYOP Center (JPOC), dedicated to the long-term development and nurturing of joint PSYOP capabilities in DoD. Among the responsibilities envisaged for the JPOC would have been developing long-range strategic PSYOP plans, and assisting both JCS and the Office of Secretary of Defense (OSD) to develop, plan and coordinate the DoD portion of national psychological operations activities. DoD placed the implementation of the JPOC on hold pending resolution of several issues resulting from the congressionally mandated reorganization of special operations, including the creation of the U.S. Special Operations Command (USSOCOM). Once military PSYOP was placed under USSOCOM, the implementation of JPOC was never executed – lost in the internecine battle for resources within USSOCOM.[98] Nevertheless, the other directives within the PSYOP Master Plan greatly strengthened and improved military PSYOP.

Reagan provided additional guidance to DoD for increasing psychological operations with Executive Order 12333. Reagan wanted to increase and expand the execution of

democratization programs in Latin America. The EO established a presidential finding for CIA covert psychological activities and directed DoD to initiate several programs in the region.

On 26 July 1984 DoD published DoD Directive S-3321.1, *Overt PSYOP Conducted by Military Services in Peacetime*, in direct response to NSDD 130 and Executive Order 12333. This directive is still valid and used daily as the policy guidance for peacetime PSYOP. DoD Directive S-3321.1 established the Overt Peacetime PSYOP Program (OP3), still operative today. Under OP3 each regional combatant commander develops and submits a plan for conducting peacetime psychological activities to support combatant commander and national security objectives within their area of responsibility. These activities are not limited to military PSYOP units, nor even to military activities – regional combatant commanders can recommend that other departments execute certain activities. Combatant commanders coordinate their OP3 plans with Ambassadors in their region, and then submit the plans to JCS. JCS obtains concurrence within the military side of the Pentagon, while concurrently sending the proposed OP3 plans to OSD. OSD then coordinates within the interagency for review, comment and deconfliction. JCS passes approval of the plans back to the combatant commander once OSD has approved the plans. This process ensures that all the key players have had an opportunity to review the OP3 plans before the combatant commander executes the plan. [99]

Reagan also created the National Endowment for Democracy (NED) as a mechanism for overseeing disbursement of funds for the support of democratic political and cultural institutions abroad.[100] In his Westminster speech, Reagan proposed an initiative "to foster the infrastructure of democracy – the system of a free press, unions, political parties, universities – which allows a people to choose their own way, to develop their own culture, to reconcile their own differences through peaceful means."[101] Congress authorized NED as part of the Fiscal Year 1984/85 State Department Authorization Act. Since its inception NED worked closely with State, USIA and, especially, private sector groups to foster abroad cultural values, institutions and organizations of democratic pluralism. By 1992, both Canada and the United Kingdom had developed similar grant programs. NED is still extant today as an independent organization which continues to work with the private sector to promote democratic institutions around the world.[102]

Despite a setback from the Iran-Contra Affair, the success and potency of Reagan's strategic influence program directly contributed to President George Bush's ("Bush I") success in building and maintaining a coalition during the Gulf War. Reagan's improvement of U.S. military PSYOP capabilities also directly resulted in a highly successful psychological operations campaign during the conflict.

When Bush I took office, many "Reaganites" continued to serve in the new administration. Bush I continued many of Reagan's policies and practices, but not all of them. Many of the Reaganites tried to re-establish the best of Reagan's conventions, particularly those dealing with strategic influence. However, none were of sufficient stature to "carry the torch" through either the aftermath of Iran-Contra or the distraction of the re-election season. During the Gulf War, Bush's National Security Council did establish and chair an ad hoc committee, the PSYOP, Propaganda and Public Diplomacy Committee (3PD). 3PD included representatives from OSD, State Department, USIA, CIA and JCS. The committee generally met at least twice a week, and focused on coordination and exchange of information between the participating agencies, rather than tasking or execution of activities. 3PD ended quickly after the Gulf War. OSD and JCS, with positive endorsements from the other members, led a drive to get it permanently established, but NSC never took action. Most of the senior Administration officials did not see the utility of a standing committee in peacetime.[103]

On 28 March 1990, Bush I signed National Security Review (NSR) 24. NSR 24 directed a broad examination of U.S. Government international broadcasting activities in the context of overall U.S. foreign policy objectives. The dramatic changes in the word political situation – the reintegration of Germany, the fall of the "Iron Curtain" and the pending dissolution of the Soviet Union – prompted the complete review of the mission, objectives and resource implications of government broadcasting. Bush I intended to use the response to NSR 24 for short-term decisions in the next two years. The NSR was very comprehensive, including directives for both a detailed assessment of current and future roles, and for the development of a broad range of policy options.[104]

Six months later, Bush I superseded NSDD 77 with National Security Directive (NSD) 51. NSD 51 reaffirmed the four basic missions for U.S. Government international broadcasting: explaining U.S. policies and actions to foreign audiences; describing and explaining American culture and institutions; providing objective news, commentary and information about U.S. and world events; and providing surrogate programming to areas of U.S. interest where there is not a free press. Additionally, NSD established a Policy Coordinating Committee on International Broadcasting, chaired by State. However, NSD 51 also directed the consolidation of broadcasting operations and other austerity measures due to constrained budget levels.[105]

Perhaps the most important directive in NSD 51 was the appointment of an independent bipartisan task force to study U.S. broadcasting assets, activities and technologies. Further, Bush I directed the task force to provide him with recommendations on the most appropriate organization and structure for a single U.S. Government broadcasting entity. This was the

genesis of the Broadcasting Board of Governors (BBG). . On 1 October 1 1999, as part of the 1998 Foreign Affairs Reform and Restructuring Act, the BBG became an independent, autonomous entity responsible for all U.S. Government and government sponsored, non-military, international broadcasting.[106]

One outcome of the Gulf War was the rise in the military of the term "command and control warfare" (C2W). C2W was a new concept for disrupting an enemy's decision cycle. C2W consisted of five elements, called "pillars": PSYOP, electronic warfare, deception, operations security, and physical destruction, all supported by intelligence as the foundation. By the end of the 1990s, C2W had become a subset of the broader "information operations," which added computer network operations and critical information infrastructure defense to the original five pillars.

When President Clinton took office, he abolished what remained of Reagan's and Bush's strategic influence interagency mechanisms. However, most of the military gains – the PSYOP Master Plan, OP3, and the improvement in military PSYOP troop units – remained, even through the post-Gulf War drawdown.

In the late 1990s, Congress pushed for significant decreases in the foreign policy budget, including public diplomacy, under the pretext that with the winning of the Cold War, such a large public diplomacy machine was no longer needed – in reality, Congress was looking for money for domestic programs. In 1998, Congress passed the Foreign Affairs Reform and Restructuring Act. Among its many actions, the Foreign Affairs Reform Act disestablished the formerly independent USIA, and merged its functions and missions under the cognizance of the Department of State, within the new Under Secretary for Public Diplomacy & Public Affairs.[107] The same act slashed the State Department's budget, a condition that persisted for over a decade. In 2001 the share of the budget devoted to international affairs was only 1.18 percent.[108]

By the end of the 1990s, the rise of the Internet and global media capabilities led to vast amounts of information, misinformation and opinions being available to the global audience. Much of the information and opinions spread by these new communications means did not reflect well on the U.S. or support national security objectives. Yet until 1999, the Clinton Administration did not have any specific national security policy concerning public diplomacy, international information, or information operations.[109] Two key events in which information was used to devastating effect – the Balkans and the genocidal wars in Rwanda – galvanized Clinton into developing a national security policy to better fight this "new" war of ideas.[110]

On 30 April 1999, President Clinton finally established a policy on strategic influence by signing Presidential Decision Directive/NSC-68, "International Public Information". The overall objective of this presidential decision directive (PDD) was to "promote understanding and support for U.S. foreign policy initiatives around the world."[111] PDD 69 goals included developing and executing a more effective and coordinated international public information (IPI) strategy, countering the growing hostile misinformation about the United States, and more effectively promoting U.S. policy, values and interests to foreign audiences. Most importantly, the PDD sought to harmonize and synchronize at the national level the efforts of all the various players and planners in IPI – including what the PDD terms "overt international military information."[112]

PDD 68 directed three key implementation strategies to ensure that IPI was integrated into national security policy-making. First, PDD 68 established the IPI Core Group (IPICG) as the interagency working group responsible for coordinating the activities and efforts of all government agencies that planned and conducted IPI activities.[113]

The State Department chaired the IPICG, with NSC serving as deputy chair. Other permanent members included Assistant Secretary-level representatives from DoD, JCS, USAID, and the National Security Council, plus a stipulation for others as required, and the option to establish sub-groups on regional, functional and transnational issues as appropriate.[114]

Second, PDD 68 directed the development of a national IPI strategy, including IPI plans for potential major regional and transnational challenges and contingencies. Plans were to address U.S. responses, resources required, scope and duration of IPI activities, and the desired result. The PDD also directed that these IPI plans be integrated into interagency planning as mandated in PDD 56, "Managing Complex Contingency Operations."[115]

Third, PDD 68 directed the IPICG to work with U.S. Government educational institutions to develop and conduct annual education and training activities designed to foster expertise in IPI and promote better coordination.[116]

At the instigation of OSD and Joint Staff, PDD 68 also directed the detailing, on a full-time, non-reimbursable basis, of one or more military personnel to the IPICG Secretariat, in recognition of the "predominant interest of DoD."[117]

PDD 68 was initially welcomed by the parties involved in its crafting. There had been no presidential guidance on strategic influence since Reagan's NSDDs in the 1980s. And as USIA had been the primary means of "telling America's story" overseas during the Cold War, there was growing concern about the U.S. Government's ability to influence foreign audiences. PDD 68 was seen as a way to alleviate these concerns.[118]

However, PDD 68 ran into problems almost from its inception. State Department had the chair, but did not have the necessary direction and tasking authority over the other departments. Meetings turned in reporting forums rather coordinating arenas.[119] The State Under Secretary also hesitated in acting and forming the IPICG; in two years only two meetings of the formal IPICG were convened, although action officers did meet. Resourcing was another issue. PDD 68 did not specifically provide any means or resources to the IPICG or to the implementing agencies. The departments hesitated to expand upon or initiate any new information activities without the assurance of funds to do so.[121]

PDD 68 was also an unclassified document. It soon appeared in the media, and critics abounded, from journalists, to former officials, to current "unnamed" officials. Criticism ranged from those who thought it would be no more than a global spin machine, to those who thought it would filter information normally widely available to reporters, to those who thought it was meant to propagandize the American public, to those who thought the party in power would use it as a political tool.[122]

PDD 68 did have some accomplishments before its denouement. Under the IPICG, the Balkan IPI Working Group has been very effective in coordinating IPI activities in support of the continuing operations in Bosnia and Kosovo. And PDD 68 was the genesis of what is today a very close, mutually beneficial working relationship between DoD, the Broadcasting Board of Governors and the Voice of America.[123]

STRATEGIC INFLUENCE TODAY

Shortly after taking office, President George W. Bush issued National Security Policy Directive (NSPD) 1, which restructured the NSC system. NSPD 1 abolished all of Clinton's standing interagency working groups (IWG) and ad hoc groups. Instead of IWGs, Bush established policy coordination committees (PCC). NSPD 1 established a number of PCCs; more would be established in later NSPDs. NSPD 1 also recreated some of Clinton's IWGs as subcommittees under one of the new PCCs.

The IPICG was one of many former IWGs that languished for several months, awaiting a decision from the new Administration. Eventually Bush decided to grandfather PDD 68, and the IPICG became a subcommittee under the new Counter Terrorism PCC. However, the IPICG lost momentum as an interagency coordinating body during its time in limbo. While it still continued to operate, it became primarily a State Department operation.[124]

The events of 11 September 2001 changed everything, not least of which was the administration's outlook concerning strategic influence. Faced with direct evidence that many people around the world actively hated the United States, Bush began taking action to more effectively explain U.S. policy overseas.

Initially the White House and DoD turned to the Rendon Group, a private public relations firm that was already under contract to burnish the U.S. image overseas. Rendon focused on the immediate 24-hours news cycle as a means to shape opinions, rather than a long-term ideological change. Rendon helped create Coalition Information Centers (CIC) in Washington, London and Islamabad. Personnel in these offices prepared daily press releases and responses to any enemy propaganda in the news, conducted polling and held focus groups, and coordinated the appearances of U.S. officials on key Arabic television programs to occur at strategic, highly watched moments.[125] Over time, Rendon's work was supplanted by other organizations.

In October 2001, Bush swore in Charlotte Beers as the new Under Secretary of State for Public Affairs and Public Diplomacy. Beers had been a highly successful advertising executive on Madison Avenue. Secretary of State Colin Powell and President Bush hoped that Beers would be able to use her advertising skills to rejuvenate State's public affairs and public diplomacy programs to sell American policy and values overseas.[126]

Reactions to Beers' appointment and to her first year in office have been mixed. Many critics doubt that the skills which succeed in selling a brand-name product to American consumers translate well into skills needed to sell policy and win a war of ideas with foreigners. Many complain that world opinion has changed little, or even worsened in the last year. Others feel that Beers has initiated several programs that may have an impact over time.[127]

Early in August 2002, Bush announced the creation of the Office of Global Communications (OGC) to help manage and shape the U.S. image abroad.[128] Five months later Bush signed Executive Order 13283, officially establishing OGC within the White House Office. Bush assigned OGC the mission to advise the President on the most effective means "to ensure consistency in messages that will promote the interests of the United States abroad, prevent misunderstanding, build support for and among coalition partners of the United States, and inform international audiences." This advice was to be given only for overt information activities.[129]

Other OGC functions specified in the Executive Order include assessing methods and strategies used by the government; coordinating the formulation of messages among appropriate agencies; working with other departments to develop a strategy for disseminating

"truthful, accurate and effective messages" about American policies, people and culture; and coordinating the creation of temporary communication teams that would deploy to areas of high global interest and media attention. Teams could not deploy without consultation with State Department and DoD.[130]

Like the Rendon Group, OGC is focusing on the short-term goal of winning the evening news cycle rather than making any long-term effort to change attitudes and opinions. Its messages are more informative, more journalistic, than persuasive. OGC reports only to the White House; it is not within the NSC structure, although it does coordinate with the two PCCs discussed below. Despite its direct link to the White House, OGC does not have any tasking authority. The last line of the Executive Order specifically states that OGC does not have authority to issue directives to other agencies.[131]

Bush split the remaining elements of strategic influence between two PCCs, the Counter Terrorism Information Strategy (CTIS) PCC and the Strategic Communications PCC (SC). NSC chairs the CTIS PCC, which is responsible for countering terrorist hostile propaganda and contains at least one subgroup, the Counter Propaganda Working Group. Both CIA and DoD participate in the CTIS PCC. NSC and State Department act as co-chairs of the SC PCC, which is responsible for overt public affairs and public diplomacy. The SC PCC has four subcommittees: Future Directions, Afghanistan, Iraq, and the State Fusion Center. Neither CIA nor DoD attends the SC PCC. And while the NSC chair of the CTIS PCC attends SC PCC meetings, the reverse is not true.[132]

In August 2002, Congress also approved spending $225 million on cultural and information programs abroad, mostly targeting Muslim countries. Representative Henry Hyde sponsored the bill, citing a need to correct a "cacophony of hate and misinformation" about the U.S. "[133]

In March 2002, the U.S. Broadcasting Board of Governors (BBG) launched Radio Sawa, an Arabic entertainment and news station that can be heard throughout the Middle East. Within just a few months, ratings increased by 33%. The BBG is now planning a television counterpart.[134]

In 2001, OSD established the Office of Strategic Influence (OSI), in an attempt to fill the gaps between Bush's PCCs and the OGC. Officials within DoD were also concerned about the void left from the nonfunctional IPICG. Bush's organizations took a long time to become fully established and begin working. DoD also felt that the three organizations were too narrowly focused on explaining U.S. policy to broad, global audiences. None appeared to be focused on

specific target audiences, with a specific strategy and objectives in mind, or on the government actions needed to affect long-term U.S. goals.[135]

OSI was headed by Major General Worden, U.S. Air Force. OSI was nominally under the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD SOLIC), who had policy oversight of psychological operations, but it reported directly to the Under Secretary of Defense for Policy. DoD did not envision that OSI would be solely a DoD organization. OSI sought input and representatives from other departments from the beginning. DoD hoped that OSI would be a catalyst for action, and once it started developing and implementing influence campaigns, State would take a bigger role, and eventually OSI would become an interagency body.[136]

MG Worden had a vision, plans and objectives for what he believed OSI should accomplish in support of national objectives – something that was lacking in the other players in strategic influence at the time. One of the first things OSI looked at was how to affect change in the madrassas, the Muslim schools, where the current curriculum and textbooks are virulently anti-American.[137]

In a classic example of the internecine battles that have always plagued strategic influence, OSI was sabotaged internally within DoD and abolished by Secretary of Defense Donald Rumsfeld less than five months after its establishment. Someone in DoD leaked information to the press that OSI intended to plant false messages and misinformation in overseas media, news that would then be reported in the U.S. as factual. This type of action was not in OSI's charter, and the charge was never substantiated. Nonetheless, Rumsfeld felt that the damage caused by the media controversy and exposure were too great to overcome, and he closed the office.

All that remains in OSD for strategic influence is a small Office of Information Activities (OIA) buried within ASD SOLIC. OIA has retained responsibility for policy oversight of military psychological operations activities. It also provides the OSD representative to the CTIS PCC. OIA hopes to implement a few of the actions recommended by OSI, but with few resources, few personnel, and little authority, its effectiveness is doubtful. Additionally, OIA is maintaining a low profile, due to fears that whoever sabotaged OSI will also sabotage OIA.[138]

JCS currently has a PSYOP division, generally six personnel headed by an Army O-6, within the J-39, Deputy Director for Information Operations (DDIO), a directorate that has existed only since 1997. Other divisions within DDIO have responsibility for other elements of information operations. The DDIO himself is a brigadier general; the first three have been Air Force generals. This gives functional responsibility for a majority of strategic influence to a

general or flag officer, something that had been missing for decades. The PSYOP Division has a multitude of responsibilities: coordinating PSYOP policy within JCS; developing and staffing JCS positions on DoD and national policy regarding PSYOP; promulgating joint PSYOP doctrine; representing JCS in the interagency; preparing and staffing deployment orders for PSYOP units; shepherding approval of PSYOP plans and orders within JCS and the Services; providing national-level PSYOP guidance to the combatant commanders; staffing PSYOP product approval within JCS and with OSD, when approval has not been delegated to the regional combatant commanders; and providing the U.S. representative to the North Atlantic Treaty Organization (NATO) PSYOP Working Group.[139]

When the War on Terrorism started in the Fall of 2001, JCS established the Information Operations Task Force (IOTF), at the direction of the Chairman of the Joint Chiefs of Staff (CJCS), General Myers. Originally, the CJCS intended the IOTF to be an interagency group that would direct information and influence operations and act as the single point of contact for the U.S. Government; its original title was "Information Operations Resource Center (IORC)." But no other agencies or departments would participate in the IORC. No other agency wanted to put their people under a DoD brigadier general.[140]

When the IORC didn't become an interagency group, JCS established the IOTF. It was given space, but few other resources. DDIO stripped almost two-thirds of its own people, including all of the PSYOP Division, away from their normal duties to fill the IOTF.[141]

The IOTF was largely ineffective and was disbanded in July 2002. It initially developed a system of public affairs, PSYOP and information operations "alerts" to provide guidance and information to DoD senior officials and the regional combatant commands. No one ever used the public affairs or PSYOP alerts. The information operations alerts became just "FYI" notes for the DoD leadership, rather than action documents. The alert system had been designed to address both foreign and domestic audiences; however, the focus quickly changed to domestic audiences to gain public support for the War on Terrorism. One positive outcome of this ill-conceived idea was that PSYOP Division personnel were returned to their normal duties, due to concerns over violation of the Smith-Mundt Act.[142]

The IOTF did create an excellent, scientific database to measure and track "Measures of Effectiveness" (MOE) for information operations. Effective MOE tracking is a shortcoming in PSYOP and information operations. However, many DoD officials questioned the resources and effort put into the MOE database when there was not an effective information operations program to track. As one official put it, "we had the Cadillac of MOE databases with the Yugo of information operations campaigns."[143]

Within the Armed Forces, there is still only one active duty organization, the 4th Psychological Operations Group (4th POG). It is a de facto national asset. This one unit provides support to all levels of DoD, from brigade to unified command, to both conventional forces and special operations, and to the other Services. 4th POG also frequently provides analytical support and PSYOP products directly to national level agencies and organizations. Within the 4th POG is the Strategic Studies Detachment – a group of high-quality civilian intelligence analysts and area experts who provide detailed PSYOP studies and assessments in support of unified commands and national-level agencies.

In early 2002, Rumsfeld published his Defense Planning Guidance (DPG). The DPG directed OSD, JCS and the Services to develop an "Information Operations Roadmap" to improve DoD capabilities. The DPG included fourteen separate sub-studies that were to be addressed in the Roadmap. These included recommendations for the establishment of a strategic PSYOP detachment, for improved education on information operations, and for improvements in the information operations career field, including the creation of flag officer positions.[144]

The DPG itself and the Information Operations Roadmap developed within DOD remain classified. The Roadmap does recommend a significant budget increase for military PSYOP. It also recommends the establishment of a strategic PSYOP unit. Officials in DoD are not commenting on what the unit will look like, where it will be located or to whom it will report. Experts in the field believe that it should be located in the Washington, D.C. area, to properly integrate into the interagency strategic influence effort, including providing support to other agencies. However, many are afraid that the controversy over OSI would extend to the new unit and limit its ability if it were located in the area; alternative sites and command structures are being explored.

THE WAY AHEAD

> "Why is the PSYOP contest so asymmetrical? One might assume that a "battle of ideas" should be won by a superpower that has more communications consultants, advertising executives, information and media specialists, political advisers, public relations professionals, and psychologists than the total number of [operatives in Al Qaeda]."[145]

Originally written about the failure of U.S. "hearts and minds" campaigns during the Vietnam War, the quote above is equally valid today. Is the Bush Administration organized

effectively to counter the growing anti-American sentiment around the world? What can the Bush Administration learn from the past?

The strongest periods of U.S. strategic influence had several common features: permanent, rather than ad hoc organizations; specific charters outlining roles and responsibilities for all agencies; top-level interest, guidance and cover; and full-time staffs. Further, the various departments had dedicated full-time people who had direct access to key policy decision makers.

It's ironic that back in Truman's and Eisenhower's Administrations, when the news media was extremely slow compared to today, there was better recognition than exists today that timeliness of decisions and activities is critical to strategic influence. This is particularly true in DoD, where the trained, experienced action officers are buried under layers of staffs levels, often headed by people who have little understanding or appreciation of the psychological impacts of policy. The 21st century information cycle will not wait while an action officer staffs policy decisions through several levels.

The Bush Administration should re-evaluate how it has organized to conduct strategic influence. The current structure is trifurcated, with responsibilities split between three different organizations (OGC, CTIS PCC, SC PCC). Additionally, due to their narrow focus and lack of participation by all departments involved in strategic influence, gaps exist. Areas available for influence are not being exploited.

One person should be in charge of strategic influence for the President - one person, who is a member of NSC, not one of the departments, agencies, PCCs, or OGC; one who can direct, coordinate and provide guidance to all. In today's Information Age, the President needs a Special Assistant to the President for Information Activities – a National Information Adviser (NIA). The NIA should be provided a full-time staff, with experts from all the agencies, as Eisenhower did with his second POCC, established in January 1954.

Both Eisenhower's POCC and Reagan's SPG, established under NSPD 77, provide models to build on. The role of the NIA would not be much different from the POCC Chair, the OCB Executive Secretary, or the SPG Chair, the National Security Adviser. The key difference is that national psychological strategy was just one of their myriad duties. Appointing an NIA, with a dedicated staff, whose sole responsibility would be strategic influence, would greatly improve coordination of strategic influence activities and the quality of advice provided to the President. The authority invested in the position would also improve implementation of activities. Both the PSB and IPICG failed because they lacked sufficient authority to direct the coordination and implementation of policy decisions, and because they could not rise above

interagency rivalry. Further, having an NIA should improve timeliness of interagency action. It has taken Bush's SC PCC nearly two years to develop a vision and charter.

Additionally, the Bush Administration needs to articulate a national psychological strategy, a strategy that is as broad and encompassing as the containment strategy of the Cold War. The nuclear threat, combined with other weapons of mass destructions (WMD), is as imminent today as ever. And the threat of another attack like 11 September is even greater. But now many of the potential perpetrators are non-state actors. Just as in the Cold War, the U.S. must use all elements of national power to deter the use of WMD. Strategic influence, as defined in the beginning of this paper, will be key to success. Persuasive information alone will not be sufficient; messages must be backed up by action or they will be ineffectual. Reagan's NSPD 130 provides a starting model, although it needs to be updated. As one writer put it, "NSDD 130 should be dusted off and made required reading throughout the executive and legislative branches. This landmark document established international information as a major instrument of national security policy, and the responsibility of no single agency of the government."[146]

Gordon Gray's priorities upon becoming director of the PSB also provide a good example of how to begin addressing a national psychological strategy. The national psychological strategy should clearly define national interests and objectives. Goals not clearly defined are rarely achieved. Goals specifically defined will guide effective action by the departments; generalized statements will lead to continued inaction and interagency rivalry, and, ultimately, an ineffective strategic influence program. Objectives should include not just adversarial or hostile audiences, but also allies and neutral audiences. The weakening of U.S. alliance structures has been a key strategic objective of U.S. opponents in recent years.[147]

A national psychological strategy should concentrate equally on long-term attitude and behavior changes as on explaining U.S. policy to foreign audiences. The feelings that begat the acts of 11 September did not occur overnight. Those attitudes had been building for years, and they will not change overnight. A national psychological strategy should also incorporate U.S. Government actions that help foster positive changes in the social and political conditions that continue to create animosity towards the U.S. This may include re-examining U.S. policies versus U.S. national interests – is it more in the national interest to continue policies which are engendering such hostile attitudes, or would it be more in the U.S. national interest to modify that policy to mitigate the negative response?

The PSB's first report on its assessment of the U.S psychological efforts noted that, "the contract between the messages of freedom and democracy that were often broadcast and the

Page 3244 of 3957

actions of the U.S. was often stark. The implication was that the current method of policy formulation could be more effective if the message and the actions were more closely coordinated."[148] One of the NIA's responsibilities would be to ensure that psychological impact of policies when communicated to foreign audiences is considered before the adoption of the policy.

Secretary Rumsfeld needs to reorganize DoD as well. First, DoD needs someone with the appropriate position and authority to oversee the policy and to coordinate DoD strategic influence activities among DoD public affairs, military PSYOP, and other military information activities. Just as the President needs an NIA, so too does Secretary Rumsfeld need an adviser who is dedicated to strategic influence. History provides an example – the Deputy for Psychological Policy under Truman. Today, however, a "Deputy for Information Policy" would best be placed directly under the Under Secretary of Defense for Policy (USDP),[149] so that the position would be above that of the several Assistant Secretaries of Defense who are players in strategic influence. OIA should then be moved under the new Deputy for Information Policy.

DoD also needs to formally establish a DoD Committee on strategic influence, as has been done several times in the past. The officers and officials within JCS and OSD do a good job of communicating and coordinating among themselves. However, formalization lends legitimacy and gets attention. Flag officers and senior officials do not perceive ad hoc groups and meetings as being important compared to committee meetings which the Secretary of Defense or the USDP has declared will occur.

One area that the Administration should address immediately is the distrust and antipathy of the military by other departments involved in strategic influence. PSB was based on the false premise that you could separate psychological strategy from national strategy. Equally fallacious in today's world of instant, worldwide communications is the notion that you can separate military psychological activities from public affairs and public diplomacy. There is a prevailing misconception in the State Department and public affairs field that military psychological operations are not truthful, and that contact with PSYOP will somehow taint public affairs and public diplomacy. While there are valid reasons for keeping the messages and activities separated in the eyes of foreign audiences, those reasons do not apply to coordination at the U.S. national level.

The initial strategic influence efforts of the Bush Administration have revealed a typically American myopic viewpoint: Americans assume that other people think as they do and want the same things that American do – that other people want to be like Americans. For instance, one of the first information products developed by Beers was a series of videos showing Muslim life

and activities in the U.S. This exemplifies the naiveté that simply showing America to foreign Muslims would convince them that they would want to emulate America and shouldn't disagree with U.S. policies. It also demonstrated little understanding of how the target audience would view the film - Muslims in this country live in luxury compared to most of the Muslims overseas that the videos targeted. The target audiences could not identify with the film, there was no emotional connection.

The Administration's efforts also appear to be hampered by "political correctness," something that has been a bane for military PSYOP for years. In an effort not to offend anybody, products are bland, without emotional impact. On other hand, terrorist propaganda does not simply reach for hearts and minds; it activates envy, fear and anger by stirring primal emotions.[150] Television provides numerous examples of angry, intense, committed anti-American protestors. Seldom do you see equally emotionally committed people protesting *for* the United States. At some point, strategic influence must go beyond simply informing and educating and must involve the emotions of the target audiences.

> "Painful as it may be to face squarely the question of American cultural inhibitions in the area of psychological-political conflict, the effort is necessary – in order not only to develop intelligent approaches to dealing with them but also to achieve the cultural self-consciousness essential for effective participation in this kind of conflict. It is essential because Americans tend to assume that people everywhere are much like themselves, with similar fundamental motivations and views of the world. But blindness to differences in national characteristics is apt to be a fatal handicap for anyone attempting to affect the psychological orientation and political behavior of foreign audiences."[151]

The answer to the question, "Why do they hate us?," is not just that they don't understand us. Simply explaining U.S. policy, U.S motives, and the U.S. way of life will not change hostile audiences if they perceive our policies as inimical to their way of life. A world-class strategic influence campaign will not be the panacea for overcoming the current difficulties in world opinion. No wizardry in communications can make bad policy decisions or actions palatable. However, having a competent strategic influence campaign is essential to U.S. victory in the War on Terrorism. Without one, anti-American sentiment will continue to grow, and the U.S will be increasingly vulnerable to more attacks like 11 September 2001.

WORD COUNT = 15,387

Page 3246 of 3957

Page 3247 of 3957

ENDNOTES

[1] Alfred H. Paddock, Jr., “Military Psychological Operations,” in *Political Warfare and Psychological Operations: Rethinking the US Approach*, ed. Frank B. Barnett and Carnes Lord (Washington, D.C.: National Defense University Press, 1989), 46.

[2] Alfred H. Paddock, Jr., *U.S. Army Special Warfare: Its Origins* (Lawrence, KS: University Press of Kansas, 2002), 3-4.

[3] Ibid., 4-6.

[4] Ibid., 6-7.

[5] Ibid., 8.

[6] Ibid., 8-9.

[7] Ibid., 9.

[8] Paddock, *Political Warfare and Psychological Operations*, 46.

[9] Paddock, *U.S. Army Special Warfare*, 12.

[10] Ibid., 15-17.

[11] Paddock, *Political Warfare and Psychological Operations*, 47.

[12] Paddock, *U.S. Army Special Warfare*, 41.

[13] Ibid., 43-45.

[14] Ibid., 20.

[15] Ferdinand Eberstadt, “Postwar Organization for National Security,” in *Decisions of the Highest Order: Perspectives on the National Security Council*, ed. Karl F. Inderfurth and Loch K. Johnson (Pacific Grove, CA: Brooks/Cole Publishing Company, 1988), 29-30.

[16] Ibid., 31.

[17] Ibid., 33.

[18] U.S. Congress, “The National Security Act of 1947,” in *Decisions of the Highest Order: Perspectives on the National Security Council*, ed. Karl F. Inderfurth and Loch K. Johnson (Pacific Grove, CA: Brooks/Cole Publishing Company, 1988), 37.

[19] Ibid., 38-39; Eberstadt, “Post War Organization”, 33.

Page 3248 of 3957

[20] Benjamin R. Rose, *Presidentially Mandated Strategic Psychological Warfare Policy Coordination Under Truman and Eisenhower: The Psychological Strategy Board and the Operations Coordinating Board* (Harrisonburg, VA: James Madison University, 1999), 10-11.

[21] The National Security Resources Board (NSRB) was created by the National Security Act of 1947, and disestablished in 1953, primarily because many of its functions were transferred to other agencies. The NSRB monitored, planned and coordinated the use of national assets in the event of an atomic attack on the U.S.

[22] Rose, 15-16.

[23] Ibid., 11-12.

[24] *Smith-Mundt Act*, *U.S. Code*, Title 22, Chapter 18, Sec. 1461 (1948); excerpt available from <http:www4.law.cornell.edu.uscode/22/1461.html>; Internet; accessed 27 February 2003.

[25] Rose, 13-15.

[26] Carnes Lord, "The Psychological Dimension in National Security," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, ed. Frank B. Barnett and Carnes Lord (Washington, D.C.: National Defense University Press, 1989), 14; Rose, 40.

[27] Rose, 18; Paddock, *U.S. Army Special Warfare*, 40.

[28] Paddock, *U.S. Army Special Warfare*, 94-95.

[29] Paddock, *Political Warfare and Psychological Operations*, 47.

[30] Rose, 20.

[31] U.S. Department of Defense, *Organization, Office of Psychological Policy*, Department of Defense Directive C-5132.1 (Washington, D.C.: U.S. Department of Defense, 21 April 1952), 1.

[32] Rose, 21.

[33] Stanley L. Falk, "The NSC Under Truman and Eisenhower," in *Decisions of the Highest Order: Perspectives on the National Security Council*, ed. Karl F. Inderfurth and Loch K. Johnson (Pacific Grove, CA: Brooks/Cole Publishing Company, 1988), 71; Thomas J. Saxon, Jr., *The Evolution of the National Security Council System Under President Nixon* (Ann Arbor, MI: University Microfilms, 1971), 94.

[34] Department of Defense Directive C-5132.1, 1.

[35] Rose, 21.

[36] Rose, 24.

[37] Rose, 22-23.

Page 3249 of 3957

[38] Department of Defense Directive C-5132.1, 1; Paddock, *U.S. Army Special Warfare*, 40.

[39] Lord, *Political Warfare and Psychological Operations*, 14.

[40] Department of Defense Directive C-5132.1, 2.

[41] Ibid., 3.

[42] Paddock, *U.S. Army Special Warfare*, 2.

[43] Rose, 29.

[44] Paddock, *U.S. Army Special Warfare*, 139.

[45] U.S. Department of Defense, *Internal Organization of the Department of Defense for Psychological Operations*, Department of Defense Directive S-3140.1 (Washington, D.C.: U.S. Department of Defense, 10 January 1953), 1.

[46] Ibid., 3.

[47] Ibid., 4.

[48] Saxon, 108; Rose, 35.

[49] National Security Council, *Responsibilities and Principles Governing the Conduct of the Foreign Information Program and Psychological Warfare*, National Security Council Memorandum (Washington, D.C.: National Security Council, 25 January 1954), 2.

[50] Saxon, 110, 117; Rose, 38, 42.

[51] Saxon, 117; Robert Cutler, "The Development of the National Security Council," in *Decisions of the Highest Order: Perspectives on the National Security Council*, ed. Karl F. Inderfurth and Loch K. Johnson (Pacific Grove, CA: Brooks/Cole Publishing Company, 1988), 59; Rose, 46-47.

[52] Saxon, 113.

[53] Saxon, 117; Falk, 73.

[54] Saxon, 117-119.

[55] National Security Council Memorandum, *Responsibilities and Principles Governing the Conduct of the Foreign Information Program and Psychological Warfare*, 2.

[56] Lord, *Political Warfare and Psychological Operations,* 19.

[57] Cutler, 61; Lord, 14.

Page 3250 of 3957

[58] National Security Council Memorandum, *Responsibilities and Principles Governing the Conduct of the Foreign Information Program and Psychological Warfare*, 3.

[59] National Security Council Memorandum, *Responsibilities and Principles Governing the Conduct of the Foreign Information Program and Psychological Warfare*, 4.

[60] Saxon, 120.

[61] Saxon, 142.

[62] National Security Council, *Wartime Organization for Overseas Psychological Operations,* National Security Council Memorandum 5812/1 (Washington, D.C.: National Security Council, 4 June 1958).

[63] Frank R. Barnett, "Afterword – Twelve Steps to Improving American PSYOP," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, ed. Frank B. Barnett and Carnes Lord (Washington, D.C.: National Defense University Press, 1989), 212.

[64] U.S Department of the Army, *The Art and Science of Psychological Operations: Case Studies of Military Application, Volume One,* Department of the Army Pamphlet 525-7-1 (Washington, D.C.: U.S. Department of the Army, April 1976), 110.

[65] Saxon, 149; Henry M. Jackson, "Organizing for National Security," in *Decisions of the Highest Order: Perspectives on the National Security Council*, ed. Karl F. Inderfurth and Loch K. Johnson (Pacific Grove, CA: Brooks/Cole Publishing Company, 1988), 85.

[66] Jackson, 86-87.

[67] Saxon, 158.

[68] McGeorge Bundy, "Questions Arising from CIA Support of Certain Activities," *National Security Action Memorandum Number 3* (Washington, D.C.: The White House, 15 April 1961).

[69] McGeorge Bundy, "An Effective Countertheme to 'Peaceful Coexistence'," *National Security Action Memorandum Number 61* (Washington, D.C.: The White House, 14 July 1961).

[70] McGeorge Bundy, "Policy Guidance and Preemption of U.S. Government-Controlled Broadcasting," *National Security Action Memorandum Number 63* (Washington, D.C.: The White House, 24 July 1961).

[71] John F. Kennedy, "Establishment of the Special Group (Counter-Insurgency)," *National Security Action Memorandum Number 124* (Washington, D.C.: The White House, 18 January 1962).

[72] Barnett, *Political Warfare and Psychological Operations,* 212.

[73] U.S. Joint Chiefs of Staff, *National Coordination of Psychological Operations,* Joint Chiefs of Staff Study (Washington, D.C.: The Joint Staff, n.d.), II-3 – II-4.

[74] Paddock, *Political Warfare and Psychological Operations*, 48.

Page 3251 of 3957

[75] Saxon, 238.

[76] Lyndon B. Johnson, “Informational and Psychological Warfare Programs in South Vietnam,” *National Security Action Memorandum Number 325* (Washington, D.C.: The White House, 12 March 1965); Lyndon B. Johnson, “Intensified and Expanded PSYOPS Activities in Vietnam,” *National Security Action Memorandum Number 330* (Washington, D.C.: The White House, 9 April 1965).

[77] Alfred H. Paddock, Jr, <paddockal@earthlink.net>, “Assistance,” electronic mail message to author, 12 February 2003.

[78] Saxon, 255.

[79] “Presidential Directives and Executive Orders,” Available from <http://www.fas.org/irp/offdocs/direct.htm>; Internet; accessed 28 January 2003.

[80] Barnett, *Political Warfare and Psychological Operations,* 212.

[81] Paddock, “Assistance.”

[82] Lord, *Political Warfare and Psychological Operations,* 15.

[83] James E. Carter, “The National Security Council System,” *Presidential Directive/NSC-2* (Washington, D.C.: The White House, 20 January 1977).

[84] Alfred H. Paddock, Jr., “U.S. Military Psychological Operations: Past, Present, and Future,“ in *Psychological Operations and Political Warfare in Long-Term Strategic Planning,* ed. Janos Radvanyi (New York: Praeger’s, 1990), 23.

[85] Ronald W. Reagan, “United States International Broadcasting,” *National Security Decision Directive Number 45* (Washington, D.C.: The White House, 15 July 1982), 1.

[86] Ibid., 1-2.

[87] Ibid., 3.

[88] Ronald W. Reagan, “Management of Public Diplomacy Relative to National Security,” *National Security Decision Directive Number 77* (Washington, D.C.: The White House, 14 January 1983), 1.

[89] Ibid., 3.

[90] Ibid., 2.

[91] Ibid., 2-3.

[92] Ronald W. Reagan, “US International Information Policy,” *National Security Decision Directive Number 130* (Washington, D.C.: The White House, 6 March 1984), 1.

[93] Ibid., 1-4.

Page 3252 of 3957

[94] Ibid., 3-4.

[95] Paddock, *Psychological Operations and Political Warfare*, 23.

[96] Ibid., 24.

[97] Ibid., 29.

[98] Ibid., 30.

[99] Jack Summe, COL (USA), Chief, Information Strategy Division, Joint Staff J-39, interview by author, 3 February 2003, The Pentagon, Arlington, VA.

[100] Lord, *Political Warfare and Psychological Operations,* 21.

[101] Dave Lowe, *Idea to Reality: A Brief History of the National Endowment for Democracy*; available from <http://www.ned.org/about/nedhistory.html>; Internet; accessed 1 February 2003.

[102] Ibid.

[103] Robert W. Trost III, COL (USA, Ret), Chief, Information Strategy Division, Joint Staff J-39, June 1997 – July 2000, interviews by author, October 2002 and February 2003, Fairfax, VA.

[104] George Bush, "Review of U.S. Government International Broadcasting Activities," *National Security Review 24* (Washington, D.C.: The White House, 28 March 1990).

[105] George Bush, "United States Government International Broadcasting," *National Security Directive 51* (Washington, D.C.: The White House, 17 October 1990).

[106] Ibid.; "About the Broadcasting Board of Governors;" available from <http:www.bbg.gov/bbg_aboutus.htm>; Internet; accessed 5 March 2003.

[107] William J. Clinton, "International Public Information," *Presidential Decision Directive/NSC-68* (Washington, D.C.: The White House, 30 April 1999); Joshua Muravchik, "Hearts, Minds, and the War Against Terror," *Commentator* (May 2002): 25-30; database on-line; available from ProQuest; accessed 1 October 2002.

[108] Richard G. Lugar, "Beating Terror," *Washington Post* (27 January 2003); available from <http://www.us.arm.mil/portal/jhtml/earlyBird/Jan2003/e20030127149168.html>; Internet; accessed 27 January 2003.

[109] Trost.

[110] Clinton, 2; Neil Munro, "Infowar: AK-47s, Lies and Videotape," *Association for Computing Machinery* (July 1999): 19-22; database on-line; available from ProQuest; accessed 22 October 2002.

[111] Clinton, 1.

Page 3253 of 3957

[112] Ibid., 2; "Overt international military information" is just one of several euphemisms used by other agencies to refer to military psychological operations.

[113] Ibid., 3.

[114] Ibid.

[115] Ibid.

[116] Ibid., 4.

[117] Ibid., 4; Trost.

[118] Clinton, 1; Muravchik.

[119] Trost.

[120] Trost.

[121] Jack Summe <jack.summe@js.pentagon.mil>, "PDD 68 & the IPI Core Group," electronic mail message to author, 22 October 2002.

[122] "The U.S. Tries Spinning the Globe," *Columbia Journalism Review* (Nov/Dec 1999): 11; database on-line; available from ProQuest; accessed 1 October 2002; "U.S. Creates New Agency; Unit to Coordinate Flow of Information Overseas," *The Washington Post* (13 August 1999): A23; database on-line; available from ProQuest; accessed 1 October 2002; Ben Barber, "Information-Control Plan Aimed at U.S., Insider Says," *The Washington Times* (29 July 1999): A1; database on-line; available from NewsLibrary; accessed 16 October 2002; Joel Bleifuss, "Ready, Aim, Inform," *In These Times* (March 2000); database on-line; available from Guerrilla News Network <http://www.guerillanews.com/counter_intel/propaganda_inc/ready_aim_inform.html>; internet; accessed 21 October 2002.

[123] Summe, "PDD 68 & the IPI Core Group."

[124] Summe, interview.

[125] Franklin Foer, "Flacks Americana: John Rendon's Shallow P.R. War on Terrorism," *The New Republic* (20 May 2002); internet; available at <http://www.tnr.com/docprint.mhtml?i=20020520&s=foer05202002>; accessed 6 Mar 2003.

[126] John Barry, Richard Wolffe, and Christopher Dickey, "The Real War will be for Muslim Hearts and Minds; Selling the United States," *Newsweek* (30 December 2002); database on-line; available from ProQuest; accessed 27 February 2002; Arundhati Parmar, "Full-Court Press," *Marketing News* (9 December 2002); database on-line; available from ProQuest; accessed 27 February 2003.

Page 3254 of 3957

[127] Ira Teinowitz, “Beers Draws Mixed Review After One Year,” *Advertising Age* (23 September 2002); database on-line; available from ProQuest; accessed 27 February 2003; Parmar.

[128] Ellen Hale, “Global Warmth for U.S. After 9/1 Turns to Frost; Military Plans Repulse Even European Allies,” *USA Today Online* (14 August 2002); database on-line; available from ProQuest; accessed 10 February 2003; Michael Holtzman, “Privatize Public Diplomacy,” *New York Times* (8 August 2002): 25; database on-line; available from ProQuest; accessed 1 October 2002.

[129] George W. Bush, “Establishing the Office of Global Communications,” *Executive Order 13283 (21 January 2003)*; available from <http:www.fas.org/irp/offdocs/eo/eo-13283.htm>; accessed 25 February 2003.

[130] Ibid.

[131] Ibid.

[132] Summe, interview; Trost; Thomas Timmes, Policy Assistant, Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, interview by author, 3 February 2003, The Pentagon, Arlington, VA.

[133] Hale.

[134] John Harwood, “Public Diplomacy Problems Predate Bush Administration,” *Wall Street Journal* (5 March 2003); database on-line; available from ProQuest; accessed 6 March 2003; Parmar.

[135] Timmes; Michael Furlong, Policy Assistant, Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, interview by author, 3 February 2003, The Pentagon, Arlington, VA; Daniel Devlin, Policy Assistant, Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, interview by author, 3 February 2003, The Pentagon, Arlington, VA.

[136] Timmes; Furlong; Devlin.

[137] Timmes; Furlong; Devlin.

[138] Timmes; Furlong; Devlin.

[139] Trost; Summe, interview.

[140] Summe, interview.

[141] Ibid.

[142] Ibid.

[143] Ibid.; Timmes.

[144] Summe, interview.

[145] Barnett, *Political Warfare and Psychological Operations,* 213. The original quote read, "…soldiers in Hanoi's army."

[146] Richard G. Stilwell, "Comment – The Psychological Dimension in National Security," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, ed. Frank B. Barnett and Carnes Lord (Washington, D.C.: National Defense University Press, 1989), 42.

[147] Lord, *Political Warfare and Psychological Operations*,17.

[148] Rose, 28.

[149] The formal title would then become, "Deputy Under Secretary of Defense for Information Policy."

[150] Barnett, *Political Warfare and Psychological Operations,* 217.

[151] Lord, *Political Warfare and Psychological Operations*, 21 –22.

Page 3256 of 3957

Page 3257 of 3957

BIBLIOGRAPHY

"About the Broadcasting Board of Governors." Available from <http://www.bbg.gov/bbg_aboutus.htm>. Internet. Accessed 5 March 2003.

"Banging the Drum for the U.S." CBS News 30 July 2002. Journal on-line. Available from <http://www.cbsnews.com/stories/2002/07/30/politics/main516881.shtml>. Internet. Accessed 23 October 2002.

Barber, Ben. "Information-Control Plan Aimed at U.S., Insider Says." *The Washington Times* (29 July 1999): A1. Database on-line. Available from NewsLibrary. Accessed 16 October 2002.

Barnett, Frank R. and Lord, Carnes, eds. *Political Warfare and Psychological Operations: Rethinking the US Approach*. Washington, D.C.: National Defense University Press, 1989.

Barnett, Frank R., Shultz, Richard H. and Tovar, B. Hugh, eds. *Special Operations in US Strategy*. Washington, D.C.: National Defense University Press, 1984.

Barry, John, Wolffe, Richard and Dickey, Christopher. "The Real War will be for Muslim Hearts and Minds; Selling the United State." *Newsweek* (30 December 2002). Database on-line. Available from ProQuest. Accessed 27 February 2002.

Bleifuss, Joel. "Ready, Aim, Inform." *In These Times* (March 2000). Database on-line. Available from Guerrilla News Network <http://www.guerillanews.com/counter_intel/propaganda_inc/ready_aim_inform.html>. Internet. Accessed 21 October 2002.

Bundy, McGeorge. "An Effective Countertheme to 'Peaceful Coexistence'." *National Security Action Memorandum Number 61*. Washington, D.C.: The White House, 14 July 1961.

Bundy, McGeorge. "Policy Guidance and Preemption of U.S. Government-Controlled Broadcasting." *National Security Action Memorandum Number 63*. Washington, D.C.: The White House, 24 July 1961.

Bundy, McGeorge. "Questions Arising from CIA Support of Certain Activities." *National Security Action Memorandum Number 3*. Washington, D.C.: The White House, 15 April 1961.

Bush, George. "Review of U.S. Government International Broadcasting Activities." *National Security Review 24*. Washington, D.C.: The White House, 28 March 1990.

Bush, George. "United States Government International Broadcasting." *National Security Directive 51*. Washington, D.C.: The White House, 17 October 1990.

Bush, George W. "Establishing the Office of Global Communications." *Executive Order 13283 (21 January 2003)*. Available from <http:www.fas.org/irp/offdocs/eo/eo-13283.htm>. Accessed 25 February 2003.

Page 3258 of 3957

Campen, Alan D. “Information Operations Seeks Blend of Missives and Missiles”. *Signal Magazine* (June 2002). Available from <http://www.us.net/signal/Archive/June02/campen-june.html>. Accessed 26 October 2002.

Carter, James E. “The National Security Council System.” *Presidential Directive/NSC-2*. Washington, D.C.: The White House, 20 January 1977.

Castro, Max. “Propaganda Office Won’t Win Over the World”. *Miami Herald* (13 August 2002). Available from <http://www.commondreams.org/views02/0813-06.htm>. Accessed 22 October 2002.

Clinton, William J. “International Public Information.” *Presidential Decision Directive/NSC-68.* Washington, D.C.: The White House, 30 April 1999.

Cutler, Robert, “The Development of the National Security Council,” in *Decisions of the Highest Order: Perspectives on the National Security Council,* ed. Karl F. Inderfurth and Loch K. Johnson, 55-65. Pacific Grove, CA: Brooks/Cole Publishing Company, 1988.

Daugherty William E. and Janowitz, Morris. *A Psychological Warfare Casebook*. Baltimore, MD: John Hopkins Press, 1958.

Devlin, Daniel, Policy Assistant, Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict. Interview by author, 3 February 2003, The Pentagon, Arlington, VA.

Eberstadt, Ferdinand, “Postwar Organization for National Security,” in *Decisions of the Highest Order: Perspectives on the National Security Council,* ed. Karl F. Inderfurth and Loch K. Johnson, 29-33. Pacific Grove, CA: Brooks/Cole Publishing Company, 1988.

Falk, Stanley L., “The NSC Under Truman and Eisenhower,” in *Decisions of the Highest Order: Perspectives on the National Security Council,* ed. Karl F. Inderfurth and Loch K. Johnson, 65-77. Pacific Grove, CA: Brooks/Cole Publishing Company, 1988.

Furlong, Michael, Policy Assistant, Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict. Interview by author, 3 February 2003, The Pentagon, Arlington, VA.

Garfield, Andrew, Director, International Centre for Strategic Analyses, King’s College, London. “The Offence of Strategic Influence: Making the Case for Perception Management Operations.” Presented to the United Kingdom Information Operations 2002 Conference, 25 September 2002. Forwarded to author via electronic mail.

Hoffman, David. “Beyond Public Diplomacy.” *Foreign Affairs* (Mar/Apr 2002): 83-95. Database on-line. Available from ProQuest. Accessed 1 October 2002.

Hale, Ellen. “Global Warmth for U.S. After 9/1 Turns to Frost; Military Plans Repulse Even European Allies.” *USA Today Online* (14 August 2002). Database on-line. Available from ProQuest. Accessed 10 February 2003.

Harwood, John. “Public Diplomacy Problems Predate Bush Administration.” *Wall Street Journal* (5 March 2003). Database on-line. Available from ProQuest. Accessed 6 March 2003.

Holtzman, Michael. "Privatize Public Diplomacy." *New York Times* (8 August 2002): 25. Database on-line. Available from ProQuest. Accessed 1 October 2002.

Hughes, John. "Why America's Story Needs to be Sent Overseas." *Christian Science Monitor* (3 April 2002): 9. Database on-line. Available from ProQuest. Accessed 10 October 2002.

Inderfurth, Karl F. and Loch K. Johnson, eds. *Decisions of the Highest Order: Perspectives on the National Security Council*. Pacific Grove, CA: Brooks/Cole Publishing Company, 1988.

"International Public Information (IPI), Presidential Decision Directive PDD 68, 30 April 1999." Available from <http://www.fas.org/irp/offdocs/pdd/pdd-68.htm>. Internet. Accessed 9 October 2002.

Jackson, Henry M. *The National Security Council: Jackson Subcommittee Papers on Policy-Making at the Presidential Level*. New York: Praeger, 1965.

Jackson, Henry M., "Organizing for National Security," in *Decisions of the Highest Order: Perspectives on the National Security Council,* ed. Karl F. Inderfurth and Loch K. Johnson, 82-87. Pacific Grove, CA: Brooks/Cole Publishing Company, 1988.

Johnson, Lyndon B. "Informational and Psychological Warfare Programs in South Vietnam." *National Security Action Memorandum Number 325*. Washington, D.C.: The White House, 12 March 1965.

Johnson, Lyndon B. "Intensified and Expanded PSYOPS Activities in Vietnam." *National Security Action Memorandum Number 330*. Washington, D.C.: The White House, 9 April 1965.

Jones, Jeffrey, COL (USA, Ret), Director, Counter Terrorism Information Strategy, National Security Council. Telephone interview by author, 14 February 2003, Fairfax, VA.

Kennedy, John F. "Establishment of the Special Group (Counter-Insurgency)." *National Security Action Memorandum Number 124*. Washington, D.C.: The White House, 18 January 1962.

Leonard, Mark. "Diplomacy By Other Means." *Foreign Policy* (Sep/Oct 2002): 48-56. Database on-line. Available from ProQuest. Accessed 1 October 2002.

Lord, Carnes. "The Psychological Dimension in National Security." In *Political Warfare and Psychological Operations: Rethinking the US Approach*, ed. Frank B. Barnett and Carnes Lord, 13-37. Washington, DC: National Defense University Press, 1989.

Lowe, Dave. *Idea to Reality: A Brief History of the National Endowment for Democracy*. Available from <http://www.ned.org/about/nedhistory.html>. Accessed 1 February 2003.

Lugar, Richard G. "Beating Terror". *Washington Post* (27 January 2003). Available from <http://www.us.arm.mil/portal/jhtml/earlyBird/Jan2003/e20030127149168.html>. Internet. Accessed 27 January 2003.

Menges, Constantine C. *Inside the National Security Council: the True Story of the Making and Unmaking of Reagan's Foreign Policy*. New York: Simon and Schuster, 1988.

Page 3260 of 3957

Munro, Neil. "Cranking Up the Volume." *National Journal* (6 October 2001): 3083-3084. Database on-line. Available from ProQuest. Accessed 1 October 2002.

Munro, Neil. "Infowar: AK-47s, Lies and Videotape." *Association for Computing Machinery* (July 1999): 19-22. Database on-line. Available from ProQuest. Accessed 22 October 2002.

Muravchik, Joshua. "Hearts, Minds, and the War Against Terror." *Commentator* (May 2002): 25-30. Database on-line. Available from ProQuest. Accessed 1 October 2002.

National Security Council. *Responsibilities and Principles Governing the Conduct of the Foreign Information Program and Psychological Warfare.* National Security Council Memorandum. Washington, D.C.: National Security Council, 25 January 1954.

National Security Council. *Wartime Organization for Overseas Psychological Operations.* National Security Council Memorandum 5812/1. Washington, D.C.: Executive Office of the President, National Security Council, 4 June 1958.

National Security Council. *Wartime Organization for Overseas Psychological Operations.* National Security Council Memorandum. Washington, D.C.: Executive Office of the President, National Security Council, 10 November 1960.

Paddock, Alfred H., Jr. "Military Psychological Operations." In *Political Warfare and Psychological Operations: Rethinking the US Approach*, ed. Frank B. Barnett and Carnes Lord, 45-65. Washington, DC: National Defense University Press, 1989.

Paddock, Alfred H., Jr. <paddockal@earthlink.net>. "Assistance." Electronic mail message to author. 12 February 2003.

Paddock, Alfred H., Jr. *U.S. Army Special Warfare: Its Origins,* revised ed. Lawrence, KS: University Press of Kansas, 2002.

Parmar, Arundhati. "Full-Court Press." *Marketing News* (9 December 2002). Database on-line. Available from ProQuest. Accessed 27 February 2003.

Peterson, Peter G. *Public Diplomacy: A Strategy for Reform – Summary*. A Report of an Independent Task Force on Public Diplomacy Sponsored by the Council on Foreign Relations. Available from <http://www.cfr.org/publication.php?id=4682>. Accessed 23 October 2002.

Peterson, Peter G. "Public Diplomacy and the War on Terrorism." *Foreign Affairs* (September/October 2002). Database on-line. Available from ProQuest. Accessed 23 October 2002.

Prados, John. *Keepers of the Keys: A History of the National Security Council from Truman to Bush*. New York: William Morrow & Company, 1991.

"Presidential Directives and Executive Orders." Available from <http://www.fas.org/irp/offdocs/direct.htm>. Internet. Accessed 28 January 2003.

Page 3261 of 3957

Radvanyi, Janos, ed. *Psychological Operations and Political Warfare in Long-Term Strategic Planning*. New York: Praeger's, 1990.

Reagan, Ronald W. "Management of Public Diplomacy Relative to National Security." *National Security Decision Directive Number 77*. Washington, D.C.: The White House, 14 January 1983.

Reagan, Ronald W. "United States International Broadcasting." *National Security Decision Directive Number 45*. Washington, D.C.: The White House, 15 July 1982.

Reagan, Ronald W. "US International Information Policy." *National Security Decision Directive Number 130*. Washington, D.C.: The White House, 6 March 1984.

Rose, Benjamin R. *Presidentially Mandated Strategic Psychological Warfare Policy Coordination Under Truman and Eisenhower: The Psychological Strategy Board and the Operations Coordinating Board*. Harrisonburg, VA: James Madison University, 1999.

Ross, Christopher. "Public Diplomacy Comes of Age." *The Washington Quarterly* (Spring 2002): 75-83. Database on-line. Available from Wilson OmniFile. Accessed 24 October 2002.

Rothschild, Leah G. "United States' Image to Receive Facelift." *Accuracy in Media* (5 August 2002). Journal on-line. Available from <http://www.aim.org/publications/ briefings/2002/aug05.html>. Internet. Accessed 22 October 2002.

Saxon, Thomas J., Jr. *The Evolution of the National Security Council System Under President Nixon*. Ann Arbor, MI: University Microfilms, 1971.

Smith-Mundt Act. U.S. Code. Title 22, Chapter 18, Sec. 1461 (1948). Excerpt available from <http:www4.law.cornell.edu.uscode/22/1461.html>. Internet. Accessed 27 February 2003.

Summe, Jack <jack.summe@js.pentagon.mil>. "PDD 68 & the IPI Core Group." Electronic mail message to author. 22 October 2002.

Summe, Jack, COL (USA), Chief, Information Strategy Division, Joint Staff J-39. Interview by author, 3 February 2003, The Pentagon, Arlington, VA.

Teinowitz, Ira. "Beers Draws Mixed Review After One Year." *Advertising Age* (23 September 2002). Database on-line. Available from ProQuest. Accessed 27 February 2003.

Timmes, Thomas, Policy Assistant, Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict. Interview by author, 3 February 2003, The Pentagon, Arlington, VA.

Trost, Robert W., COL (USA, Ret), Chief, Information Strategy Division, Joint Staff J-39, June 1997 – July 2000. Interviews by author, October 2002 and February 2003, Fairfax, VA.

U.S. Advisory Commission on Public Diplomacy. *Building America's Public Diplomacy Through a Reformed Structure and Additional Resources.* Washington, D.C.: U.S. Advisory Commission on Public Diplomacy, The State Department, A 2002 Report.

Page 3262 of 3957

U.S. Congress, "The National Security Act of 1947" in *Decisions of the Highest Order: Perspectives on the National Security Council*, ed. Karl F. Inderfurth and Loch K. Johnson, 37-39. Pacific Grove, CA: Brooks/Cole Publishing Company, 1988.

U.S Department of the Army. *The Art and Science of Psychological Operations: Case Studies of Military Application, Volume One*. Department of the Army Pamphlet 525-7-1. Washington, D.C.: U.S. Department of the Army, April 1976.

U.S Department of the Army. *The Art and Science of Psychological Operations: Case Studies of Military Application, Volume Two*. Department of the Army Pamphlet 525-7-2. Washington, D.C.: U.S. Department of the Army, April 1976.

U.S Department of Defense. *Internal Organization of the Department of Defense for Psychological Operations*. Department of Defense Directive S-3140.1. Washington, D.C.: U.S. Department of Defense, 10 January 1953.

U.S Department of Defense. *Organization, Office of Psychological Policy*. Department of Defense Directive C-5132.1. Washington, D.C.: U.S. Department of Defense, 21April 1952.

U.S Department of Defense. *Report to the President's Committee on International Information Activities*. Department of Defense, Office of Psychological Policy Report. Washington, D.C.: U.S. Department of Defense, n.d.

USIA Fact Sheet. Available from <http://dosfan.lib.uic.edu/usia/usiahome/factshe.htm>. Accessed 1 February 2003.

U.S Joint Chiefs of Staff. *National Coordination of Psychological Operations*. Joint Chiefs of Staff Study. Washington, D.C.: The Joint Staff, n.d.

"The U.S. Tries Spinning the Globe." *Columbia Journalism Review* (Nov/Dec 1999): 11. Database on-line. Available from ProQuest. Accessed 1 October 2002.

"U.S. Creates New Agency; Unit to Coordinate Flow of Information Overseas." *The Washington Post* (13 August 1999): A23. Database on-line. Available from ProQuest. Accessed 1 October 2002.

Zorthian, Barry, President, Time-Life Broadcast, Inc. "The Use of Psychological Operations in Combating 'Wars of National Liberation'." Presented to the National Strategy Information Center Conference, 11-14 March 1971.

Exclusive news, data and analytics for financial market professionals LSEG

United States

US Army intelligence analyst charged with selling military secrets to China

By Jasper Ward and Kanishka Singh

March 7, 2024 5:12 PM EST · Updated 2 months ago

WASHINGTON, March 7 (Reuters) - A U.S. Army intelligence analyst was arrested on Thursday and charged with conspiring to sell sensitive defense information to China.

Federal prosecutors charged Korbein Schultz with conspiracy to disclose national defense information, exporting defense articles and technical data without a license, and bribery of a public official, the U.S. Justice Department said in a press release.

Schultz, who was arrested at Kentucky's Fort Campbell, was paid approximately $42,000 to provide an individual he believed lived in Hong Kong with information about U.S. plans in the event Taiwan came under military attack, according to the release. Schultz put "personal profit above the security of the American people," Assistant Attorney General Matthew G. Olsen said in the statement. "Today's arrest shows that such a betrayal does not pay — the Department of Justice is committed to identifying and holding accountable those who would break their oath to protect our nation's secrets."

Get weekly news and analysis on the U.S. elections and how it matters to the world with the newsletter On the Campaign Trail. Sign up here.

Reporting by Jasper Ward; Editing by Caitlin Webber

Our Standards: The Thomson Reuters Trust Principles.

Purchase Licensing Rights

Jasper Ward
Thomson Reuters

Jasper Ward is a breaking news reporter in Washington. She primarily covers national affairs and U.S. politics. Jasper was previously based in The Bahamas where she covered the collapse of FTX and the subsequent arrest of its founder Sam Bankman-Fried. She was a part of the Reuters team that won the Gerald Loeb Award for breaking news for its FTX coverage.

Kanishka Singh
Thomson Reuters

Kanishka Singh is a breaking news reporter for Reuters in Washington DC, who primarily covers US politics and national affairs in his current role. His past breaking news coverage has spanned across a range of topics like the Black Lives Matter movement; the US elections; the 2021 Capitol riots and their follow up probes; the Brexit deal; US-China trade tensions; the NATO withdrawal from Afghanistan; the COVID-19 pandemic; and a 2019 Supreme Court verdict on a religious dispute site in his native India.

Read Next

Environment
Iowa tornado kills 'multiple' people in small town reduced to rubble

United States
Biden cancels $7.7 bln more in student debt for 160,000 borrowers

United States
Trump opts not to take witness stand in hush money case as testimony ends

United States
Democratic U lawmakers in bill to bar for payments to

World ›

RULES ISRAEL-PALESTINIANS
New routes planned for halted Gaza aid from US-built pier

Africa
Chad's PM Masra resigns after disputed election, Deby

Exclusive news, data and analytics for financial market professionals LSEG

Reuters World Business Markets Sustainability Legal Breakingviews Technology Investigations More My View Sign In Register

UK defence minister says intelligence has evidence of Chinese lethal aid to Russia

World · May 22, 2024 · 5:27 AM EDT · 5 min ago

British defence minister Grant Shapps accused China on Wednesday of providing or preparing to provide Russia with lethal aid for use by Moscow in its war against Ukraine.

World
Russia dismisses U.S. claim that Moscow put an anti-satellite weapon in space
5:19 AM EDT · Updated 13 min ago

Lifestyle
Belgium crowns Top Woman in pageant of inner beauty
5:18 AM EDT · Updated 15 min ago

© 2024 Reuters. All rights reserved

Page 3264 of 3957

Joint Military Intelligence College

November 1997
DVP-2600-1828-97

DEFENSE AND INTELLIGENCE ABBREVIATIONS AND ACRONYMS

The Joint Military Intelligence College supports and encourages research on intelligence issues that distills lessons and improves support to policy-level and operational consumers.

DEFENSE AND INTELLIGENCE ABBREVIATIONS AND ACRONYMS

JOINT MILITARY INTELLIGENCE COLLEGE
WASHINGTON, DC
NOVEMBER 1997

This document has been approved for unrestricted public release by the Office of the Secretary of Defense (Public Affairs)

CONTENTS

Foreword..... V

Abbreviations and Acronyms..... 1

Codes for Geopolitical Areas..... 230

Geopolitical Areas by Codes..... 239

DEFENSE AND INTELLIGENCE ABBREVIATIONS AND ACRONYMS

Foreword

This comprehensive list of intelligence abbreviations and acronyms includes those used presently, as well as those in use for approximately the last ten years. Sources for this list include the last DIA Lexicon published in 1991, numerous glossaries from Unified Command and Combat Support Agency documents, and contributions, from the faculty of the Joint Military Intelligence College. The expansion of any item may vary somewhat from one organization to another, but this list will hopefully contribute to greater standardization.

This editor is indebted to kSgt Hannah Reddy (USA) and SSgt Angela Wimbush (USAF) of the College, who spent many hours in collating this list. Debbie Linesberry of the U.S. Special Operations Command collaborated by adding that command's most frequently used acronyms. 2LT Vincent Littrell (USAF) and SFC Mark McCurry (USA) helped ensure that the list contains as few errors as possible, and the editor extends his thanks for that dedicated assistance.

All users are invited to submit additions and corrections. To promote the usefulness of the list, older or superseded acronyms will be discarded only if their retention would create confusion. This list is also published under the JMIC home page on Intelink, where it will be updated regularly. Readers are urged to send new acronyms or abbreviations by mail to: Defense Intelligence Agency, Joint Military Intelligence College, MC Attn: Dr. R. Swenson, Bolling AFB, Washington, DC 20340-5100: by Ingternet to AFswerg@dia.osis.gov, or by Fax to (202) 231-2171.

Dr. Russell G. Swenson, Editor and Director, Office of Applied Research

Page 3269 of 3957

ABBREVIATIONS AND ACRONYMS

A

A2	Air Force Intelligence Staff Officer (component level)
AA	(1) Attack Assessment; (2) Attrition Analysis; (3) Antiaircraft; (4) Avenue of Approach; (5) Automatic Associator
AAA	(1) Antiaircraft Artillery; (2) Air Avenue of Approach
AAAOB	Antiaircraft Artillery Order of Battle
AABNCP	Advanced Airborne National Command Post
AAC	Alaskan Air Command
AACB	Aeronautics and Astronautics Coordinating Board
AACE	Army Alternate Command and Control Element
AACOMS	Army Area Communications System
AACS	Attitude and Antenna Control Subsystem
AAD	Airborne Assault Division
AADC	(1) Army Air Defense Command; (2) Area Air Defense Commander
AADCCS	Area Air Defense Command and Control System
AADP	Area Air Defense Plan
AADS	Antiaircraft Defense System
AAE	Army Acquisition Executive
AAF	Army Airfield
AAFES	Army & Air Force Exchange Service
AAFIF	Automated Air Facilities Information File
AAG	Army Artillery Group
AAI	Air-to-Air Intercept
AAIFF	Air-to-Air Identification Friend or Foe
AAM	Air-to-Air Missile
AAO	Analysis of the Area of Operations
AAR	(1) Active Array Radar; (2) After Action Report
AAS	Analyst Automation Segment
AASLT	Air Assault
AATS	Automated Architecture Tool Suite
AAVS	Aerospace Audiovisual Service
AAW	Anti Air Warfare
AAWC	Anti Air Warfare Commander
AB	Air Base
AB2	Air Battle Command System (ABCS) Brigade and Below
ABC	Airborne Corps
ABCCC	Airborne Battlefield Command and Control Center
ABCOMM	Alternate/Backup Communications

Page 3270 of 3957

ABCS	Army Battle Command System
ABIC	Army Battlefield Interface Concept
ABIT	(1) Airborne Imagery Transmission; (2) Airborne Information Transmission Program
ABM	(1) Antiballistic Missile; (2) Automatic Building Machines
ABMA	Army Ballistic Missile Agency
ABN/Abn	Airborne
ABNCP	(1) Airborne Command Post; (2) Airborne National Command Post
ABR	Available Bit Rate
ABW	Air Base Wing
AC	(1) Air Crew; (2) Active Component; (3) Air Conditioning; (4) Alternating Current
A/C	Aircraft
A2C2	Army Airspace Communications and Control
AC-130	AFSOF Spectre Gunship
AC2SMAN	Alaskan Command and Control System Military Automated Network
AC2MP	Army Command and Control Master Plan
ACA	(1) Alternate Command Authority; (2) Airspace Control Authority
ACAAM	Air Courses of Action Assessment Model
ACACS	Army Command and Area Communications System
ACAT	Acquisition Category
ACC	(1) Access Control Center; (2) Air Control Center; (3) Aviation Component Commander, (4) Air Component Commander, (5) Air Combat Command; (6) Army Component Command
ACCB	Army Configuration Control Board
ACCHAN	Allied Command Channel
ACCIS	Allied Command and Control Information System
ACCISS	(1) Automated Command and Control Intelligence Support System; (2) Alaskan C2 Intelligence Support System
ACCO	Army Central Control Office
ACCS	(1) Airborne Command and Control Squadron; (2) Airborne Command and Control System; (3) Advanced Communications Control System
ACDA	Arms Control and Disarmament Agency
ACDS	Advanced Combat Direction system
ACDUTRA	Active Duty Training
ACE	(1) Allied Command, Europe; (2) Advance Communications Element; (3) Aviation Combat Element; (4) Analysis Control Element; (5) Assistant Corps of Engineers; (6) Airborne Command Element
ACES	Automated Command and Control Evaluation System
ACEVAL	Air Combat Evaluation
ACF	Alternate Command Facility
ACFT	Aircraft
ACI	Airborne Controlled Intercept

Page 3271 of 3957

ACINT	Acoustic Intelligence
ACIS	Arms Control Intelligence Staff
ACL	Access Control List
ACLANT	Allied Commander Atlantic
ACO	(1) Access Control Officer; (2) Airspace Control Officer
ACOC	(1) Area Communications Operations Center; (2) Air Combat Operations Center
ACOM	Atlantic Command
ACOS	Assistant Chief of Staff
ACOS/I	Assistant Chief of Staff for Intelligence (Navy)
ACOUSTINT	Acoustical Intelligence
ACP	(1) Alternate Command Post; (2) Assault CP; (3) Allied Communications Publications; (4) Airspace Control Plan
ACPERS	Army Civilian Personnel System
ACQ	Acquisition
ACR	(1) Armored Cavalry Regiment; (2) Automated Change Recognition
ACS	(1) Afloat Correlation System; (2) Aerial Common Sensor; (3) AUTODIN Switching Center; (4) Airborne COMINT System; (5) Assistant Chief of Staff
ACS/I	Assistant Chief of Staff for Intelligence
ACSA	Allied Communications Security Agency
ACSB	Amphibious Contingency Support Briefs
ACSC	Air Command and Staff College
ACSI	Assistant Chief of Staff Intelligence, HQ USAF
ACT	(1) Air Combat Tactics; (2) Advanced Concepts and Technology Program
ACTD	Advanced Concept Technology Demonstration
ACTEDS	Army Civilian Training, Education, & Development System
ACTS	(1) Advanced Communications Technology; (2) Advanced Communications Technology Satellite
ACUS	(1) Area Common User Systems; (2) Army Common User System
ACV	(1) Armored Command Vehicle; (2) Air Cushion Vehicle; (3) Armored Combat Vehicle
ACW	(1) Aircraft Control and Warning; (2) Anticarrier Warfare; (3) Air Control Wing
AD	(1) Air Defense; (2) Destroyer Tender; (3) Air Division; (4) Artillery Division; (5) Active Duty
A/D	Analog/Digital
ADA	Air Defense Artillery
ADACP	Alcohol & Drug Abuse Control Program
ADAPCP	Alcohol & Drug Abuse Prevention & Control Program
ADAPT	Automated Decisionmaking and Program Timeline
ADARS	Army Defense Acquisition Regulation Supplement
ADATS	Air Defense Antitank System
ADBT	Advanced Data Base Technology

Page 3272 of 3957

ADC	(1) Aide-de-Camp; (2) Air Direction Center; (3) Assistant Division Commander; (4) Air Data Computer; (5) Air Defense Coordinator
ADCAP	Advanced Capability
ADCC	Air Defense Command Center
ADCCP	Advanced Data Communications Control Procedures
ADCOM	(1) Aerospace Defense Command (now SPACECOM); (2) Administrative Command
ADCON	Administrative Control
ADCSOPS	Assistant Deputy Chief of Staff for Operations and Plans
ADD	(1) Air Defense District; (2) Assistant Deputy Director (DIA)
ADDIS	Advanced Deployable Digital Imagery System
ADDISS	Advanced Deployable Digital Imagery Support System
ADDO	Associate Deputy Director of Operations
ADDO(MA)	Associate Deputy Director of Operations for Military Affairs (DIA)
ADDO(MS)	Associate Deputy Director of Operations for Military Support (NSA)
ADDS	Army Data Distribution System
ADDU	Additional Duty
ADE	(1) Audio Deception Emitter; (2) Aerial Delivery Equipment
ADEW	Airborne Directed Energy Weapons
ADF	Automatic Direction Finding
ADFH	Air Deployable Forward Headquarters
ADG	Deperming Ship
ADI	Air Defense Initiative
ADIC	Aerospace Defense Intelligence Center
ADIEC	Army Deployable Imagery Exploitation Capability
ADIO	Additional Duty Intelligence Officer
ADISS	Advanced Defense Intelligence Support System
ADIZ	Air Defense Identification Zone
ADL	(1) Ada Design Language; (2) Armistice Demarcation Line
ADLP	Advanced Datalink Protocol
ADM	(1) Atomic Demolition Munitions; (2) Advanced Development Model; (3) Acquisition Decision Memorandum
Admin	Administration/Administrative
ADN	ACE DGZ Number (NATO)
ADNET	Antidrug Network
ADOC	Air Defense Operations Center
ADP	(1) Automated Data Processing; (2) Airborne Data Processing
ADP-MIS	Automated Data Processing Management Information System

Page 3273 of 3957

ADP-T	(1) Automated Data Processing and Associated Telecommunications; (2) Automated Data Processing and Associated Training
ADPCM	Adaptive Differential Pulse-Code Modulation
ADPE	Automated Data Processing Equipment
ADPS	(1) ASARS Deployable Processing Station; (2) Automated Data Processing System
ADPSSM	Automated Data Processing Systems Security Manual
ADPSSO	ADP Special Security Officer
ADPSSP	Automated Data Processing System Security Program
ADRG	Advanced Digitized Raster Graphics
ADRI	Arc Digital Raster Imagery
ADS	(1) Automated Data System; (2) Air Defense Sector; (3) Airlift Defensive System; (4) Acoustic SOF Detection System; (5) Advanced Distributed Simulation
ADSS	Aerospace Defense Systems Subcommittee
ADSTAR	Advanced Document Storage & Retrieval System
ADSW	Active Duty for Special Work
ADT	(1) Active Duty For Training; (2) Additional Duty Training
ADTLP	Army Doctrine and Training Literature Program
ADTOC	Air Defense Tactical Operations Center
ADTS	Adversary Threat Squadron
ADV	Advance(d)
ADVAL	Air Defense Evaluation Test
ADVON	Advanced Echelon
ADW	Air Defense Warning
ADX	Air Defense Exercise
ADZ	Air Defense Zone
AE	(1) Atomic Energy; (2) Assault Echelon; (3) Ammunition Ship; (4) Aerial Exploitation; Application Entity
AEAO	Airborne Emergency Action Officer
AEB	Aerial Exploitation Battalion
AEC	ASARS Exploitation Cell
AEDS	Atomic Energy Detection System
AEELS	(1) Automatic ELINT Emitter Location System; (2) Airborne ELINT Emitter Location System
AEICC	Area Emergency Information Coordination Center
AEM	Missile Tender
AEMS	Automated Edge Measurement System
AEN	Arbitrary ELINT Notation
AEOS	Advanced Electro-Optical Sensor
AEROFLOT	Former Soviet Union Civil Airline
AES	(1) Atomic Energy Site; (2) Airborne ELINT System
AESC	Aerospace Environmental Support Center
AETC	Air Education and Training Command
AETCAE	Army Europe Technical Control and Analysis Element
AEV	Armored Engineer Vehicle

Page 3274 of 3957

AEW	Airborne Early Warning
AEW&C	Airborne Early Warning and Control
AF	(1) Air Force; (2) Armed Forces; (3) Stores Ship
AFAC	Airborne Forward Air Controller
AF ACSI	Air Force Chief of Staff Intelligence
AFAITC	Armed Forces Air Intelligence Training Center (Goodfellow AFB, TX).
AFAL	Air Force Armament Laboratory
AFAMPE	USAF Automated Message Processing Exchange
AFAMRL	Air Force Aerospace Medical Research Laboratory
AFAP	Artillery-Fired Atomic Projectile
AFARN	Air Force Air Request Net
AFAS	Advanced Field Artillery System
AFATDS	Advanced Field Artillery Tactical Data System
AFB	(1) Air Force Base; (2) Airframe Bulletin; (3) Antifriction Bearing
AFC	(1) Automatic Frequency Control; (2) All-source Fusion Center (Marine Corps)
AFC4A	USAF Command, Control, Communications and Computer Agency
AFCA	Air Force Collection Assets
AFCC	(1) Air Force Communications Command; (2) Air ForceComponent Command
AFCEA	Armed Forces Communications Electronics Association
AFCENT	Allied Forces Central Europe (NATO)
AFCS	(1) Automatic Flight Control System; (2) Army Facility Component System
AFCSC	Air Force Cryptologic Support Center
AFDB	Auxiliary Floating Drydock (large)
AFDD	Air Force Doctrine Document
AFDIGS	Air Force Digital Graphic Systems
AFDL	Auxiliary Floating Drydock (small)
AFDM	Auxiliary Floating Drydock (medium)
AFDT	AEELS Fixed Downlink Terminal
AFEOC	Air Force Emergency Operations Center
AFEWC	Air Force Electronic Warfare Center
AFFIS	Airfield Facilities Information System
AFFOR	Air Force (Component) Forces
AFGCCS	USAF Global Command and Control System
AFGL	Air Force Geophysics Laboratory
AFGWC	Air Force Global Weather Central
AFGWC/FNOC	Air Force Global Weather Center/Fleet Numerical Operations Center
AFGWS	Air Force Ground Weather Stations
AFIA	Air Force Intelligence Agency
AFIC	(1) Air Force Information Center; (2) Air Force Intelligence Command; (3) Air Force Intelligence Center

Page 3275 of 3957

AFICE	Air Forces Iceland
AFICP	Air Force Intelligence Communications Plan
AFIES	Armed Forces Imagery Exploitation System
AFIISP	Air Force Intelligence Information Systems Plan
AFIO	Association of Former Intelligence Officers
AFIP	Air Force Intelligence Plan
AFIS	Air Force Intelligence Service/Study
AFISA	Air Force Intelligence Support Agency
AFIT	Air Force Institute of Technology
AFITC	Air Force Intelligence Training Center
AFIWC	Air Force Information Warfare Center
AFLAN	AFSOC Local/Wide Area Network
AFLANT	U.S. Air Forces, Atlantic
AFLC	Air Force Logistics Command
AFLE	Air Force Liaison Element
AFLO	Air Force Liaison Office
AFM	Air Force Manual
AFMD/GF	Air Forces of the Military District/Group of Forces
AFMC	Air Force Materiel Command
AFMIC	Armed Forces Medical Intelligence Center
AFMPC	Air Force Military Personnel Center
AFMSIS	Air Force Modeling and Simulation Information System
AFMSS	Air Force Mission Support System
AFNET	(1) Air Force Network; (2) Air Force Data Network
AFNORTH	Allied Forces Northern Europe (NATO)
AFNORTHWEST	(1) Allied Forces Northwest Europe (NATO); (2) Air Forces Northwest Region
AFOC	Air Force Operations Center
AFOE	Assault Follow-On Echelon
AFOSI	Air Force Office of Special Investigations
AFOSP	Air Force Office of Security Police
AFOSR	Air Force Office of Scientific Research
AFOTEC	Air Force Operational Test and Evaluation Center
AFR	(1) Air Force Reserve; (2) Air Force Regulation
AFRES	Air Force Reserve
AFS	(1) Air Force Station; (2) Combat Stores Ship
AFSAA	Air Force Studies and Analyses Agency
AFSAC	Air Force Special Activities Center
AFSAT	Air Force Satellite
AFSATCOM	Air Force Satellite Communications System
AFSC	(1) Air Force Systems Command; (2) Air Force Specialty Code; (3) Armed Forces Staff College
AFSCOORD	Assistant Fire Support Coordinator
AFSCF	Air Force Satellite Control Facility
AFSCN	Air Force Satellite Control Network

AFSIP	Air Force Satellite Intelligence Program
AFSOB	Air Force Special Operations Base
AFSOC	Air Force Special Operations Command
AFSOD	Air Force Special Operations Detachment
AFSOE	Air Force Special Operations Element
AFSOF	Air Force Special Operations Forces
AFSOS	Air Force Special Operations School
AFSOUTH	Allied Forces Southern Europe (NATO)
AFSOUTHCOM	Air Force Southern Command
AFSPACECOM	Air Force Space Command
AFSPC	Air Force Space Command
AFSPCIP	Air Force Space Command Intelligence Plan
AFSPOC	Air Force Space Operations Center
AFSSE	Air Force Space Surveillance Element
AFSST	Air Force Space Support Team
AFSTC	Air Force Space Technology Center
AFTAC	Air Force Technical Applications Center
AFTACIES	Air Force Tactical Imagery Exploitation System
AFTF	Air Force Task Force
AFTFWC	Air Force Tactical Fighter Weapons Center
AFV	Armored Fighting Vehicle
AF/VC	Air Force Vice Chief of Staff
AFWAL	Air Force Wright Aeronautical Laboratory
AFWARNS	Air Force Warning System
AFWCCS	Air Force Wing Command and Control System
AFWL	Air Force Weapons Laboratory
AG	(1) Adjutant General; (2) Miscellaneous Auxiliary Ship
AGARD	Advisory Group for Aerospace Research and Development (NATO)
AGB	Icebreaker
AGC	Automatic Gain Control
AGCCS	Army's Global Command and Control System
AGDS	Deep Submergence Support Ship
AGE	Experimental Auxiliary
AGEF	Frigate Research Ship
AGEH	Experimental Auxiliary (Hydrofoil)
AGER	Intelligence Research Ship
AGES	Advanced Ground Exploitation System
AGF	Miscellaneous Command Ship
AGHS	Patrol Combatant Support Ship
AGI	Intelligence Collection Ship
AGL	(1) Buoy Tender; (2) Above Ground Level
AGM	(1) Air-to-Ground Missile; (2) Missile Range Instrumentation Ship
AGMR	Major Communications Relay Ship

Page 3277 of 3957

AGMS	Armored Ground Mobility System
AGOR	Oceanographic Research Ship
AGOS	(1) Ocean Surveillance Ship; (2) Air-Ground Operations School (NATO); (3) Air-Ground Operations System
AGP	Patrol Craft Tender
AGR	Army Guard Reserve
AGS	(1) Hydrographic Survey Ship; (2) FSU Automatic Grenade Launcher
AGT	Agent
AGZ	Actual Ground Zero
AH	(1) Hospital Ship; (2) Alternate Headquarters
AHFEWS	Army High Frequency Electronic Warfare System
AI	(1) Airborne Intercept; (2) Air Intelligence; (3) Artificial Intelligence; (4) Air Interdiction; (5) Airborne Interceptors; (6) Area of Interest; (7) All-Source Intelligence
A3I	Accelerated Architecture Acquisition Initiative
AIA	(1) Army Intelligence Agency; (2) ACE Intelligence Architecture; (3) ACE Interface Architecture; (4) Air Intelligence Agency
AIAA	American Institute of Aeronautics and Astronautics
AIA/IRD	Air Intelligence Agency/Intelligence Reserve Detachment
AIAWS	Automated Intelligence Analyst Workstation
AIB	Atlantic Intelligence Board
AIC	(1) Atlantic Intelligence Command; (2) Afloat Intelligence Center
AICBM	Anti-Intercontinental Ballistic Missile
AID	(1) U.S. Agency for International Development; (2) Aerospace Information Digest; (3) Army Information Digest; (4) Accident, Incident, Deficiencies; (5) Active Integral Defense
AIDES	(1) Analyst Intelligence Information Display and Exploitation System; (2) Automated Intelligence Display and Exploitation System
AIDS	(1) Acoustic Intelligence Data System; (2) Advanced Identification System; (3) Acquired Immune Deficiency Syndrome
AIF	(1) Automated Installations Intelligence File; (2) Army Industrial Fund; (3) Airfield Installation File; (4) Air Intelligence Flight; (5) Automated Installation File
AIFV	Armored Infantry Fighting Vehicle
AIG	(1) Address Indicator Group; (2) Air Intelligence Group
AIIC	Advanced Imagery Interpretation Course
AIIF	Automated Installation Intelligence File
AIIRS	Automated Intelligence Information Retrieval System
AIM	(1) Air Intercept Missile; (2) Active Inert Missile; (3) ADCOM Intelligence Memorandum
AIMD	Aircraft Intermediate Maintenance Department
AIMP	(1) Army Intelligence Management Plan; (2) Army Intelligence Master Plan; (3) Advanced Imagery Management Program; (4) Automated Information Management Program

Page 3278 of 3957

AIMTB	Artificial Intelligence Module Testbed
AIN	Advanced Intelligence Network
AIO	Air Intelligence Officer
AIOEC	Association of Iron Ore Exporting Countries
AIP	(1) Architecture Implementation Plan; (2) Anti-Surface-Warfare Improvement Program
AIPR	Automated Information Processing Request
AIR	American Institute for Research
AIRA	Air Attache
AIRCENT	(1) Air Forces Central Region (NATO); (2) Allied Air Forces Central Europe
AIRCOM	Air Command
AIRCOMTERM	Airborne Communications Terminal
AIRES	Advanced Imagery Requirements and Exploitation System
AIRES II	Airborne Reconnaissance Electronic System II
AIREW	Airborne Infrared Early Warning
AIRK	Area Interswitch Rekeying Key
AIRLO	Air Liaison Officer
AIRREQRECON	Air Request Reconnaissance
AIR	(1) Replenishment Oiler; (2) American Institute of Research
AIRS	(1) Advanced Inertial Reference Sphere; (2) Automated Information Retrieval Systems
AIRTAPS	Aerial Imagery Reconnaissance Tracking and Plotting System
AIS	(1) Automated Indicator System; (2) Advanced Indications Structure; (3) Advanced Indications System; (4) Army Intelligence Survey; (5) Automated Information System; (6) Air Intelligence Squadron
AISA	Automated Intelligence Support Activity
AISS	Automated Information Systems Security
AIST	Air Intelligence Support Team
AITE	Advanced Indications Technology Experiment
AIU	Army Interrogation Unit
AIWO	Air Intelligence Warning Officer
AIWS	Advanced Interdiction Weapon System
AJ	Antijamming
AJCC	Alternate Joint Communications Center
AJFP	Adaptive Joint Force Package
AJNPE	Airborne Joint Nuclear Planning Element
A/JSIC	Alternate JSIC
AK	(1) Cargo Ship; (2) FSU Kalashnikov Family of Assault Rifles; (3) Automatic Remote Rekeying
AKA	Also Known As
AKDC	Automatic Key Distribution Center
AKD/RCU	Automatic Key Distribution/Rekeying Control Unit
AKL	Light Cargo Ship
AKM	(1) Apogee Kick Motor; (2) AK-47 Assault Rifle
AKMC	Automated Key Management Center

Page 3279 of 3957

AKMS	Automated Key Management System
AKR	Vehicle Cargo Ship
AKTCAE	Army Korea Technical Control And Analysis Element
ALAIRCOM	Alaskan Air Command
ALARM	Alert, Locate and Report Missiles
ALASAT	Air-Launched Antisatellite
ALASCOM	Alaskan Communications Inc.
ALB	Air-Land Battle Doctrine (FM 100-5)
ALBM	Air-Launched Ballistic Missile
ALC	Accounting Legend Code
ALCATS	Automated Lines of Communication and Target System
ALCC	Airlift Control Center
ALCE	Airlift Control Element
ALCM	Air-Launched Cruise Missile
ALCOM	Alaskan Command
ALCOP	Alternate Command Post
ALCOR	ARPA Lincoln C-Band Observable Radar
ALCS	Airborne Launch Control System
ALD	Airlift Division
ALE	(1) AIRES Lifecycle Extension; (2) Automated Link Establishment
ALERT	Attack and Launch Early Report to Theater (AF)
ALES	AIRES Life Extension System
ALF	Auxiliary Landing Field
ALFA	Advanced Liaison Forward Area
ALL	Airborne Laser Laboratory
ALMS	Automated Logistics Management System
ALO	(1) Air Liaison Officer; (2) Authorized Level of Organization
ALOC(S)	Air Line(s) of Communication
ALPS	Accidental Launch Protection System
ALRAAM	Air-Launched Long-Range Air-to-Air Missile
ALRP-S	Army Long-Range Plan for Space
ALRPG	Army Long-Range Planning Guidance
ALS	(1) Active Laser Seeker; (2) Airborne Link Segment
ALSA	Air-Land-Sea Application (Center)
ALSS	Advanced Location Strike System
ALT	(1) Alternate; (2) Altitude
ALTAlR	ARPA Long-Range Tracking and Instrumentation Radar
ALTREV	Altitude Reservation
ALUSNA	American Legation U.S. Naval Attache
ALUSNLO	American Legation U.S. Naval Liaison Officer
ALWT	Advanced Lightweight Torpedo
ALWTIC	Annual Land Warfare Technical Intelligence Conference

Page 3280 of 3957

AM	(1) Ante Meridian (Before Noon); (2) Amplitude Modulation; (3) Asset Manager; (4) Aerographers Mate
AMAB	Air Mobile Assault Brigade
AMASS	(1) Advanced Marine Airborne SlGlNT System; (2) Advanced Marine Air Support System
AMBISS	Automated Map-Based Intelligence Support System
AMC	(1) Airspace Management and Control; (2) Army Materiel Command (Formerly DARCOM); (3) Air Mobility Command; (4) Air Mission Commander
AMCC	(1) Ashore Mobile Contingency Communications; (2) Ashore Mobile Command Center
AMC/IN	AMC Deputy Chief of Staff for Intelligence
AMCIT	American Citizen
AMCM	Airborne Mine Countermeasures
AMD	Activated Metal Decoy
AMDT	AEELS Mobile Downlink Terminal
AME	Airspace Management Element
AMEMB	American Embassy
AMETS	Artillery Meteorological System
AMF	Allied Command Europe Mobile Force (NATO)
AMH	Automated Message Handling
AMHA	Army Management Headquarters Activity
AMHS	Automated Message Handling System
AMIDS	Airborne Mine Detection System
AMIM	Army Modernization Information Memorandum
AMIP	Army Model Improvement Plan
AMIRS	Army Multispectral Imagery Requirements Study
AMIS	Advanced Microwave Imaging Sensor
AMM	Army Modernization Memorandum
Ammo	Ammunition
AMMS	(1) Allowance Material Management System; (2) Acquisition Milestone Management System
AMOPES	Army Mobilization and Operations Planning and Execution System
AMOPS	Army Mobilization Operations and Planning System
AMOS	Air Force Maui Optical System
AMP	(1) Amplification; (2) Army Modernization Plan; (3) Acquisition Master Plan
AMPDS	Automated Message Processing Dissemination System
AMPE	Automated Message Processing Exchange
AMPHI	Aerial Mission Photographic Indoctrination
AMPHIB	Amphibious
AMPL	Amplitude
AMPS	(1) Automated Mission Planning System; (2) Automated Message Processing System; (3) Aim Point System
AMRAAM	Advanced Medium-Range Air-to-Air Missile

Page 3281 of 3957

AMRWS	Advanced Remote Miniaturized Weather Station
AMS	(1) Automated Message System; (2) Auto-Manual System; (3) Autonomous Message Switch; (4) Advanced Mapping Spectrometer
AMSAT	Amateur Radio Satellite
AMSC	Advanced Military Spaceflight Capability
AMS-H	Advanced Missile System Heavy
AMSSA	Assured Mission Support Space Architecture
AMST	Advanced Medium STOL Transport
AMT	ACTS Mobile Terminal
AMTF	Airmobile Task Force
AMTP	Army Mission Training Plan
AMU	Astronaut Maneuvering Unit
AMW	Amphibious Warfare
AN	(1) Net Tender; (2) Army/Navy
ANALIT	Analyst-to-Analyst Message Format
ANC	African National Congress
ANCC	(1) Ashore Navy Communications Capability; (2) Automated Network Control Center
ANDVT	Advanced Narrowband Digital Voice Terminal
ANEX	Analyst-to-Analyst Exchange Message Format
ANFO	Ammonium Nitrate Fuel Oil
ANG	Air National Guard
ANGB	Army National Guard Base
ANGLlCO	Air and Naval Gunfire Liaison Company
ANL	Net-Laying Ship
ANLYS	Analysis
ANMCC	Alternate National Military Command Center
ANMIC	Alternate National Military Intelligence Center
ANR	(1) Alaskan NORAD Region; (2) Active Noise Reduction
ANRPC	Association of Natural Rubber-Producing Countries
ANSI	American National Standards Institute
ANVIS	Aviator’s Night Vision Imaging System
AN/VRC	Army Navy Vehicle Radio Communications
ANZUS	Australia, New Zealand, United States
AO	(1) Action Officer; (2) Oiler; (3) Authenticator Organization; (4) Area of Operations; (5) Aerial Observer
AOA	(1) Amphibious Objective Area; (2) Angle of Attack; (3) Angle of Arrival; (4) Airborne Optical Adjunct
AOB	(1) Air Order of Battle; (2) Advanced Operational Base
AOBTS	Air Order of Battle Textual Summary
AOC	(1) Air Officer Commanding (U.K.); (2) Air Operations Center; (3) Army Operations Center
AOCC	Area Operations Control Center
AOCS	Aviation Officers Candidate School
AOE	Fast Combat Support Ship
AOFDA	U.S. AID Office for Foreign Disaster Assistance

Page 3282 of 3957

AOG	Gasoline Tanker
AOI	(1) Area of Influence; (2) Area of Interest
AOIC	Assistant Officer in Charge
AOIR	(1) ACE Operational Intelligence Requirements; (2) Area of Intelligence Responsibility
AOL	Area of Limitation
AO&M/NM	Administration, Operations, and Maintenance/Network Management
AOO	Air Operations Order
AOP	(1) Area of Probability; (2) Air Operations Plan
AOR	Area of Responsibility
AOS	(1) Special Liquids Tanker; (2) Amphibious Objective Study; (3) Area of Separation
AOSG	Amphibious Operation Support Graphic
AOSS	Automated Office Support System
AOT	Transport Oiler
AOTF	Acoustic-Optic Tunable Filter
AP	(1) Armor-Piercing; (2) Air Police; (3) Transport Ship; (4) Associated Press; (5) Ammonium Perchlorate; (6) Antipersonnel; (7) Application Processor
AP-I	Armor Piercing Incendiary
APB	(1) Self-Propelled Barracks Ship; (2) All Points Bulletin; (3) Antipersonnel Bomb; (4) Acquisition Program Baseline
APC	(1) Armored Personnel Carrier; (2) Area of Positive Control; (3) Adaptive Predictive Coding
APCC	Alternate Processing and Correlation Center
APFSDS	Armor-Piercing, Fin-Stabilized, Discarding Sabot
APHIS	USDA Animal and Plant Health Inspection Service
APL	(1) Barracks Craft (non self-propelled); (2) Applied Physics Laboratory (Johns Hopkins University)
APM	Army Program Memorandum
APMS	(1) Automated Production Management System; (2) Advanced Precision Measurement System
APO	(1) Army Post Office; (2) Air Post Office
APOD	Aerial Port of Debarkation
APOE	Aerial Port of Embarkation
APORTS	Aerial Ports File (JOPES)
APP	Application
APPS	Applications
Appl	Application
Approx	Approximately
APPS	Analytical Photogrammetric Position System
APS	(1) ASARS-II Processing Segment; (2) Air Planning System
APT	(1) Automatic Picture Transmission; (2) Airport
APU	Auxiliary Power Unit
APVO	FSU Air Defense Aviation
APW	American Prisoner of War

Page 3283 of 3957

AQF	Advanced QUICKFIX
AR	(1) Advanced Readiness; (2) Army Regulation; (3) Action Required; (4) Repair Ship; (5) Agent Report; (6) Army Reserve; (7) Army
ARABSAT	Arab Satellite (Communications Organization)
ARB	Battle Damage Repair Ship
ARC	(1) Cable Ship; (2) Acquisition Review Committee; (3) Armored Reconnaissance Carrier; (4) Air Reserve Component
ARCENT	U.S. Army Forces Central Command
ARCENT-K	USACENT forward element-Kuwait
ARCENT-SA	USACENT forward element-Saudi Arabia
ARCH	Architecture
ARCOM	Army Command
ARDC	Air Research and Development Command
AREC	Air Element Coordinator
ARCS	(1) Automated Reproduction and Collating System; (2) Acquisition Radar and Control System
ARD	Auxiliary Repair Drydock
ARDF	Airborne Radio Direction Finding
ARDM	Auxiliary Repair Drydock
AREPT	Agent Report
ARF	Airborne Relay Facility
ARFCOS	Armed Forces Courier Service
ARFOR	Army Force(s)
ARG	(1) Amphibious Readiness Group; (2) Internal Combustion Engine Repair Ship
ARIS	Advanced Range Instrumentation Ship
ARL	(1) Landing Craft Repair Ship; (2) Airborne Reconnaissance Low; (3) Army Research Lab; (4) Aerial Reconnaissance Liaison
ARL-I	Airborne Reconnaissance Low-Imagery
ARLANT	U.S. Army Forces, LANTCOM
ARLEA	Army Logistics Evaluation Agency
ARLO	Air Reconnaissance Liaison Officer
ARM	(1) Antiradiation Missile; (2) Atmospheric Radiation Measurement
ARMA	Army Attache
ARMISE	Army Reserve Military Intelligence Support Element
ARMLO	Army Liaison Officer
ARMS	Automated Resource Management System
ARNG	Army National Guard
ARO	(1) Area Records Officer; (2) Auxiliary Readout
ARP	Alert Response Plan
ARPA	Advanced Research Projects Agency
ARPAC	Army Pacific
ARPANET	Advanced Research Projects Agency Network
ARPS	Advanced Radar Processing System

Page 3284 of 3957

ARPV	Advanced Remotely Piloted Vehicle
ARR	Radiological Repair Ship
ARRC	(1) ACE Rapid Reaction Corps; (2) Allied Rapid Reaction Corps
ARRN	Andean Ridge Radar Network
ARRS	Aerospace Rescue and Recovery Service
ARS	(1) Salvage and Rescue Ship; (2) Aerial Reconnaissance and Surveillance; (3) Airborne Receiver System; (4) Air Rescue Service
ARSA	(1) Annual Reevaluation of Safe Areas; (2) Airborne Reconnaissance and Surveillance Architecture
ARSGS	Airborne Reconnaissance SIGINT Ground Systems
ARSO	Assistant Regional Security Officer
ARSOA	Army Special Operations Aviation
ARSOC	Army Special Operations Command
ARSOF	Army Special Operations Forces
ARSOFE	Army Special Operations Forces, Europe
ARSOFSUPCOM	Army Special Operations Forces Support Command
ARSOTF	Army Special Operations Task Force
ARSP	Advanced Reconnaissance Support Program
ARSPACE	Army Space Command
ARSPACECOM	Army Space Command
ARSPOC	Army Space Operations Center
ARSST	Army Space Command Space Support Team
ARSTAF	Army Staff
ART	(1) Aerial Reconnaissance Team; (2) Amateur Radio Transceiver
ARTADS	Army Tactical Data System
ARTAS-K	Army Training and Support-Kuwait (former name for ARCENT-K)
ARTBASS	Army Training Battle Simulation Systems
ARTCC	Air Route Traffic and Control Center
ARTEP	(1) Army Readiness Training Evaluation Program; (2) Army Training and Evaluation Program
ARTISS	Advanced Requirements Tasking Information and Support System
ARTPP	Airborne Reconnaissance Technology Program Plan
ARTS	Automated Remote Tracking Station
ARTY	Artillery
ARV	(1) Armored Recovery Vehicle; (2) Armored Reconnaissance Vehicle; (3) Aircraft Repair Ship
ARW	Air Refueling Wing

Page 3285 of 3957

AS	(1) Submarine Tender; (2) Air Surveillance; (3) Analysis Sub-system; (4) Air Station; (5) Anti Spoofing; (6) Advanced Sensors
ASA	Army Space Agency
ASA	(M&RA)Assistant Secretary of the Army (Manpower and Reserve Affairs)
ASAB	All-Source Analysis Branch
ASAC	All-Source Analysis Center
ASAP	(1) As Soon As Possible; (2) Advanced Sensor Applications Program
ASAR	Advanced Synthetic Aperture Radar
ASARC	Army Systems Acquisition Review Council
ASARS	Advanced Synthetic Aperture Radar System
ASART	(1) AEELS Support Analysis Reporting Terminal; (2) Analysis Support and Reporting Terminal
ASAS	All-Source Analysis System
ASAS-AS	All-Source Analysis System All-Source Workstation
ASAS-E	All-Source Analysis System-Extended
ASAS-SS	All-Source Analysis System Single-Source Workstation
ASAS-W	All-Source Analysis System WARRIOR
ASAT	(1) Antisatellite; (2) Antisatellite Treaty; (3) Advance Satellite Antenna Technology
ASB	(1) Air Surveillance Broadcast; (2) Army Science Board
ASC	(1) AUTODlN Switching Center; (2) Army Service Component; (3) Army Space Command; (4) Advanced Systems Course
ASCAMP	Advanced Single-Channel Manpack
ASCII	American Standard Code for Information Interchange
ASCC	(1) Air Standardization Coordinating Committee; (2) Alternate Space Control Center
ASCII	American National Standard Code for Information Interchange
ASCM	Antiship Cruise Missile
ASCON	Automatic Switched Communications Network
ASD	Assistant Secretary of Defense
ASD (C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASD (C4I)	Assistant Secretary of Defense (Command, Control, Communications, Computers and Intelligence)
ASD (ISA)	Assistant Secretary of Defense for International Security Affairs
ASD (S&R)	Assistant Secretary of Defense for Strategy and Requirements
ASD (SO/LIC)	Assistant Secretary of Defense for Special Operations and Low Intensity Conflict
ASDC	Advanced Space Data Corporation
ASDEP	Army Space Exploitation Demonstration Programs
ASDIA	All-Source Document Index
ASDIAZ	All-Source Document Index Automated File-Compartmented
ASDIAZO	All-Source Document Index Automated File-ORCON
ASDIC	Armed Services Documents Intelligence Center

Page 3286 of 3957

ASDS	(1) Automated SIGINT Dissemination System; (2) Advanced SEAL Delivery System
ASDV	Auxiliary SEAL Delivery Vehicle
ASE	(1) Aircraft Survivability Equipment; (2) Airborne Support Element
ASEAN	Association of Southeast Asian Nations
ASED	Army Space Exploitation Demonstration
ASEDP	Army Space Exploitation Demonstration Program
ASEMA	Army Special Electronic Mission Aircraft
ASF	All-Source Format
ASFC	All-Source Fusion Center
ASG	Area Support Group
ASGOBS	Army Standard Ground Order of Battle System
ASI	(1) Additional Skill Indicator; (2) U.S. Army Space Institute; (3) All-Source Intelligence
ASIC	All-Source Intelligence Center
ASICC	All-Source Intelligence Coordinating Center
ASIDS	Airborne Secondary Imagery Dissemination System
ASIP	All-Source Imagery Processor
ASIPS	Army Standard Intelligence Plotter System
ASIS	Army Space Initiatives Study
ASIT	Adaptable Surface Interface Terminal
ASM	(1) Air-to-Surface Missile; (2) Antiship Missile; (3) Attache Support Message
ASMD	Antiship Missile Defense
ASMT	Assessment
ASN (RDA)	Assistant Secretary of the Navy (Research, Development and Acquisition)
ASOC	Air Support Operations Center
ASOG	Air Support Operations Group
ASOS	Air Support Operations Squadron
ASP	Ammunition Supply Point
ASPAC	Asian and Pacific Council
ASPADOC	Alternate Space Defense Operations Command
ASPB	Assault Patrol Support Boat (Riverine Warfare Craft)
ASPIC	Armed Services Personnel Interrogation Center
ASPJ	Airborne/Advanced Self-Protection Jammer
ASPO	Army Space Program Office
ASPS	All-Source Production Section
ASR	(1) Submarine Rescue Ship; (2) Airport Surveillance Radar; (3) Adaptive Situation Recognizer
ASRP	(1) Airborne SIGINT Reconnaissance Program; (2) Airborne SIOP Reconnaissance Plan
ASRRS	Army Survivable, Recovery and Reconstitution System
ASSC	Alternate Space Surveillance Center
ASSET	All Source Satellite Evaluation Tool

Page 3287 of 3957

ASSIST	(1) Army System for Standard Intelligence Support Terminals; (2) Automated Special Security Terminals; (3) Automated Special Security Information System; (4) Automated Information System Security Incident Support Team
ASSM	Antiship Surface Missile
ASSOTW	Airfields and Seaplane Stations of the World
ASSR	Autonomous Soviet Socialist Republic
ASST	(1) Antiship Surveillance and Tracking; (2) Assistant
ASSW	Antisurface Ship Warfare
ASTAG	Army Service and Technology Advisory Group
ASTEC	Advanced Satellite Technology and Extremely High Frequency Communications
ASTERIX	Automated Analyst Support Tools
ASTMP	Army Science and Technology Master Plan
ASTP	APOLLO-SOYUZ Test Program
ASU	(1) FSU Airborne Self-Propelled Antitank Gun; (2) Approved for Service Use
ASUW	Antisurface Warfare
ASU SWA	Administrative Support Unit Southwest Asia
ASUWC	Antisurface Warfare Commander
ASV	Armored Support Vehicle
ASW	(1) Antisubmarine Warfare; (2) Aircrew Survival Weapon
ASWC	Antisubmarine Warfare Commander
ASWCCS	Antisubmarine Warfare Command and Control System
ASWOC	Antisubmarine Warfare Operations Center
ASWTF	Antisubmarine Warfare Task Force
AT	(1) Antitank; (2) Air Transit; (3) Simple Antenna (Electronic Component); (4) Air Technician; (5) Awaiting Transportation; (6) Antiterrorism, (7) Annual Training
ATA	(1) Actual Time of Arrival; (2) Ocean Tug; (3) Air Transport Association; (4) Advanced Tactical Aircraft; (5) Air Traffic Agency
ATAC	ASAP Technical Advisory Committee
ATACC	Advanced Tactical Air Command Center
ATACMS	(U.S.) Army Tactical Missile System
ATACMS ER	Army Tactical Missile System Extended Range
ATACS	(1) Analyst-to-Analyst Communications Service; (2) Army Tactical Communications System
ATAF	Allied Tactical Air Force (NATO)
ATARS	Advanced Tactical Aerial Reconnaissance System
ATAS	(1) Air-To-Air Stinger; (2) Automatic Terrain Avoidance System
ATB	(1) Air Technical Battalion; (2) Advanced Technology Bomber
ATBM	Antitactical Ballistic Missile
ATC	(1) Air Traffic Control; (2) Air Training Command, USAF; (3) Air Target Chart; (4) Mini-Armored Troop Carrier (Riverine Warfare Craft)
ATCAE	Army Technical Control and Analysis Element

Page 3288 of 3957

ATCC	Air Traffic Control Center
ATCCS	Army Tactical Command and Control System
ATCH	ASW Torpedo-Carrying Helicopter
ATCU	Airfield Traffic Control Unit
ATD	(1) Actual Time of Departure; (2) Advanced Technology Demonstration
ATDB	ACE Target Data Base
ATD/IFD	Advanced Technology Demonstration/Integrated Feasibility Demonstration
ATDL	Automated Tactical Data Link
ATDS	Airborne Tactical Data System
ATE	Automatic Test Equipment
ATETS	Atomic Heat and Powerplant
ATF	(1) Advanced Tactical Fighter; (2) Amphibious Task Force; (3) Fleet Ocean Tug; (4) Aviation Turbine Fuel; (5) After the Fact
ATFD	Automated Tactical Fusion Division
ATGIN	Atomic Ground Intercept
ATGL	Antitank Guided Launcher
ATGM	Antitank Guided Missile
ATH	Above The Horizon
ATI	Automated Tactical Intelligence
ATIC	Aircraft Technical Intelligence Conference
ATIMS	Advanced Technical Information Management System
ATL	ACE Threat List
ATLIS	Airborne Tracking Laser Identification System
atm	Atmosphere
ATM	(1) Antitank Missile; (2) Air Target Materials; (3) Air Target Mosaic; (4) Antitactical Missile; (5) Asynchronous Transfer Mode; (6) Air Tasking Message
A-TM	Alpha Team (Special Forces Operational Detachment)
ATMDE	Army Theater Missile Defense Element
ATMG	Arms Transfer Management Group
ATMOS	Atmospheric Trace Molecules Spectroscopy
ATMP	Air Target Materials Program
ATO	(1) Air Tasking Order; (2) Abort-To-Orbit
ATOC	Allied Tactical Operations Center (NATO)
AFTOCONF	Air Tasking Order Confirmation
ATOL	Assisted Takeoff & Landing
ATOS	Atlantic Theater Operational Intelligence System
ATP	(1) Allied Tactical Publication (NATO); (2) Advanced Technology Program; (3) Advanced Tracking Prototype; (4) Advanced Tactical Planner
ATP-FO	Automated Tracking Prototype Follow-On
ATP/RMBUX	Advance Tracking Prototype/Rocky Mountain Basic UNIX
ATR	Automatic Target Recognition
ATRS	Advanced Tactical Reconnaissance System

Page 3289 of 3957

ATS	(1) Salvage and Rescue Ship; (2) Automated Tasking System; (3) Audit Trail Server; (4) Applications Technology Satellite
ATSS	Alaskan Transportable Satellite System
AT&T	American Telephone and Telegraph
ATT	Technical Assistance Training Team
ATTCS	Army Tactical Command and Control System
ATTD	Advanced Technology Transition Demonstration
ATTE	Assistant Theater Topographic Engineer
ATTG	Automated Tactical Target Graphic
ATTN/Attn	Attention (to the attention of)
ATTP	ACOM Tactics, Techniques, and Procedures
ATWC	Atmospheric Tactical Warning Connectivity
AU	Air University
AUD	Arbitrary Unit Designator
AUGTDA	Augmentation Table of Distribution and Allowances
AUM	Air-to-Underwater Missile
AUS	Army of the United States
AUSA	Association of the United States Army
AUSCANUKUS	Australia, Canada, United Kingdom, United States
AUSD	Assistant Deputy Under Secretary for Defense
AutoID	Automatic Identification
AUTODIN	Automatic Digital Network
AUTOSEC	Automation Security
AUTOSEVOCOM	Automatic Secure Voice Communications Network
AUTOVON	Automatic Voice Network
AUTUMN FORGE	NATO Exercise
AUXCP	Auxiliary Command Post
AV	(1) Armored Vehicle; (2) Audio-Visual; (3) Air Vehicle; (4) Auxiliary Vector
AVCS	Attitude and Velocity Control System
AVF	All-Volunteer Force
AVGAS	Aviation Gasoline
AVHRR	Advanced Very High Resolution Radiometer
AVIM	Aviation Intermediate Maintenance
AVLB	Armored Vehicle-Launched Bridge
AVMF	FSU Naval Aviation
AVMT	Aviation Maintenance Trainer
AVN	Aviation
AVP	Authorized Vendor Program
AVR	Aircraft Rescue Vehicle
AVSAT	Aviation Satellite System
AVSCOM	Aviation System Command
AVT	Auxiliary Aircraft Landing Training Ship
AVUM	Aviation Unit Maintenance

Page 3290 of 3957

AW	(1) Air Warning; (2) Automatic Weapon(s); (3) Water Tanker; (4) All-Weather
AWACS	Airborne Warning and Control System
AWADS	Adverse Weather Aerial Delivery System
AWARS	All-Weather Reconnaissance System
AWC	(1) Air War College; (2) Army War College; (3) Air Warfare Center
AWDS	Automated Weather Distribution System
AWE	Advanced Warfighting Experiment
AWESS I	Automatic Weapon Effect Signature Simulator
AWGN	Additive White Gaussian Noise
AWIS	(1) Army WWMCCS Information System; (2) Aircraft Wireless Intercom System
AWN	Automated Weather Network
AWOP	(1) Absent Without Pay; (2) Automated Weaponeering Optimization Program
AWS	(1) Air Weather Service; (2) Advance Warning System; (3) Analyst Workstation
AWSS	Area Weapon Scoring System
AWT	Water Transport
AWWIMS	Automated Worldwide Warning Indicator Monitoring System
AWX	All-Weather
AXAF	Advanced X-ray Astrophysics Facility
AXP	Allied Exercise Publication
AXT	Training Ship
AZ	Azimuth

Page 3291 of 3957

B

BA	(1) Budget Authority; (2) Budget Activity
BAA	Broad Agency Announcement
BAC	(1) Budget Activity Code; (2) Broad Area Coverage
BAD	Baseline Assessment Document
BADGE FINDER	Proper Name of System
BADGE KEEPER	Proper Name of System
BAE	Battlefield Area Evaluation
BAG	Battalion Artillery Group
BAI	(1) Battlefield Air Interdiction; (2) Backup Aircraft Inventory; (3) Battlefield Artificial Intelligence
BALTAP	Baltic Approaches (NATO Naval Command)
BAN	Base Area Network
BANDIT	Bragg Area Network for Digital Intelligence Transmission
BAO	Basic Attack Option
BAOR	British Army of the Rhine
BARB	Beacon-Aided Radar Bombing
BARCS	Battlefield Area Reconnaissance System
BAS	(1) Broad Area Search; (2) Battlefield Automated Systems; (3) Billet Access System
BASIC	Battle Area Surveillance & Integrated Communications
BASOPS	Base Operations
BASS	Battlefield Surveillance System
BAT-D	Battlefield Deception
BATF	Bureau of Alcohol, Tobacco, and Firearms
BATO	Balloon-Assisted Take-Off
BATS	Ballistic Aerial Target System
BAWB	Bomber Activity Weekly Brief
BB	Battleship
BBBG	Battleship Battle Group
BBLS	Barrels
BBO	Booster Burnout
BBS	Brigade/Battalion Simulation
B2C2	Brigade and Below Command and Control System
BCA	Broadcast Control Authority
BC2A	Bosnia Command and Control Augmentation
BCBL	Battle Command Battle Lab
BCC	Base Communications Center
BCDSS	Battle Command Decision Support System
BCE	Battlefield Coordination Element
BCI	Bit-Count Integrity
BCR	(1) Battlefield Communications Review; (2) Baseline Change Request
BCS	Broadcast Control Station

Page 3292 of 3957

BCT	(1) Base Consolidated Telecommunications; (2) Betac Command Team
BCTP	Battle Command Training Program
BCV	Battle Command Vehicle
Bd	Baud
BDA	(1) Battle Damage Assessment; (2) Bomb Damage Assessment
BDA/PSA	Bomb Damage Assessment/Post Strike Assessment
BDE/Bde	Brigade
BDM	Budget Decision Memorandum
BDP	Battlefield Development Plan
BDS	(1) Base Development Survey; (2) Bulk Data Service
BDSP	Battle Dress System Project
BE	Basic Encyclopedia
BEMT	Basic Electronic Maintenance Trainer
BENELUX	Belgium, Netherlands, Luxembourg
BER	Bit Error Rate
BES	Budget Estimate Submission
BETA	Battlefield Exploitation and Target Acquisition
BEYOND DUTY	Proper Name of System
BF	Battle Force
BFA	Battlefield Function Area
BFACS	BFA Control System
BF(S)BL	Battle Focus (Support) Battle Lab
BFCS	Ballistic Framing Camera System
BFE	Blacker Front End
BFI	Battlefield Interdiction
BFM	Basic Flight Maneuvers
BFMA	Battlefield Functional Mission Area
BFOV	Broad Field of View
BG	(1) Battle Group; (2) Brigadier General
BGN	Board on Geographic Names
BGPHES	Battle Group Passive Horizon Extension System
BGW	Battlefield Guided Weapon
BGWU	Battle Group Workup
BH	Busy Hour
B-H	Bosnia-Hercegovina
BI	Background Investigation
BIACC	Basic Integrated Aircraft Command and Control
BIC	Battlefield Information Center
BICC	Battlefield Information Coordination Center
BICES	Battlefield Information Collection and Exploitation Systems (NATO)
BICM	Battlefield Intelligence Collection Model
BIDS	Battlefield Information Distribution System
BIF	Basic Imagery File

BIFF	Bistatic Identification Friend or Foe
BIIB	Basic Imagery Interpretation Brief
BIIR	Basic Imagery Interpretation Report
BIM	Ballistic Intercept Missile
BIOLDEF	Biological Defense
BIOLOPS	Biological Operations
BIOLWPN	Biological Weapons
BISS	Baseline Intelligence Summary Supplement
BIT	Binary Digit
BITE	Built-In Test Equipment
BITS	Base Information Transfer System
BIU	Bus Interface Unit
Bks	Barracks
BKS	Broadcast Keying Station
BL	Bomb Line
BLDG	Building
BLEST	Berm-Loaded Explosive Simulation Technique
BLEU	Belgium-Luxembourg Economic Union
BLIP	Background Limited IR Photography
BLOS	Beyond Line-of-Sight
BLSS	Base Level Self-Sufficiency Spares
BLT	Battalion Landing Team
BLUE FLAG	ACC command and control exercise
BM	(1) FSU Truck-Mounted Multiple Rocket Launcher; (2) Ballistic Missile
BMATT	Briefcase Multi-Mission Advanced Tactical Terminal
BM/C2	Battle Management/Command and Control
BM/C3	Battle Management/Command, Control, and Communications
BMC	Battle Management Cell
BMCT	Beginning of Morning Civil Twilight
BMD	(1) Ballistic Missile Defense; (2) FSU Airborne Combat Vehicle
BMDO	(1) Ballistic Missile Defense Organization; (2) Ballistic Missile Defense Office
BMDSCOM	U.S. Army Ballistic Missile Defense Systems Command
BMEWS	Ballistic Missile Early Warning System
BMG	Basic Mission Guidance
BMNT	Beginning of Morning Nautical Twilight
BMP	FSU Armored Infantry Combat Vehicle
BMSS	Ballistic Missile Systems Subcommittee
BN/Bn	Battalion
BND	Bundesrepublik Nachrichtendienst (German Intelligence Service)
BOA	Broad Ocean Area
BOCCA	Board for Coordination of Civil Aircraft (NATO)
BOIP	Basis of Issue Plan

Page 3294 of 3957

BOMREP	Bombing Report
BOQ	Bachelor Officers' Quarters
BOS	(1) Battlefield Operating System; (2) Base Operating Support
BP	(1) Battle Position; (2) Bandpass
BPA	(1) Battlefield Psychological Activities; (2) Blanket Purchase Agreement
BPE	Beacon Precision Enlarger
BPF	Bandpass Filter
BPI	Bits Per Inch
BPPBS	Biennial Planning, Programming, and Budgeting System
BPR	Business Process Reengineering
BPS	(1) Basic Psychological Operations Study; (2) Bits Per Second; (3) Beachman Processing System
BPSK	Burst Pulse Shift Key
BR	Blade Rate
B/R	Bridge/Router
BR/Br	Branch
BRAC	Base Realignment and Closure (Commission)
BRDM	FSU Wheeled Amphibious Armored Reconnaissance Vehicle
BRET	Bistatic Reflected Energy Target
BRI	Basic Rate Interface
BRIXMIS	British Commanders-In-Chief Military Liaison Mission
BRL	Bomb Release Line
BRP	Bomb Release Point
BRS	(1) Beachman Reporting System; (2) Backup and Recovery System (3) Beach Reconnaissance System
BRU	Bomb Release Unit
BS	Broadcast Service
BSA	Brigade Support Area
BSD	(1) Battlefield Surveillance Device; (2) Battlefield Surveillance Display
BSS	Broadcast Satellite Service
BSSC	Battle Staff Support Center
BSSG	Brigade Service Support Group
BST	(1) Battle Staff Team; (2) Betac Support Team
BSTS	(1) Boost Surveillance and Tracking System; (2) Boost Phase Surveillance and Tracking System
BT	Basic Training
BTA	Best Technical Approach
BTF	Battalion Task Force
BTG	Basic Target Graphic
BTI	Balanced Technology Initiative
BTR	FSU Armored Personnel Carrier
BTRY	(1) Battery; (2) Field Artillery
BTU	British Thermal Unit
BTW	By The Way

Page 3295 of 3957

BUD/S	Basic Underwater Demolition/Sea-Air-Land (SEAL)
BUIC	Back-Up Intercept Control
BUNT	British Underground Nuclear Test
BUR	Bottom Up Review
BVITS	Baseline Video Imagery Transmission System
BVR	Beyond Visual Range
BW	(1) Biological Warfare; (2) Bandwidth; (3) Beamwidth; (4) Bomb Wing
B&W	Black and White
BWC	Biological Weapons Convention
BWP	Basic Working Paper
BZ	Buffer Zone

Page 3296 of 3957

C

C	(1) Crisis; (2) Confidential; (3) Coniferous
C1	Combined Staff Personnel Officer
C2	(1) Command and Control; (2) Combined or Coalition Forces Intelligence Staff
C2S2LAN	Command and Control Support System LAN
C2W	Command & Control Warfare
C3	Command, Control, and Communications
C3OB	C3 Order of Battle
C3S	Command, Control, and Communications Systems
C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
C4S	Command, Control, Communications, and Computer System
C5	Combined Staff Strategic Planning and Policy Officer
C6	Combined Staff Command, Control and Communications Systems Officer
CA	(1) Cryptanalysis; (2) Heavy Cruiser; (3) Civil Affairs; (4) Combat Assessment; (5) Controlling Authority; (6) COMSEC Account; (7) Command Authority; (8) Counterair
CAA	(1) Concepts Analysis Agency (U.S. Army); (2) Combined Arms Army (FSU); (3) Command Arrangement Agreement
CAB	(1) Current Analysis Branch; (2) Civil Affairs Brigade; (3) Civil Affairs Battalion
CAC	(1) Combined Arms Center; (2) Collection Advisory Center; (3) Control and Analysis Center; (4) Crisis Action Center; (5) Civil Affairs Command; (6) Civil Applications Committee; (7) U.S. Army Combined Arms Command
CACDA	Combined Arms Combat Development Activity
CACM	Central American Common Market
CACTIS	Community/Computer Automated Counterterrorism Intelligence System
CAD	(1) Computer-Assisted Design; (2) Conceptual Architecture Document
CADES	COMIREX Advanced Exploitation System
CADIZ	(1) Canadian Air Defense Identification Zone; (2) Coastal Air Defense Identification Zone
CADOB	Consolidated Air Defense Order of Battle
CADS	Containerized Ammunition Distribution System
CADST	Civil Affairs Direct Support Team
CAE	Computer Aided Engineering
CAF	(1) Crisis Augmentation Facility; (2) Combat Air Forces
CAFMS	Computer-Assisted Force Management System
CAG	(1) Carrier Air Group; (2) Collective Address Group; (3) Commander, Air Group
CAI	Computer-Aided Instruction
CAIF	Command Automated Intelligence File

Page 3297 of 3957

CAIMS	Conventional Ammunition Information Management System
CAJIT	Central America Joint Intelligence Team
CaLANdar	Da Vinci E-Mail Application
CALS	Computer-Aided Acquisition and Logistics Support
CALT	Civil Affairs Liaison Team
CAM	(1) Computer-Assisted Modeling; (2) Computer Aided Manufacturing
CAMO	Computer-Aided Manual Operation
CAMPS	(1) Computer-Aided Management Planning System; (2) Computer-Aided Mission Planning System; (3) Compartmented All-Source Analysis System Message Processing System
CAMS	(1) COMIREX Automated Management System; (2) Communications Area Master Station
CANDOB	Consolidated Aerospace Defense Order of Battle
CANR	Canadian NORAD Region
CAN	Coastal Air Navigation Supplement
CANT	Chinese Atmospheric Nuclear Test
CANUK	US Canada, United Kingdom, United States
CANUS	Canadian - United States
CANUS LANDOP	Canada-United States Land Operations Plan
CAO	(1) Crisis Action Organization; (2) Chief Administrative Officer; (3) Central Action Office
CAO(SOP)	Coordination of Atomic Operations (Standard Operating Procedure)
CAOC	Combined Air Operations Center
CAOCC	Combined Air Operations Coordination Center
CAP	(1) Combat Air Patrol; (2) Civil Air Patrol; (3) Countermeasures Advisory Panel; (4) Crisis Action Planning; (5) Crisis Action Procedures; (6) Capabilities
CAPSULE JACK	Proper Name of System
CAR	(1) Canadian Airborne Regiment; (2) Chief, Army Reserve
CARC	Corrective Action Review Committee
CARDA	(1) Continental Airborne Reconnaissance for Damage Assessment; (2) CONUS Airborne Reconnaissance for Damage Assessment
CARE	Cooperative for American Relief Everywhere, Inc.
CARG	Crisis Action Review Group
CARGRU	Carrier Group
CARIBJIC	Caribbean Joint Intelligence Center
CARIBROC	Caribbean Regional Operations Center
CARICOM	Caribbean Common Market
CARIFTA	Caribbean Free Trade Association
CARL	Category Assignment Responsibility List
CARP	Computed Air Release Point
CARS	(1) Contingency Airborne Reconnaissance System; (2) Common Automated Recovery System

Page 3298 of 3957

CARVE	Criticality, Accessibility, Recuperability, Vulnerability, and Effect
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effects and Recognizability
CAS	(1) Close Air Support; (2) Calibrated Air Speed; (3) Collision Avoidance System; (4) Crisis Action System; (5) Crisis Action Staff; (6) Combined Arms and Services Staff School
CASC	Crisis Action Support Cell
CASE	Computer-Assisted Software Engineering
CASIC	Combined All-Source Intelligence Center
CASLAN	Command Automated Software Local Area Network
CASS	(1) Collection Analysis Support Subsystem; (2) Command Activated Sonobuoy System
CAST	(1) Catalogue of Approved Scientific and Technical Intelligence Tasks; (2) Canadian Air/Sea Transport Group; (3) Computer-Assisted Self Training; (4) Computer Assisted Satellite Track
CAT	(1) Conventional Arms Transfer; (2) Crisis Action Team; (3) Combined Arms Team; (4) Crisis Augmentation Team; (5) Category
CAT-1	RECategory-1 Receive Equipment
CATF	(1) Commander, Amphibious Task Force; (2) Civil Affairs Task Force
CATIS	(1) Computer-Aided Tactical Information System; (2) Computer-Aided Tactical Intelligence System
CATIS/IESS	Computer-Aided Tactical Information System/Imagery Exploitation Support System
CATS	(1) Combined Arms Training Systems; (2) Combat Airlift Tactics' School
CATSS	Cartographic Applications for Tactical and Strategic Systems
CAV	Cavalry
CAVU	Ceiling And Visibility Unlimited
CAWS	Commercial Analyst Work Station
CB	Chemical, Biological
C-band	3.9 to 6.2 GHz Communications Band
CBD	Commerce Business Daily
CBF	Common Budget Framework
CBI	(1) Complete Background Investigation; (2) Computer Based Instruction
CBI/T	Computer-Based Instruction/Training
CBJB	Congressional Budget Justification Book
CBM	Confidence Building Measure(s)
CBO	Congressional Budget Office
CBR	(1) Chemical, Biological, and Radiological; (2) Case Based Reasoning; (3) Constant Bit Rate
CBRN	Caribbean Basin Radar Network
CBRS	Concept Based Requirements System
CBS	Combat Battle Simulation
CBT	(1) Computer-Based Training; (2) Combating Terrorism

Page 3299 of 3957

CBTDEV	Combat Developer
CBTI	Combat Intelligence
CBU	Cluster Bomb Unit
CBW	Chemical and Biological Warfare
CBZ	Confidence Building Zone
CC	(1) Command Center; (2) Command Ship; (3) Cloud Cover; (4) Collection Center; (5) Computer Compatible; (6) Communications Controller; (7) Commander
C-C3	Counter Command, Control, and Communications
CCA	Communications Control Authority
CCB	Configuration Control Board
CCC	(1) CARDA Control Center; (2) Consolidated Command Center; (3) Command and Control Center
CCD	(1) Conference of the Committee on Disarmament; (2) Charged Coupled Device; (3) Camouflage, Concealment, and Deception
CCE	Contingency Communications Element
CCEB	Combined Communications Electronic Board
CCEP	Commercial COMSEC Endorsement Program
CCF	Collection Coordination Facility
CCF-SS	Collection Coordination Facility-Support System
CCG	(1) Combat Control Group; (2) Crisis Coordination Group; (3) Combat Communications Group
CCG-NB	Communications Control Ground-Narrowband
CCGD	Commander, Coast Guard District
CCGP	Combat Communications Group
CCHC	Headquarters Commandant
CCI	Controlled Cryptographic Item
CCIC	Concentrated Counterdrugs Intelligence Collection
CCIP	Command Center Improvement Program
CCIR	International Radio Consultative Committee (French Acronym)
CCIRID	Charge-Coupled Infrared Imaging Device
CCIRM	Collection Coordination and Intelligence Requirements Management
CCIS	(1) Command, Control, and Intelligence Support; (2) Common Channel Intelligence Signaling
CCISCMO	Community Counterintelligence and Security Countermeasures Office
CCISS	Command & Control Intelligence Support Squadron
CCITT	Consultative Committee for International Telephone and Telegraph
CCJ1	USCENTCOM Manpower, Personnel, and Administration Directorate
CCJ2	USCENTCOM Intelligence Directorate
CCJ3	USCENTCOM Operations Directorate
CCJ4/J7	USCENTCOM Logistics and Security Assistance Directorate
CCJ5	USCENTCOM Plans and Policy Directorate

Page 3300 of 3957

CCJ6	USCENTCOM Command, Control, Communications, and Computer Systems Directorate
CCJA	USCENTCOM Staff Judge Advocate
CCM	(1) Cross-Country Movement; (2) Counter-Countermeasure
C3CM	Command, Control, and Communications Countermeasures
CCMF	Consolidated Collection Management Facility
CCN	Crisis Communications Network (CIA)
CCO	(1) Communication Collection Outstation; (2) COMINT Collection Outstation; (3) Circuit Control Officer; (4) Chief, Combat Operations
CCO/SCO	Central Control Office/Sub-Control Office
CCP	(1) Consolidated Cryptologic Program; (2) Communications Checkpoint; (3) Contingency Communications Package
CCPC	Critical Collection Problems Committee
CCPDS	Command Center Processing and Display System
CCPDS-R	Command Center Processing and Display System Replacement
CCS	(1) Collection Capabilities Statement (HUMINT); (2) COMINT Collection Subsystem (3) Combat Control Squadron; (4) Communications Control Set; (5) Command and Control Systems; (6) Constellation Control Station
CCS2	Command and Control Subordinate System
CCSA	USCENTCOM Scientific and Technical Advisor
CCSC	Cryptologic Combat Support Console
CCT	(1) Combat Control Team; (2) Combat Coordination Team
CCTC	Command and Control Technical Center
CCTF	(1) Contingency Communications Test Facility; (2) Combined Coalition Task Force
CCTP	Continuously Computed Target Point
CCTS	Combat Crew Training Squadron
CCTT	Close Combat Tactical Trainer
CCTV	Closed Circuit Television
CCTW	Combat Control Training Wing
CCWT	Command Center Watch Team
CD	(1) Controlled Dissemination; (2) Certificate of Destruction; (3) Civil Defense; (4) Coastal Defense; (5) Calendar Day; (6) Committee on Disarmament; (7) Collateral Damage; (8) Compact Disc; (9) Command Ship; (10) Counter Drug; (11) Command Director; (12) Combat Developments; (13) Community/Service-Developed
C&D	Cover and Deception
CDA	Congressionally Directed Action
CDC	(1) Career Development Course; (2) Combat Direction Center; (3) Combat Development Center
CD-ROM	Compact Disk-Read-Only Memory
CDAS	Central Data and Applications Support
C-Day	Day in Which Movement From Origin Begins
CDB	Central Data Base
CDCS	Communications Distribution Control Segment

Page 3301 of 3957

CDE	(1) Conference on Disarmament in Europe; (2) Compound Damage Expectancy; (3) Center of Distance Education
CDEC	Captured Document Exploitation Center
CDF	Central Document File
CDI	Compact Disc Interactive
CDIP	(1) Consolidated Defense Intelligence Program; (2) Council of Defense Intelligence Producers
CDIS	(1) Communications Data Interface System; (2) Counterdrug Intelligence System
CDIST	Canadian Department of Industry, Science, and Technology
CDL	Common (high bandwidth) Data Link
CDLF	Consolidated Domestic Launch Forecast
CDM	Common Digital Map
CDMA	Code Division Multiple Access
CDP	(1) Central Data Processor; (2) Company Distributing Point
CDPS	Coherent Data Processing System
CDR	(1) Critical Design Review; (2) Commander
CDRL	Contract Data Requirements List
CDRUSAJFKSWC	Commander, United States Army John F. Kennedy Special Warfare Center
CDRUSELEMNORAD	Commander, U.S. Element NORAD
CDRWESTCOM	Commander, U.S. Army Western Command
CDS	(1) Chief of Defence Staff (Canadian); (2) Combat Delivery System; (3) Cryptographic Device Services; (4) Combat Direction System
CDSE	Cryptologic Direct Support Element
CDSORG	Civil Direction of Shipping Organization
CDST	C3CM Data Support Team
CDT	(1) Central Daylight Time; (2) Communications Data Terminal
CDTS	Computer-Directed Training System
CDU	Control Display Unit
CDV	Compressed Digital Video
CE	(1) Circular Error; (2) Cost Effectiveness; (3) Civil Engineer; (4) Communications-Electronics; (5) Corps of Engineers (U.S. Army); (6) Current Exploitation; (7) Counterespionage; (8) Command Element; (9) Collection Emphasis
C&E	Collection and Exploitation
C-E	Communications Electronics
CEAO	West African Economic Community
CEC	(1) Cooperative Engagement Capability; (2) Consolidated Expenditure Center
CECOM	Communications and Electronics Command
CED	(1) Collection, Exploitation, and Dissemination; (2) Captured Enemy Document
CEE	Captured Enemy Equipment
CEI	Communications Electronic Instructions

Page 3302 of 3957

CEL	Celestial
CELT	Current Emitter Location Testbed
CEM	Concepts Evaluation Model
CEMA	Council for Mutual Economic Assistance
CENTAF	(1) Central Region Air Forces (NATO); (2) U.S. Air Force Component, USCENTCOM
CENTAG	Central Army Group (NATO)
CENTAM	Central America
CENTCOM	U.S. Central Command
CENTJIC	Joint Intelligence Center USCENTCOM
CENTLANT	Central Sub-Area of Eastern Atlantic Area
CENTO	Central Treaty Organization
CEO	(1) Communications Electronic Officer (USMC); (2) Chief Executive Officer
CEOI	Communications Electronics Operations Instructions
CEP	(1) Circular Error Probable; (2) Construction Electrician (Power); (3) Common Electronic Parts; (4) Civil Emergency Planning; (5) Committee for Energy Policy of OECD; (6) Capital Equipment Plan; (7) Concept Evaluation Program
CEPG	Combined Exercise Planning Group
CEPIR	Current Exploitation Photographic Interpretation Report
CEPR	Compromising Emanation Performance Requirement
CER	(1) Cryptographic Equipment Room; (2) Communication Equipment Room
CERP	(1) Combined Economic Reporting Program; (2) Capital Equipment Replacement Program
CERT	Computer Security Emergency Response Team
CES	Concept Exploration Studies
CESM	Cryptologic Electronic Warfare Support Measures
CEST	Contingency Exploitation Support Team
CETA	Chinese-English Translation Assistance
CEWI	Combat Electronic Warfare Intelligence
CF	Canadian Forces
C6F	Commander, U.S. Sixth Fleet
C7F	Commander, U.S. Seventh Fleet
CFA	(1) Combined Field Army (Korea); (2) Covering Force Area; (3) Combined Force Air Component Commander
CFB	Canadian Forces Base
CFC	(1) Combined Field Command (Korea); (2) Combined Forces Command (ROK/US); (3) Combined Federal Campaign
CCFC	Commander in Chief, ROK-U.S. Combined Forces Command
CFD	Common Fill Device
CFE	(1) Conventional Forces Europe; (2) Communications Front-End
CFER	CFE Replacement
CFE-U	Communications Front-End-Upgrade
CFI&I	Center for Integration and Interoperability
CFIS	Combined Forces Command Information System, (CFC)

Page 3303 of 3957

CFL	(1) Coordinated Fire Line; (2) Cease-Fire Line
CFMS	Combat Fuels Management System
CFP	(1) Contingency Force Pool; (2) Concept Formulation Process
CFR	Commander Force Reconnaissance
CFSO	Counterintelligence Force Protection Source Operations
CFSR	Contract Funds Status Report
CFV	Cavalry Fighting Vehicle
cg	Center of Gravity
CG	(1) Guided-Missile Cruiser; (2) Consolidated Guidance; (3) Commanding General; (4) Coast Guard; (4) Chairman's Guidance
CGEUSA	Commanding General, 8th US Army
CGF	Central Group of Forces (FSU Forces in Czechoslovakia)
CGFMFLANT	Commanding General, Fleet Marine Forces Atlantic
CGM	Computer Graphics Metafile
CGN	Guided Missile Cruiser Nuclear Powered
CGS	(1) Coast & Geodetic Survey; (2) Common Ground Station; (3) CONUS Ground Station
CGSC	Command and General Staff College (U.S. Army)
CGUSARPAC	Commanding General U.S. Army Pacific
cGy/hr	CentiGray hour
CH	(1) Aviation Cruiser; (2) Channel; (3) Communication Helmet
CHAALS	Communications High Accuracy Airborne Location System
CHAALS-X	CHAALS Exploitation
CHABNCP	Chief, Airborne Command Post
CHAMPUS	Civilian Health And Medical Program of the Uniformed Services
CHARS	Characters
CHB	Cargo Handling Battalion
CHBDL	Communications High Bandwidth Data Link
CHCMSA	Chief, Cruise Missile Support Activity
CHCSS	(1) Chief, Central Security Service; (2) Chief, Cryptologic Support Service
CHG	Guided-Missile Aviation Cruiser
CHGN	Nuclear-Powered Guided-Missile Aviation Cruiser
CHIP	Communications Handbook for Intelligence Planners
CHJUSMAGK	Chief, Joint U.S. Military Assistance Group, Korea
CHJUSMAGPHIL	Chief, Joint U.S. Military Assistance Group, Philippines
CHJUSMAGTHAI	Chief, Joint U.S. Military Assistance Group, Thailand
CHMAAGDOMREP	Chief, Military Assistance and Advisory Group, Dominican Republic
CHMDO JAPAN	Chief, Military Defense Office, Japan
CHN	Nuclear-Powered Aviation Cruiser
CHODC INDIA	Chief, Office of Defense Cooperation, India
CHOP	(1) Change of Operational Command; (2) Change of Operational Control
C-HUMINT	Counter Human Resources Intelligence

Page 3304 of 3957

CHUSMLO	Chief, U.S. Military Liaison Office
CI	(1) Counterintelligence; (2) Counterinsurgency; (3) Current Intelligence
C2I	Command, Control, & Intelligence
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, & Intelligence
C4I2	Command, Control, Communications, Computers, Intelligence and Information
CIA	Central Intelligence Agency
CIAC	Computer Incident Assessment Capability
CIAD	(1) Combat Intelligence Applications Division; (2) Command Intelligence Architecture Document
CIAP	(1) CIA Program; (2) Command Intelligence Architecture/Planning Program
CIARDSCIA	Retirement and Disability System
CIAS	Counterintelligence Analysis Section
CIB	Combat Infantryman's Badge
CIC	(1) Combat Information Center; (2) Combat Intelligence Center; (3) Combined Intelligence Center
C3IC	Coalition Coordination and Communications Integration Center
CICAC	Counterintelligence Control and Analysis Center
CICC	Consolidated Intelligence Communications Center
CIC Server	Combined Intelligence Center Server
CICWS	Combined Intelligence Center Workstation
CID	(1) Criminal Investigation Division; (2) Combat Intelligence Division
CIDBS	Combined Intelligence Center Integrated Database Server
CIDC	Combined Interview and Debriefing Center
CIE	Communication Intercept and Exploitation
CIEF	Consolidated Imagery Exploitation Facility
CIF	(1) Corps Interrogation Facility; (2) Consolidated Intelligence Facility
CIFAX	Enciphered Facsimile
C4IFTW	C4I For The Warrior
CIG	(1) Computer Image Generation; (2) Combined Intelligence Group
CIGSS	Common Imagery Ground Surface System
CIHS	Classified Information Handling System
CIK	Crypto-Ignition Key
CIIC	Current Intelligence and Indications Center
CIID	Command Intelligence Implementation Document
CILMS	Covert Infrared Lighting and Marking System
CILO	Counterintelligence Liaison Office(r)
CILOP	Conversion in Lieu of Procurement
CIM	Corporate Information Management
CIMAS	CENTCOM Iranian Military Activities Summary
CIMEX	Civil Military Exercise (NATO)

Page 3305 of 3957

C-IMINT	Counter Imagery Intelligence
CIMOC	Civil Military Operations Center
CIMP	COMSEC Interoperability Master Plan
CIN	Cargo Increment Number
CINC	(1) Commander in Chief; (2) Commander of a Combatant Command
CINCACOM	Commander in Chief, U.S. Atlantic Command
CINCAFLANT	Commander in Chief, United States Air Forces, Atlantic
CINCAL	Commander in Chief, Alaska
CINCARLANT	Commander in Chief, United States Army Forces, Atlantic
CINCCENT	Commander in Chief, Allied Forces Central Europe (NATO)
CINCCFC	Commander in Chief, Combined Forces Command, Korea
CINCEASTLANT	Commander in Chief, Eastern Atlantic (NATO)
CINCENT	Commander in Chief, Allied Forces, Central Europe
CINCEUR	Commander in Chief, U.S. Forces Europe
CINCFOR	Commander in Chief, Forces Command
CINCFORSCOM	Commander in Chief, U.S. Army Forces
CINCHAN	Commander in Chief, Channel (NATO)
CINCIBERLANT	Commander in Chief, Iberian Atlantic Area
CINCLANT	Commander in Chief, Atlantic Command
CINCLANTFLT	Commander in Chief, Atlantic Fleet
CINCLANTFLTDETSO	Commander in Chief, Atlantic Fleet Detachment SOUTHCOM
CINCMAC	Commander in Chief, Military Airlift Command (archaic)
CINCNORAD	Commander in Chief, North American Air Defense Command
CINCNORTH	Commander in Chief, Allied Forces Northern Europe (NATO)
CINCONAD	Commander in Chief, Continental Air Defense Command
CINCPAC	Commander in Chief, Pacific Command
CINCPACAF	Commander in Chief, Pacific Air Force
CINCPACFLT	Commander in Chief, Pacific Fleet
CINCPACREP	Commander in Chief, Pacific Representative
CINCSAC	Commander in Chief, Strategic Air Command
CINCSOC	Commander in Chief, Special Operations Command
CINCSO	Commander in Chief, Southern Command
CINCSOUTH	Commander in Chief, Allied Forces Southern Europe (NATO)
CINCSPACE	Commander in Chief, U.S. Space Command
CINCSPECOMME	Commander in Chief, Specified Command, Middle East
CINCTAC	Commander in Chief, Tactical Air Command
CINCTRANS	Commander in Chief, Unified Transportation Command
CINCTRANSCOM	Commander in Chief, U.S. Transportation Command
CINCUKAIR	Commander in Chief, United Kingdom Air Defense Region (NATO)
CINCUNC	Commander in Chief, United Nations Command
CINCUSACOM	Commander in Chief, U.S. Atlantic Command
CINCUSAFE	Commander in Chief, U.S. Air Forces, Europe
CINCUSAREUR	Commander in Chief, United States Army, Europe

Page 3306 of 3957

CINCUSARPAC	Commander in Chief, United States Army, Pacific
CINCUSNAVEUR	Commander in Chief, U.S. Naval Forces, Europe
CINCWESTLANT	Commander in Chief, Western Atlantic (NATO)
CINF	Community Imagery Needs Forecast
CINSGCY	Counterinsurgency
CIO	(1) Central Imagery Office; (2) Chief Information Officer
CIOC	(1) Combined Intelligence Operations Center (Korea); (2) Combat Intelligence Operations Center
CIOP	(1) Controlled Intelligence Operational Proposal; (2) CIO Program
CIP	(1) Consolidated Intelligence Program; (2) Country Information Package; (3) Critical Intelligence Parameter; (4) Combined Interoperability Program; (5) Crypto-Ignition Plug; (6) Correlation and Integration Processor
CIPE	(US) CENTCOM Imagery Production Element
CIPEC	Intergovernmental Council of Copper Exporting Countries
CIPHONY	Enciphered Telephone
CIPL	ClNC's Integrated Priority List
CIPMS	Career Intelligence Professional Management System
CIPR	(1) Consolidated Intelligence Production Requirement; (2) Counterintelligence Production Registry
CIPS	Counterintelligence Periodic Summary
C2IPS	C2 Information Processing System
CIR	(1) Central Intelligence Report; (2) Continuing Intelligence Requirement
CIRC	Central Information Reference and Control
CIRCOL	Central Information Reference and Control On-Line System
CIRIS	Consolidated Intelligence Resources Information System
CIRK	Common Interswitch Rekeying Key
CIRL	Current Intelligence Requirements List
CIRT	Computer Security Incident Response Team
CIRVlS	Communications Instructions for Reporting Vital Intelligence Sightings
CIS	(1) Country Intelligence Study; (2) Communications Intercept System; (3) Compensated Imaging System; (4) Canadian Intelligence Service; (5) Chief, Intelligence and Security (Canadian); (6) Combat Instruction Set; (7) Combat Information System; (8) Commonwealth of Independent States; (9) Combat Intelligence System
CISA	C4I Integration Support Activity
CISC	Counterintelligence Support Cell
C3ISC	C3I Systems Committee
CI/SCM	Counterintelligence and Security Countermeasures
CISD	Command Intelligence Strategy Document
CISE	(1) (US) CENTCOM Intelligence Support Element; (2) Corps Intelligence Support Element
CISO	(1) Counterintelligence Support Officer; (2) Counterintelligence Staff Officer
CISPOTREP	CI Spot Report

Page 3307 of 3957

CISR	Communications Intelligence Security Regulation
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CIT	Counterintelligence Team
CITA	Combat Intelligence and Targeting on Arrival
CITS	CENTCOM Imagery Transmission System
CIV	Civilian
CIVC	Carrier Intelligence Center
CIVIC	Civilian Vulnerability Indicator Code
CISION	Enciphered Television
CIW	(1) Consolidated Intelligence Watch; (2) CMOC Intelligence Watch
CIWC	CIW Commander
CIWG	Cooperative Interaction Working Group
CIWS	Close-In Weapon System
C&J	Collection and Jamming
CJB	Congressional Justification Book
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJIATF-E	Commander, Joint Interagency Task Force-East
CJIATF-W	Commander, Joint Interagency Task Force-West
CJIT	Combined Joint Interrogation Team
CJTF	Commander, Joint Task Force
CJTF-AK	Commander, Joint Task Force-Alaska
CJTF-FA	Commander, Joint Task Force-Full Accounting
CK	Compartment Key
CKG	Cooperative Key Generation
CL	Light Cruiser
C-LAMP	Community Laser Measurement Program
CLASS	Close Air Support System
Class	Classification/Classified
C&LB	Coasts and Landing Beaches
CLF	Commander, Landing Force
CLMD	COMSEC Local Management Device
CLNC	Clearance
CLO	(1) Counterdrug Liaison Officer; (2) Chief Logistics Officer
CLOCE	Contingency Lines of Communication, Europe
CLS	(1) Contractor Logistics Support; (2) Clandestine Lighting System
CLSC	COMSEC Logistics Support Center
CLSP	Composite Launch Sequence Plan
CL/TECH	Clear Language Technical Report
cm	Centimeter
CM	(1) Memorandum by the Chairman, Joint Chiefs of Staff; (2) Collection Management; (3) Countermeasure(s); (4) Cruise Missile; (5) Collection Manager; (6) Collection Management Division; (7) Countermine; (8) Countermine Activities

Page 3308 of 3957

CMA	(1) Countermission Analysis; (2) Collection Management Authority; (3) Community Management Account
CMAA	(1) Command Master at Arms; (2) Chief Master at Arms
CMAFB	Cheyenne Mountain Air Force Base
CMAFS	Cheyenne Mountain Air Force Station
CMAH	CINC Mobile Alternate Headquarters
CMAS	Cheyenne Mountain Air Station
C-MASINT	Counter-Measures and Signature Intelligence
CMB	Collection Management Branch
CMC	(1) Cheyenne Mountain Complex; (2) Commandant, U.S Marine Corps; (3) Command Master Chief
C/MC	Command Master Chief
CMCA	Cruise Missile Carrier Aircraft
CMCC	(1) Commander in Chief, Mobile Command Center; (2) Component Mobile Command Center
CMCDS	Community Multilateral Counterterrorism Database System
CMCI	Computed Mission Coverage Index
CMCM	Commandant, U.S. Marine Corp Memorandum
CMCS	(1) COMSEC Material Control System; (2) COMINT Mission Control System
CMD	(1) Collection Management Division; (2) Command
CMDC	Command Cell
CMDR	Commander
CM&D	Collection Management and Dissemination
CME	Communications Monitoring Equipment
CMEA	Council for Mutual Economic Assistance
CMEC	Captured Material Exploitation Center
CMF	Combat Mission Folder
CMFC	Combined Marine Forces Command
CMIC	Combined Military Interrogation Center
CMISE	Corps Military Intelligence Support Element
CML	Chemical
CMO	(1) Collection Management Office; (2) Civil Military Operations; (3) Central MASINT Office
CMOC	(1) Cheyenne Mountain Operations Center; (2) Civil Military Operations Center; (3) Central MASINT Operations Cell
CMOS	Complementary Metal-Oxide Semiconductor
CMOTF	Civil Military Operations Task Force
CMP	(1) Combat Mission Planning; (2) Configuration Management Plan
CMPF	Confidential Military Purpose Funds
CMPS	Compartmented Mode Processing System
CMR	Crisis Management Room
CMRS	Collection Management Requirements System
CMS	(1) Combat Mission Section; (2) Command and Management System; (3) Community Management Staff; (4) Collection Management System; (5) Common Mapping Standard

Page 3309 of 3957

CMS/RMG	Community Management Staff, Resource Management Group
CMSA	Cruise Missile Support Activity
CMSI	Civilian Multi-Spectral Imagery
CMSS	Collection Management Support System
CMST	(1) Collection Management Support Terminal; (2) Collection Management System Tools
CMT	(1) Crisis Management Team; (2) Critical Mobile Target
CMTC	Combat Maneuver Training Center
CMTC-IS	CMTC-Instrumentation System
CMTS	(1) Critical Mobile Target Server; (2) Compliance Monitoring Tracking System
CMW/CMWS	Compartmented Mode Workstation
CN	Counternarcotics
CNA	(1) Center for Naval Analysis; (2) Coordinates Not Available; (3) Critical Node Analysis
CNAC	(1) Customs National Air Command, Oklahoma City; (2) Customs National Aviation Center
CNAD	Conference on NATO Armament Directors
CNAVSPACECOM	Commander, Navy Space Command
CNC	(1) Counternarcotics Center; (2) Computerized Numerical Control
CNCS	Cryptonet Control Station
CN-CMS	Counternarcotics Command and Management System
CNES	Centre National d'Etudes Spatiales (French National Space Agency)
CNET	(1) Chief of Naval Education and Training; (2) Centre National d'Etudes Des Telecommunications
C3NET	Command, Control, and Communications Networks
CNFJ	Commander, U.S. Naval Forces Japan
CNFK	Commander, U.S. Naval Forces Korea
CNFM	Commander, U.S. Naval Forces Marianas
CNI	(1) Communicating NATO Intentions; (2) Communications, Navigation, or Identification
CNIC	Combined Naval Intelligence Center
CNIN	Composite Network, Front-End Internal Network
CNIPS	Counternarcotics Information Processing System
CNK	Cryptonet Key
CNMI	Commonwealth of the Northern Mariana Islands
CNN	Cable News Network
CNO	Chief of Naval Operations
C/No	Ratio of carrier to noise in a 1Hz bandwidth
CNOC	(1) Counternarcotics Operations Center; (2) Combined Naval Operations Center
CNOM	Chief of Naval Operations Memorandum
CNOR	Command Not Operationally Ready
CNR	(1) Chief of Naval Research; (2) Combat Net Radio
CNRIU	Combat Net Radio Interface Unit
CNS	Commercial Network Survivability

Page 3310 of 3957

CNSWTG	Commander, Naval Special Warfare Task Group
CNTL	Command Nuclear Target List
CNVFD	Color Night Vision Fusion Device
CNWDI	Critical Nuclear Weapons Design Information
CO	(1) Commanding Officer; (2) Company
CO3	Combined Staff Public and Governmental Affairs Officer
CO6	Combined Staff Judge Advocate
CO7	Combined Staff Command Surgeon
COA	Course of Action
COB	(1) Close of Business; (2) Collated Operating Base; (3) Chief of Base; (4) Command Operating Budget
COBE	Cosmic Background Explorer
COBOL	Common Business Oriented Language
COC	Combat Operations Center
COCOM	(1) Coordinating Committee; (2) Combatant Command
COD	Carrier On-board Delivery
CODIS	Continuity of Defense Intelligence Systems
COE	Common Operating Environment
COEA	Cost and Operational Effectiveness Analysis
COFIR	Compendium of Future Intelligence Requirements
COFs	Central Operating Facilities
CofS	Chief of Staff
COG	(1) Combined Operations Group; (2) Continuity of Government; (3) Center of Gravity
COI	Communities of Interest
COIC	Combat Operations Intelligence Center (USAFE)
COIN	Counterinsurgency
COINS	(1) Consolidated On-Line Intelligence System; (2) Community On-Line Intelligence Network Systems
COINS-II	Community On-Line Intelligence System-II
COIR	Commander's Operational Intelligence Requirements
COIS	Combat Operations Intelligence System
COLISEUM	Community On-Line Intelligence System for End Users and Managers
COLL	Collection
COLLECT	Collection
COLOP	Collection Opportunity (messages)
COLT	Combat Observation and Laser Team
COM	(1) Computer Output to Microform; (2) Chief of Mission (U.S. Embassy); (3) Collection Operations Management; (4) Commander
COMA	Court of Military Appeals
COMACC	Commander, Air Combat Command
COMAAFCE	Commander, Allied Air Forces Central Europe
COMAFFOR	Commander, Air Force Forces
COMAFOSI	Commander, Air Force Office of Special Investigations

Page 3311 of 3957

COMAFSOC	Commander, U.S. Air Force Special Operations Command
COMAFSPACE	Commander, Air Force Space Command
COMALCOM	Commander, Alaskan Command
COMAMC	Commander, Air Mobility Command
COMARSPACECOM	Commander, Army Space Command
COMASPC	Commander, Air Force Space Command
COMAINT	Command Maintenance
COMAIR-BALTAP	Commander, Allied Air Forces, Baltic Approaches
COMAIRSOUTH	Commander, Allied Air Forces, Southern Europe
COMALCOM	Commander, Alaskan Command
COMALF	Commander of Airlift Forces
COMANR	Commander, Alaskan NORAD Region
COMANTDEF-COM	Commander, Antilles Defense Command
COMARFOR	Commander, Army Forces
COMARSOC	Commander, U.S. Army Special Operations Command
COMARSOF	Commander, U.S. Army Special Operations Forces
COMATF	Commander, Amphibious Task Force
COMBALTAP	Commander, Allied Forces, Baltic Approaches
COMBAT DF	Combat Direction Finding
COMBENE-CHAN	Commander, Benelux Sub-Area Channel
COMBISCLANT	Commander, Bay of Biscay Submarine Area
COMCANLANT	Commander, Canadian Atlantic Submarine Area
COMCARGRU	Commander Carrier Group
COMCENTAG	Commander, Central Army Group, Central Europe
COMCENTLANT	Commander, Central Submarine Area
COMCM	Communication Countermeasures & Deception
COMCO	Canadian SSO
COMCRUDESGRU	Commander Cruiser Destroyer Group
COMDT COGARD	Commandant, U.S. Coast Guard
COMECON	Council for Mutual Economic Assistance
COMEDCENT	Commander, Central Mediterranean Area
COMEDEAST	Commander, Eastern Mediterranean Area
COMEDNOREAST	Commander, Northeast Mediterranean Area
COMEDOC	Commander, Western Mediterranean Area
COMEDS	CONUS Meteorological Data System
COMEDSOUEAST	Commander, Southeast Mediterranean Area
COMEX	(1) Committee on Exchanges; (2) Communications Exercise
COMFAIRKEF	Commander, Fleet Air Keflavik
COMFIVEATAF	Commander, Fifth Allied Tactical Air Force, Southern Europe
COMFLDCOMDASA	Commander, Field Command, Defense Atomic Support Agency
COMFOURATAF	Commander, Fourth Allied Tactical Air Force Central Europe
COMGIB	Naval Commander, Gibraltar
COMGIBMED	Commander, Gibraltar Mediterranean Command
COMGTMODEFCOM	Commander, Guantanamo Defense Command
COMICEDEFOR	Commander, Iceland Defense Force

Page 3312 of 3957

COMIDEASTFOR	Commander, Middle East Force (USN)
COMINEWARCOM	Commander, Mine Warfare Command
COMINT	Communications Intelligence
COMINTADTSK	COMINT Advisory Tasking Message
COMIREX	Committee on Imagery Requirements and Exploitation
COMIS	Collection Management Information System
COMJAM	Communications Jamming
COMJSOC	Commander, Joint Special Operations Command
COMJSOTF	Commander, Joint Special Operations Task Force
COMJTF	Commander, Joint Task Force
COMJUWATF	Commander, Joint Unconventional Warfare Task Force
COML	Commercial
COMLANDFOR	Commander, Land Forces
COMLANDJUT	Commander, Allied Land Forces, Schleswig-Holstein & Jutland
COMLANDNORWAY	Commander, Allied Land Forces, Norway
COMLANDSOUTH	Commander, Allied Land Forces, Southern Europe
COMLANDZEALAND	Commander, Allied Land Forces, New Zealand
COMLANTAREA	Commander, Coast Guard Atlantic Area
COMLOGNET	Combat Logistics Network
COMM	(1) Communication; (2) Commercial
COMM(S)	Communication(s)
COMMAIRCHAN	Commander, Allied Maritime Air Force, Channel
COMMAIRNORLANT	Maritime Air Commander, Northern Submarine Area
COMMARBASPAC	Commander, Marine Corps Base, Pacific
COMMARDEZSECAK	Commander, U.S. Maritime Defense Zone Sector, Alaska
COMMARFOR	Commander, Marine Forces
COMMARFORJAPAN	Commander, Marine Forces, Japan
COMMARFORK	Commander, Marine Forces, Korea
COMMARFORPAC	Commander Marine Corps Forces, Pacific
COMMARFORSOUTH	Commander, Marine Corps Forces, South
COMMCEN	Communications Center
COMMDET	Communications Detachment
COMMO	Communications
COMMS CTR	Communications Center
COMMZ	Communications Zone
COMNAVAIR	Commander, Naval Air Forces
COMNAVAIRLANT	Commander, Naval Air Forces, Atlantic
COMNAVAIRPAC	Commander, Naval Air Forces, Pacific
COMNAVBALTAP	Commander, Allied Naval Forces, Baltic Approaches
COMNAVFOR	Commander, Naval Forces
COMNAVFORK	Commander, Naval Forces, Korea
COMNAVINTCOM	Commander, Naval Intelligence Command
COMNAVLOG	Commander, Naval Logistics
COMNAVMARIANAS	Commander, Naval Forces, Marianas
COMNAVNON	Commander, Allied Naval Forces, North Norway

Page 3313 of 3957

COMNAVSCAP	Commander, Allied Naval Forces, Scandinavian Approaches
COMNAVSEASYSCOM	Commander, Naval Sea Systems Command
COMNAVSECGRU	Commander, Naval Security Group
COMNAVSOF	Commander, Naval Special Operations Forces
COMNAVSPACECOM	Commander, Naval Space Command
COMNAVSPECWARCOM	Commander, Naval Special Warfare Command
COMNAVSURF	Commander, Naval Surface Forces
COMNAVSURFLANT	Commander, Naval Surface Force, U.S. Atlantic Fleet
COMNAVSURFPAC	Commander, Naval Surface Force, Pacific
COMNORECHAN	Commander, Northern Submarine Area, Channel
COMNORLANT	Commander, Northern Submarine Area
COMNORTHAG	Commander, Northern Army Group, Central Europe
COMNSWU	Commander, Naval Special Warfare Unit
COMOCEANLANT	Commander, Ocean Atlantic
COMOCEANSYSLANT	Commander, Oceanographic Systems Atlantic
COMOCEANSYSPAC	Commander, Oceanographic Systems Pacific Company
COMOPS	Communications Operations Summary
COMP	Compatible
COMPACAF	Commander, Pacific Air Forces
COMPASS	Computerized Movement Planning and Status System
COMPATWINGSLANT	Commander, Patrol Wings Atlantic
COMPHIBGRU	Commander, Amphibious Group
COMPLYMCHAN	Commander, Plymouth Submarine Area, Channel
COMPUINT	Computer Intelligence
COMPUSEC	Computer Security
COMPW	Composite Wing
COMPWING	Composite Wing
COMS	Collection Operations Management System (HUMINT)
COMSAT	Communications Satellite
COMSC	Commander, Military Sealift Command
COMSEC	Communications Security
COMSECONDFLT	Commander, U.S. Second Fleet
COMSEVENTHFLT	Commander, U.S. Seventh Fleet
COMSIXATAF	Commander, Sixth Allied Tactical Air Force, Southeastern Europe
COMSIXTHFLT	Commander, U.S. Sixth Fleet
COMSOC	Commander, Special Operations Command
COMSOC-K	Commander, Special Operations Command, Korea
COMSOCEUR	Commander, Special Operations Command, Europe
COMSOCLANT	Commander, Special Operations Command, Atlantic
COMSOCPAC	Commander, Special Operations Command, Pacific
COMSOCSOUTH	Commander, Special Operations Command, Southern Command
COMSOTFE	Commander, Support Operations Task Force, Europe
COMSPOT	Communications Spot Report
COMSTAT	Communication Status Report

Page 3314 of 3957

COMSTRATCOMWING ONE	Commander, Strategic Communications Wing One
COMSTRICKFLANT	Commander, Striking Fleet Atlantic (Afloat)
COMSTRIKFLTLANT	Commander, Striking Fleet, Atlantic
COMSTRIKFORSOUTH	Commander, Striking Force, South
COMSTS	Commander, Military Sea Transportation Service
COMSUBACLANT	Commander, Submarine Forces, Allied Command, Atlantic
COMSUBEASTLANT	Commander, Submarine Force, Eastern Atlantic
COMSUBGRU	Commander, Submarine Group
COMSUBGRU 8/CTF MED	Commander Submarine Group (Mediterranean)/Commander Task Force Mediterranean
COMSUBLANT	Commander, Submarine Force, U.S. Atlantic Fleet
COMSUBMED	Commander, Submarines, Mediterranean
COMSUBPAC	Commander, Submarine Forces, Pacific
COMSUBWESTLANT	Commander, Submarine Force, Western Atlantic Area
COMSUPNAVFOR	Commander, Supporting Naval Forces
COMTAFNORNOR	Commander, Allied Tactical Air Force, North Norway
COMTAFSONOR	Commander, Allied Tactical Air Force, South Norway
COMTASKFORNON	Commander, Allied Task Force, North Norway
COMTECHREP	Complementary Technical Report
COMTHIRDFLT	Commander, Third Fleet
COMTRAPAC	Commander, Training Command, Pacific
COMTWOATAF	Commander, Second Allied Tactical Air Force, Central Europe
COMUKADR	Commander, UK NATO Air Defense Region
COMUSAFAK	Commander, U.S. Air Forces, Alaska
COMUSAFFOR	Commander, United States Air Force Forces
COMUSAFJ	Commander, U.S. Air Forces, Japan
COMUSAFK	Commander, U.S. Air Forces, Korea
COMUSAFTF	Commander, United States Air Force Task Force
COMUSARAK	Commander, U.S. Army Forces, Alaska
COMUSARCENT	Commander, U.S. Army Forces Central Command
COMUSARFOR	Commander, United States Army Forces
COMUSARSO	Commander, United States Army Forces Southern Command
COMUSARSPACE	Commander, U.S. Army Space Command
COMUSARTF	Commander, United States Army Task Force
COMUSASOC	Commander, U.S. Army Special Operations Command
COMUSFOR KOREA	Commander, U.S. Forces Korea
COMUSFK	Commander, U.S. Forces, Korea
COMUSFORAZ	Commander, U.S. Forces, Azores
COMUSFORCARIB	Commander, U.S. Forces, Caribbean
COMUSFORCNTY	Commander US Forces Country
COMUSJ	Commander, U.S. Forces, Japan
COMUSJAPAN	Commander, U.S. Forces, Japan (also COMUSJ)
COMUSJTF	Commander, United States Joint Task Force
COMUSJUWTF	Commander, United States Joint Unconventional WarfareTask Force

Page 3315 of 3957

COMUSKOREA	Commander, U.S. Forces, Korea (also COMUSK)
COMUSLANDFOR	Commander, United States Land Forces
COMUSMACTHAI	Commander, United States Military Assistance Command, Thailand
COMUSMARCENT	Commander, U.S. Marine Forces Central Command
COMUSMARDEZLANT	Commander, U.S. Maritime Defense Zone, Atlantic
COMUSMARDEZPAC	Commander, U.S. Maritime Defense Zone, Pacific
COMUSMARFOR	Commander, United States Marine Forces
COMUSMARTF	Commander, United States Marine Task Force
COMUSMILGP	Commander, United States Military Group
COMUSNAVAK	Commander, U.S. Naval Forces, Alaska
COMUSNAVCENT	Commander, U.S. Naval Forces, Central Command
COMUSNAVEUR	Commander, U.S. Naval Forces, Europe
COMUSNAVFOR	Commander, United States Naval Forces
COMUSNAVPHIL	Commander, U.S. Naval Forces, Philippines
COMUSNAVSO	Commander, U.S. Naval Forces South
COMUSNAVTF	Commander, United States Naval Task Force
COMZEALAND	Commander, Allied Land Forces, New Zealand
CON	Control(led)
CONAD	Continental Air Defense Command
CONDECA	Central America Defense Council
CONF	Confidential
CONFIG	Configuration
CONG	Congress
CONGEN	Consul General
CONGINT	Congressional Interest
ConNMJIC	Contingency NMJIC
CONOBJTR	Conscientious Objector
CONOP(S)	Concept of Operation(s)
CONOPS	(1) United States Army Intelligence Command Continental (United States) Operations; (2) Concept of Operations
CONPG	Chairman, Operational Nuclear Planning Group
CONPLAN	(1) Concept Plan; (2) Contingency Plan
CONR	CONUS NORAD Region
CONTEXT	Conferencing and Text Manipulation System
CONTRA-	Against, Opposite (Prefix)
CONUS	Continental United States
CONUSA	Continental United States Army
CONVL	Conventional
COOP	Continuity of Operations Plan
COORD	Coordination
COP	(1) Command Observation Post; (2) Crashout Package
COPG	Chairman, Operational Planners Group
COPRA	Comparative Postwar Recovery Analysis
COPRL	Command Operations Priority Requirements List

Page 3316 of 3957

COPSTRAT	Continuity of Operations Plan (USSTRATCOM)
COR	(1) Command Operationally Ready; (2) Central Office of Record; (3) Contracting Officer's Representative
CORCEN	Correlation Center
CORE	Contingency Response (Program)
CORL	(1) Collection Opportunity Requirements List; (2) Chief of Receive Location
CORM	Commission on Roles and Missions
CORPS SAM	Corps Surface-to-Air Missile
CORTRAIN	Corps/Division Training Coordination Program
COS	(1) Combat Operations Staff; (2) Chief of Station; (3) Chief of Staff; (4) Communications Segment
cos	Cosine
COSAL	Consolidated Ship/Squadron Allowance
COSCOM	Corps Support Command
COSIN	Control Staff Instructions
COSA	Commander, Oceanographic Systems, Atlantic
COSP	Commander, Oceanographic Systems, Pacific
COSPO	Community Open Source Program Office Cotangent
COTP	Captain of the Port
COTR	Contracting Officer's Technical Representative
COTS	(1) Commercial Off-the-Shelf; (2) Container Offloading Transfer System
COUNTERMASINT	Counter Measurements and Signature Intelligence
COVCOM	Covert Communications
CoVRT	Commanders (and Staff) Visualization Research Tool
CP	(1) Contingency Planning; (2) Command Post; (3) Character Position; (4) Communications Processor; (5) Central Processor; (6) Career Program; (7) Counterproliferation
C&P	Characteristics and Performance
C-P	Counterproliferation
CPA	(1) Chairman's Program Assessment; (2) Collection Planning Aid; (3) CJCS Preparedness Assessment
CPAT	Collection Planning and Targeting
CPB	Charged Particle Beam
CPBS	(1) Capabilities Programming and Budgeting System; (2) Consolidated Program and Budgeting System
CPC	(1) Coastal Patrol Boat; (2) Collection and Processing Center; (3) Central Processing Center
CPE	(1) Circular Probable Error; (2) Central Production Element
CPFL	Contingency Planning Facilities List
CPI	Communications Processor and Interface
CPIA	Chemical Propulsion Information Agency
CPIC	Coastal Patrol and Interdiction Craft
CPM	Cycles Per Minute
CPMIEC	China Precision Machinery Import Export Corporation
CPNET	Custom Product Network

Page 3317 of 3957

CPO	(1) Command Project Officer; (2) Chief Petty Officer
CPP	Communist Party of the Philippines
CPR	(1) Cardio-Pulmonary Resuscitation; (2) Chairman's Program Recommendations
CPS	(1) Collection Problem Set; (2) Correlation Processing Sub-system; (3) Characters Per Second; (4) COMSEC Parent Switch; (5) Craft Positioning System
CPSB	Career Program Selection Board
CPSS	Computer Systems Squadron
CPSU	Communist Party of the Soviet Union
CPT	Command Post Terminal
CPU	(1) Central Processing Unit; (2) Communications Processing Unit; (3) Computer Processing Unit
CPX	Command Post Exercise
CP OSCAR	Command Post Operations Support Center and Rear
CP TANGO	Command Post Tactical Air, Naval, Ground Operations
CQB	Close Quarter Battle
C-QUIP	Combined Quarterly Intelligence Production Listing
CR	(1) Crisis Relocation; (2) Combat Radius; (3) Collection Request; (4) Close Range; (5) Collections Requirement
CRAF	Civil Reserve Air Fleet
CRB	Contingency Reference Book
CRBIF	Crisis Basis Imagery File
CRC	(1) Command and Reporting Center; (2) Control and Reporting Center; (3) CONUS Replacement Center
CRDC	United States Army Chemical Research & Development Center
CRDL	Collateral Recurring Document Listing
CRE	(1) Combat Readiness Evaluation; (2) Control and Reporting Element
CREST	Covert Reconnaissance/Strike
CRF	(1) Crisis Response Force; (2) Cable Reports File
CRIMP	Crisis Management Plan
CRIS	Command Resources Information System
CRISCON	Crisis Condition (I&W System)
C-RISTA	Counter-Reconnaissance, Intelligence, Surveillance, and Target Acquisition
CRITIC	(1) Critical Intelligence; (2) Critical Intelligence Message; (3) Critical Intelligence Communication
CRITICOM	Critical Intelligence Communications Network
CRJOIC	Central Region Joint Operational Intelligence Center
CRL	Certificate Revocation List
CRM	Collection Requirements Management
CRMA	Collection Requirements Management Architecture/Application
CRMO	Collection Requirements Management Office(r)
CRMP	Collection Requirements Management Program or Plan
CRMS	Collection Requirements Management System
CRN	Combat Radio Net

Page 3318 of 3957

CROF	Crete Remote Operating Facility
CROM	Continuous Read-Only Memory
CRP	(1) Control and Reporting Post; (2) COMSEC Resources Program
CRRC	Combat Rubber Raiding Craft
CRRES	Combined Release and Radiation Effects Satellite
CRRS	Customer Requirements Registration System
CRS	(1) COMIREX Requirements Structure; (2) Combined Recording Site; (3) Comprehensive Retrieval Subsystem; (4) Catholic Relief Service; (5) Congressional Research Service; (6) Community Relations Service
CRT	(1) Cathode Ray Tube (Terminal); (2) Combat Readiness Training; (3) Crisis Response Team
CRTA	Chief of Rocket Troops and Artillery
CRUDESGRU	Cruiser-Destroyer Group
CRWG	Current Requirements Working Group
CRYPTO	(1) Cryptography/Cryptographic; (2) Cryptologic
CS	(1) Combat Support; (2) Communications Subsystem; (3) Constant Source; (4) Chief of Staff; (5) Central Servers; (6) Coalition Support
CS1	Critical-Sensitive Level 1
CSA	(1) Chief of Staff, U.S. Army; (2) Central Supplies Agency of NATO; (3) Corps Support Activity; (4) Combat Support Agency(ies)
CSABE	Central and South African Basic Encyclopedia
CSAF	Chief of Staff, U.S. Air Force
CSAFM	Chief of Staff, Air Force Memorandum
CSAM	Chief of Staff, Army Memorandum
CSAR	Combat Search and Rescue
CSAW	Cryptologic Support to Amphibious Warfare
CSB	(1) Close Silo Basing; (2) Collection Support Brief (HUMINT); (3) Current Situation Branch
CSBR	Commander, Special Boat Squadron
CSC	(1) Community Support Center; (2) Customer Support Center; (3) Combat Support Cell
CSCE	Conference on Security and Cooperation in Europe
CSCG	Communications Security Control Group
CSCI	(1) Commercial Satellite Communications Initiative; (2) Computer Software Configuration Interface
CSCR	Computer System Change Request
CSDS	Command Spatial Display System
CSCT	Combat Support Coordination Team
CSE	(1) Cryptologic Support Element(s); (2) Command Support Element; (3) Client Server Environment; (4) Canadian SIGINT Establishment; (5) Communi-cations Security Element
CSE-SS	Client Server Environment-System Services
CSEL	Combat Survivor-Evader Locator
CSENCNET	Satellite Education Network
CSF	Command Support Functions

Page 3319 of 3957

CSFOCI	Force Protection Operations
CSG	(1) Cryptologic Support Group; (2) Chairman's Staff Group; (3) Combat Support Group; (4) Corps Support Group
CSG-SOCOM	Cryptologic Support Group/USSOCOM
CSGN	Nuclear Strike Cruiser
CSI	Commercial Satellite Interconnectivity
C-SIGINT	Counter Signals Intelligence
CSIS	Canadian Security and Investigative Service
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSMO	Cryptologic Support to Military Operations
C3SMP	Command, Control, Communications System Master Plan
CSMR	Coarse Spatial Resolution, Multispectral
CSOC	Consolidated Space Operations Center
CSP	(1) Communications Support Processor; (2) Crisis Staffing Procedures; (3) Contingency Support Package
CSP/HOL	Communications Support Processor/High Order Language
CSPAR	(1) Central Strategic Processing, Analysis, and Reporting; (2) CINC's Preparedness Assessment Report
CSPO	Consolidated SAFE Project Office
CSR	(1) Current Situation Room; (2) Coastal Surveillance Radar; (3) Controlled Supply Rate; (4) Collection Support Requirement; (5) Combat Search & Rescue
CSRD	Communication-Computer Systems Requirement Document
CSRS	Civil Service Retirement System
CSS	(1) Communications Security System; (2) Communications Support System; (3) Central Security Service; (4) Combat Service Support; (5) Collateral Support System; (6) Contingency Support Study; (7) Communications System Segment; (8) Common Sensor System; (9) COMSEC Subordinate Switch; (10) Combat Surveillance Service; (11) Continuous Signature Service; (12) Coded Switch System; (13) Command Specific Server
CSSA	Cryptologic Shore Support Activity
CSSCS	(1) Combat Service Support Control System; (2) Combat Service Support Computer System
CSSD	Combat Service Support Detachment
CSSE	Combat Service Support Element
CSSO	Contractor Special Security Officer
CSSP	Combined Services Support Program
CSSOC	Combat Service Support Operations Center
CSSR	CSS Replacement
CSST	Combat Service Support Team
CST	(1) Central Standard Time; (2) Coastal Survey Team; (3) Coalition Support Team
CSTC	Consolidated Space Test Center
CSTIP	Combined Strategic Intelligence Training Program
CSTOL	Cargo Short Take-Off & Landing
CSTVRP	Computer Security Technical Vulnerability Reporting Program
CT	(1) Training Cruiser; (2) Counterterrorism; (3) Combating Terrorism; (4) Cryptologic Technician

Page 3320 of 3957

CTA	(1) Central Technical Authority; (2) Common Table of Allowances
CTAI	Continuous-Tone Aerial Imagery
CTAK	Cypher-Text Auto-Key
CTAPS	Contingency Theater Automated Planning System
CTB	Comprehensive Test Ban
CTBT	Comprehensive Test Ban Treaty
CTC	(1) Combat Targeting Center; (2) Counterterrorism Center; (3) Combat Training Center
CTD	(1) Collective Training Directorate; (2) Charge Transfer Device
CTDR	Commercial Training Device Requirements
CT&E	Certification Test and Evaluation
CTE	Coefficient of Thermal Expansion
CTEA	Cost and Training Effectiveness Analysis
CTF/JTF	(1) Crisis Task Force; (2) Commander Task Force; (3) Central Training Flight; (4) Combined Task Force; (5) Joint Task Force; (6) Consolidated Training Facility
CTF-B	Combined Task Force-Bomber
CTF-BM	Combined Task Force-Battle Management
CTF-C2	Combined Task Force Director of Intelligence
CTF PC II	CTF Provide Comfort II
CTG	Commander, Task Group
CTH	Aviation Training Cruiser
CTIA	Counter Technical Intelligence Activities
CTIS	Commander's Tactical Information System
CTL	Critical Task List
CTLZ	Control Zone
CTOC	Corps Tactical Operations Center
CTOCSE	CTOC Support Element
CTOL	Conventional Take-Off and Landing
CTP	Consolidated Telecommunications Program
CTR	Center
CTRL	Control
CTS	(1) Course Training Standards; (2) Communications Technology Satellite
CTSCR	Critical Time-Sensitive Collection Requirement
CTT	(1) Commanders' Tactical Terminal; (2) Common Task Test; (3) Combat Control Team
CTTA	Certified TEMPEST Technical Authority
CTT-H	Commanders' Tactical Terminal-Hybrid
CTTP	(1) USCENTCOM Tactics, Techniques, and Procedures Manual; (2) Component Tactics, Techniques, and Procedures Manual
CTU	Commander Task Unit
CU	Channel Unit
CUBB	Collateral Users Bulletin Board
CUBIC	Common User Baseline for the Intelligence Community
CUCV	Commercial Utility Cargo Vehicle

Page 3321 of 3957

CUDIXS	Common-User Digital Information Exchange System
CUL	Combined User Language
CURR	Current
CUSRPG	Canadian-U.S. Regional Planning Group (NATO)
CUWTF	Combined Unconventional Warfare Task Force
CV	(1) Multipurpose Aircraft Carrier; (2) Carrier Vehicle; (3) Aircraft Carrier
CUP	COMSEC Utility Program
CVA	Clandestine Vulnerability Analysis
CVAN	CINCPAC Voice Alert Network
CVBF	Carrier Battle Force
CVBG	Carrier Battle Group
CVG	Guided-Missile Aircraft Carrier
CVGN	Nuclear-Powered Guided-Missile Aircraft Carrier
CVH	V/STOL Aircraft Carrier
CVHG	Guided-Missile V/STOL Aircraft Carrier
CVHGN	Nuclear-Powered Guided-Missile V/STOL Aircraft Carrier
CVHN	Nuclear-Powered V/STOL Aircraft Carrier
CVIC	Carrier-Based Intelligence Center
CVL	Light Aircraft Carrier
CVLGN	Nuclear-Powered Guided-Missile Light Aircraft Carrier
CVLN	Nuclear-Powered Light Aircraft Carrier
CVN	Nuclear Powered Aircraft Carrier
CVRT	Combat Vehicle (Reconnaissance, Tracked)
CVS	(1) Antisubmarine Aircraft Carrier; (2) Commercial Vendor Services
CVSD	Continuously Variable-Slope Delta Modulation
CVT	Training Aircraft Carrier
CVTS	Compressed Video Transmission Service
CVW	Carrier Air Wing
CW	(1) Chemical Warfare; (2) Carrier Wave; (3) Continuous Wave; (4) CONSTANT WATCH; (5) Composite Wing; (6) Commonwealth
C/W	Crisis/Wartime
CWC	(1) Composite Warfare Commander; (2) Conventional Weapons Guide
CWG	Coordinates Working Group
CWI	Conventional Weapons Index
CWIS	Crisis Window Information System
CWO	(1) Communications Watch Office; (2) Chief Warrant Officer
CWS	(1) Compartmented Work Station; (2) Collateral Workstation (ASAS)
CWT	Chemical Weapons Treaty
C2X	CCTF C2 OBI/CI Support Element
CY	Calendar Year
CYCLOPS	Fleet Support Message
CZ	(1) Combat Zone; (2) Convergent Zone

Page 3322 of 3957

D

5D	Demand-Driven Direct Digital Dissemination
D	(1) Deciduous; (2) Density
D2	Data Distribution
DA	(1) Department of the Army; (2) Long-Range Aviation (USSR); (3) Double Agent; (4) Direct Action
D/A	Digital/Analog
DAA	Designated Approval Authority
DAB	Defense Acquisition Board
DABM	Defense Against Ballistic Missiles (Now SDI)
DABS	Dynamic Air Blast Simulator
DAC	(1) Development Assistance Committee of OECD; (2) Department of Army Civilian; (3) Discretionary Access Control
DACCO	Department of the Army Central Control Office
DACCS	Digital Access Cross-Connect System/Switch
DACOM	Data Communications
DACOS	Deputy Assistant Chief of Station
DACOS/I	Deputy Assistant Chief of Staff-Intelligence
DACT	Dissimilar Air Combat Tactics
DACU	(1) Device Access Control Unit; (2) Device Attachment Control Unit
DAD	Dual Air Density
DAES	Defense Acquisition Executive Summary
DAF	Department of the Air Force
DAG	(1) Defense Special Security Communications Systems Address Group; (2) Divisional Artillery Group (FSU)
DAIRSDIA	Advanced Imagery Reproduction System
DAISY	Daily Summary
DAJDIA	Office Symbol for JMITC
DALASP	Defense Advanced Language and Area Studies Program
DALATS	Data Logging and Transmission System
DAMA	Demand Assigned Multiple Access
DAMI	Department of the Army Military Intelligence
DAMPL	Department of the Army Master Priority List
DAO	Defense Attache Office
DAP	Designated Acquisition Program
DAPA	Drug and Alcohol Program Advisor
DAR	Designated Area for Recovery
DARC	District Area Command
DARO	Defense Airborne Reconnaissance Office
DARP	Defense Airborne Reconnaissance Program
DARPA	Defense Advanced Research Projects Agency
DARS	(1) Daily Aerial Reconnaissance and Surveillance; (2) Daily Apportionment and Reconnaissance Scheduling; (3) Daily Aerial Reconnaissance Syndicate

Page 3323 of 3957

DARSC	Defense Airborne Reconnaissance Steering Committee
DARSP	Defense Academic Research Support Program
DART	(1) Developmental Air Reports Tracker; (2) Deployable Automated Remote Terminal
DARTS	Digital Antijam Radio Teletype System
DAS	(1) Defense Attache System; (2) Data Acquisition Segment
DASC	Direct Air Support Center
DASD	(1) Deputy Assistant Secretary of Defense; (2) Direct Access Storage Device
DASD(I&S)	Deputy ASD (Intelligence and Security)
DASH	Deployable Automated Support Host
DASPA	Defense Attache System Property Accounting
DASR	Defense Analysis Special Report
DASVA	Defense Attache System Vehicle Accounting
DAT	Direct Action Team
DATAINT	Data Intelligence
DATEXT	Data Extract
DATPS	Diver Active Thermal Protection System
DATS	Data Automated Tower Simulation
DATT	Defense Attache
DAWN	Defense Attache Worldwide Network
DAWS	Defense Automated Warning System
DAYLT	Daylight
dB	Decibel
DB	Data Base
DBA	Data Base Administrator
DBAS	Data Base Applications System
DBBL	Dismounted Battlespace Battle Lab
DBC	Data Base Correlation
DBCTRL	Data Base Control
DBD	Data Burst Device
dBi	Decibel (referenced to isotropic radiator)
DBIDI	Data Base of Imagery-Derived Information
DBK	Dominant Battlefield Knowledge
dB/K	Decibels per Degrees Kelvin
dBm	Decibels (referred to 1 milliwatt)
DBMAINT	Data Base Administrator
DBMS	Data Base Management System
DBQ	Data Base Query
DBS	(1) Data Broadcast System (also known as SCAMPI); (2) Direct Broadcast Service
dBSM	Decibels Per Square Meter
dBw	Decibels Referenced to One Watt of Power
DC	(1) District Commissioner; (2) Damage Control; (3) Defense Council; (4) Direct Current

Page 3324 of 3957

DCA	(1) Defense Communications Agency; (2) Defense Cooperation Agreement; (3) Defensive Counter Air
DCAEUR	Defense Communications Agency Europe
DCAOC	DCA Operations Control Center
DCAPSS	Dual Criteria Aimpoint Selection System
DCAS	(1) Deployable Consolidated Applications Server; (2) Deployable Communications Applications Shelter
DCCC	Defense Collection Coordination Center
DCE	(1) Defensive Counter Espionage; (2) Data Communications Equipment
D-Cell	Deployment Cell
DCF	DOCS Certification Facility
DCG	Deputy Commanding General
DCGS	Distributed Common Ground System
DCI	Director of Central Intelligence
DCIA	Director, Central Intelligence Agency
DCIB	Defense Counterintelligence Board
DCID	Director of Central Intelligence Directive
DCII	Defense Central Index of Investigations
DCI&S	Director of Counterintelligence and Security
DCIIS	Defense CI Integrated Information System
DCINC	Deputy Commander in Chief
DCIP	Defense Counterdrug Intelligence Program
DCL	Direct Communications Link
DCM	Deputy Chief of Mission
DCMM	Database Creation and Management Module
DCMS	Database Creation and Management Segment
DCN	Defense Communications Network
DCO	(1) Defense Communications Office; (2) Deputy Commander for Operations (USAFE); (3) Dial Central Office; (4) Deputy Commanding Officer
DCOS	Deputy Chief of Staff
DCOSIPR	Deputy Chief of Staff, Intelligence Plans and Requirements
DCP	(1) Disaster Control Plan; (2) Decision Coordinating Paper; (3) Defense Cryptologic Program
DCR	Data Change Request
DCRSI	Digital Cassette Recording System (Improved)
DCS	(1) Defense Communications System; (2) Deputy Chief of Staff; (3) Defense Courier Service
DCS/I	Deputy Chief of Staff Intelligence
DCS/IN	Deputy Chief of Staff for Intelligence
DCSCA	Defense Communications System Central Area
DCSEC	Deputy Chief of Staff, Security
DCSI	Deputy Chief of Staff, Intelligence
DCSIM	Deputy Chief of Staff, Information Management
DCSI/DCSINT	Deputy Chief of Staff Intelligence (USAREUR)
DCSINT	Deputy Chief of Staff for Intelligence (U.S. Army)

Page 3325 of 3957

DCSLOG	Deputy Chief of Staff for Logistics
DCSO	Deputy Commander for Space Operations
DCSOPS	Deputy Chief of Staff for Operations & Plans
DCSP	Design Controlled Spare Part(s)
DCSPER	Deputy Chief of Staff for Personnel
DCS/SSI	Deputy Chief of Staff for Safety, Security, and Intelligence
DCSTOP	Damage Criteria Study Target Data Base
DCTN	Defense Commercial Telecommunications/Teleconferencing Network
DD	(1) Destroyer; (2) Deputy Director; (3) Department of Defense; (4) Differential Doppler
D&D	Denial and Deception
DDAC	Foreign Denial and Deception Analysis Committee
D/DARO	Director, DARO
D-Day	Day in which a particular operation begins
DDC	(1) Defense Documentation Center; (2) Data Distribution Center
DDCI	Deputy Director of Central Intelligence
DDCMP	Digital Data Communications Message Protocol
DDDDD	Demand-Driven Direct Digital Dissemination System
DDG	Guided Missile Destroyer
DDGN	Nuclear-Powered Guided-Missile Destroyer
DDH	Aviation Destroyer (ASW)
DDHG	Guided-Missile Aviation Destroyer
DDHGN	Nuclear-Powered Guided-Missile Aviation Destroyer
DDHN	Nuclear-Powered Aviation Destroyer
DDI	Deputy Director of Intelligence
DDL	Direct Data Link
DDN	(1) Defense Data Network; (2) Defense Dissemination Network
DDO	(1) Deputy Director of Operations; (2) Deputy Duty Officer
DDP	Defense Dissemination Program
DDPO	Defense Dissemination Program Office
DDR&E	Director, Defense Research and Engineering
DDRS	Defense Data Repository System
DDS	(1) Defense Dissemination System; (2) Dry Deck Shelter; (3) Dual Driver Service (courier)
DDS/RL	Defense Dissemination System/Receive Location
DDSP	Defense Development Sharing Project
DDSS	Document Dissemination and Storage Segment
DDT	(1) Training Destroyer; (2) Distributed Decision-Aid Terminal
DDU	Distant Device Unit
DE	(1) Damage Expectancy; (2) Directed Energy; (3) Directorate for Estimates (DIA)
DE-U	Dissemination Element-Upgrade
DE/EW	Directed Energy/Electronic Warfare
DEA	Drug Enforcement Administration
DEACON	Defense Estimates Analytical Computer On-Line Network

Page 3326 of 3957

DEB	(1) Digital European Backbone; (2) Defense Estimative Brief; (3) Debris (Orbital)
DEC	Digital Equipment Corporation
DEC (VAX)	Digital Equipment Corporation (Virtual Address Extension)
DECCO	Defense Commercial Contracting Office (now DITCO)
DECM	(1) Defense Electronic Countermeasures; (2) Deceptive Electronic Countermeasures
DECON	Decontaminate(ion)
DEDAC	Deception and Denial Analysis Committee
DEDDF	Digital Elevation Data Dubbing Facility
DEF	Defense
DEFCON	(1) Defense Condition; (2) Defense Readiness Condition
DEFCOS	Defense Courier System
DEFPLAN	Defense Plan
DEFSMAC	Defense Special Missile and Astronautics Center
Deg	Degree
DEGRAD	Degradation
DELORME	a Digital Mapping Computer Program
DEMEX	Demonstration Exercise
DEMOD	Demodulator
DEMONS	Demonstration System
DEMPC	Data Exploitation, Mission Planning, Communications/Center
DENAS	Daily European Naval Activity Summary
DEP	(1) Deflection Error Probable; (2) Defense Estimate for Production; (3) Deployed
DEPCOMNAVCENT	Deputy COMNAVCENT
DEPCOMUSNAVCENT	Deputy Commander, U.S. Naval Forces Central Command
DEPREP	Deployment Report
DEPSECDEF	Deputy Secretary of Defense
DEPT	Department
DES	(1) Digital Exploitation System; (2) Data Encryption Standard
DESA	Defense Evaluation Support Activity
DESC	Defense Electronics Supply Center
DESIGN	Designator (U.S. Navy)
DESIST	Decision Support and Information System for Terrorism
DESS	Defense Exploitation Support System
DESRON	Destroyer Squadron
DET/Det	Detachment
DEW	(1) Distant Early Warning; (2) Directed Energy Weapon
DEWLINE	Distant Early Warning Line
DF	(1) Direction Finding; (2) Disposition Form; (3) Deuterium Floride
DFAD	Digitized Feature Analysis Data
DFDS	Data Facility Dataset Services
DFED	Digitized Features Data
DFH	Deployed Forward Headquarters

Page 3327 of 3957

DFLP	(1) Defense Foreign Language Program; (2) Democratic Front for the Liberation of Palestine
DFM	Deterrent Force Modules
DFOV	Dual Field of View
DFRIF	Defense Freight Railway Interchange Fleet
DFS	Direction Finding Subsystem
DFT	(1) Deployed for Training Team; (2) Deployment for Training
DG	Defense Guidance
DGCL	Ground Mobile Forces Control Link
DGCS	Downsized Ground Control Station
DGCT	Downsized Ground Control Terminal
DGIAP	Defense General Intelligence Applications Program
DGIF	Deployable Ground Intercept Facility
DGIS	Director General Intelligence and Security
DGITS	Digital Graphics Information Tailoring System
DGS	Deployable Ground Station
DGU	Downgrade to Unclassified
DGZ	(1) Desired Ground Zero; (2) Designated Ground Zero
DH-7	deHavilland Dash 7 (Drug Interdiction Aircraft)
DHCA	Data Handling Capability Analysis
DHFN	Direct Hire Foreign National
DHS	Defense HUMINT Service
DI	(1) Director of Intelligence (USEUCOM); (2) Directorate for Foreign Intelligence (DIA)
DIA	(1) Defense Intelligence Agency; (2) Defense Intelligence Assessment
DIA/CS	Defense Intelligence Agency/Command Support
DIAAPR	Defense Intelligence Agency Appraisal
DIAC	Defense Intelligence Analysis Center
DIAI	DIA Instruction
DIAIAPPR	DIA Intelligence Appraisal
DIAL	Defense Intelligence Agency Liaison
DIAL-J	DIA Liaison Office for Japan
DIALO	DIA Liaison Office
DIALOG	DIA Information Retrieval System
DIAM	Defense Intelligence Agency Manual
DIAMCP	DIA Master Contingency Plan
DIANM	DIA Analytical Memorandum
DIAOB	Defense Intelligence Air Order of Battle
DIAOLS	DIA On-Line System
DIAPF	DIA Part File
DIAR	DIA Regulation
DIATP	DIA Tactical Program
DIATS	DIA Terrorism Summary
DIB	(1) Defense Intelligence Board; (2) Defense Intelligence Brief; (3) Directory Information Base

Page 3328 of 3957

DIC	(1) Defense Intelligence Community; (2) Difference in Condition; (3) Defense Intelligence College (Now JMIC); (4) Defense Intelligence Commentary
DICBM	Depressed Intercontinental Ballistic Missile
DICP	Defense Intelligence Counterdrug Program
DID	(1) Data Line Description; (2) Defense Intelligence Digest (Now Military Intelligence Digest); (3) Data Item Description
DIDHS	Deployable Intelligence Data Handling System
DIDOP	Digital Image Data Output Product
DIDS	Defense Intelligence Dissemination System
DIDSRS	Defense Intelligence Dissemination, Storage and Retrieval System
DIE	Defense Intelligence Estimate
DIEB	Defense Intelligence Executive Board
DIEC	Deployable Imagery Exploitation Capability
DIEPS	Digital Imagery Exploitation and Production System
DIEM	Defense Intelligence Estimates Memorandum
DIEOB	Defense Intelligence Electronic Order of Battle
DIFAR	(1) Directional Frequency Analysis and Recording System; (2) Directional Frequency and Ranging
DIFAX	(1) Defense Intelligence Facsimile; (2) Defense Intelligence Security Facsimile Network
DIFM	Defense Intelligence Functional Manager
DIFR	Defense Intelligence Facility Report
DIGITS	Digital Geographic Information Tailoring System
DIGOB	Defense Intelligence Ground Order of Battle
DIH	Daily Intelligence Highlights
DIHEST	Direct Induced High-Explosives Simulation Technique
DII	Defense Information Infrastructure
DIIN	Defense Imagery Intelligence Notice
DIIP	Defense Intelligence Interoperability Panel
DIIPS	Digital Imagery Interactive Processing System
DIIS	DIA Integrated Intelligence System
DILC	Dedicated Intelligence Loop Circuit
DIM	Defense Intelligence Memorandum
DIMES	Digital Image Manipulation & Enhancement System
DIMMD	Diver Integral Magnetic Mine Detector
DIMOB	Defense Intelligence Missile Order of Battle
DIMSS	DSN Integrated Management Support System
DIN	(1) Defense Intelligence Notice; (2) Defense Intelligence Network; (3) AUTODIN
DINAH	Desktop Interface to AUTODIN Host
DINOB	Defense Intelligence Naval Order of Battle
DINSUM	Defense Intelligence Summary

Page 3329 of 3957

DIO	(1) Defense Intelligence Officer (DIA); (2) District Intelligence Officer (U.S. Navy); (3) Defence Intelligence Organisation (Australian)
DIOB	Defense Intelligence Order of Battle
DIOBS	Defense Intelligence Order of Battle System
DIOP	Defense Intelligence Objectives and Priorities
DIP	(1) Defense Intelligence Plan; (2) Defense Imagery Program
DIPC	Defense Intelligence Production Council/Conference
DIPFAC	(1) U.S. Diplomatic Facilities Graphic; (2) Diplomatic Facility
DIPOLES	Defense Intelligence Photoreconnaissance On-Line Exploitation System
DIPP	Defense Intelligence Projection for Planning
DIPS	(1) Defense Intelligence Production Schedule; (2) Digital Imagery Processing System; (3) Def Intelligence Production Study
DIR	(1) Defense Intelligence Report; (2) Directive; (3) Defense Imagery Report; (4) Director; (5) Direction
DIRCM	Direct Infrared Countermeasures
DIRES	Defense Imagery Requirements and Exploitation System
DIRINT	Director of Intelligence
DIRLAUTH	Direct Liaison Authorized
DIRNSA	Director, National Security Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DIROI	Directorate Operating Instruction
DIRS	(1) Defense Intelligence Reference Series; (2) Defense Imagery Reference Series
DIS	(1) Defence Intelligence Staff (U.K.); (2) Defense Investigative Service; (3) Defense Intelligence Summary; (4) Daily Intelligence Summary; (5) Distributive Interactive Simulation; (6) Data Integration System; (7) Defense Information System
DISA	Defense Information Systems Agency
DISA-EUR	Defense Information Systems Agency-Europe
DISA-PAC	DISA-Pacific
DISA WESTHEM	DISA Western Hemisphere
DISAM	Defense Institute of Security Assistance Management
DISC	Daily Intelligence Summary Cable
DISC4	Director of Information Systems Command, Control, Communications and Computers
DISCAS	Defense Intelligence Special Career Automated System
DISE	Deployable Intelligence Support Element
DISECS	Defense Intelligence Space Exploitation and Correlation System
DISES	Defense Intelligence Senior Executive Service
DISIDS	Display and Information Distribution System/Subsystem
DISMOB	Defense Intelligence Strategic Missile Order of Battle
DISN	Defense Information Systems Network
DISNET	Defense Integrated Secure Network
DISO	Defense Intelligence Support Office

Page 3330 of 3957

DISOB	Defense Intelligence Space Order of Battle
DISP	Defense Industrial Security Program
DISPEWT	Defense Intelligence Space Electronic Warfare Threat Data Base
DISR	(1) Daily Indicator Status Report; (2) Defense Indications Status Report
DISS	(1) Digest of Intelligence and Security Services; (2) Dissemination
DISSEM	Dissemination
DISSO	Deputy Information Systems Security Officer
DIST	Digital Imagery Support Terminal
DISTAFF	Directing Staff (NATO Commands, JECG)
DISTS	Defense Intelligence Secure Telephone System
DISTP	Defense Intelligence Special Technologies Program
DISUM	(1) Daily Intelligence Summary; (2) Defense Intelligence Summary
DIT	Defense Intelligence Thesaurus
DITB	Digital Imagery Test Bed
DITCO	Defense Information Technology Contracting Office (formerly DECCO)
DITDS	Defense Intelligence Threat Data System
DITEQ	Defense Intelligence Thesaurus Equivalency List
DITFOR	Defense Intelligence Technical Forum
DITS	Digital Imagery Transmission System
DITSUM	Defense Intelligence Terrorism Summary
DIV	(1) Division; (2) Defense Intelligence Videocassette
DIVARTY	Division Artillery
DIVISION	Enciphered Television
DIW	Dead in Water
DIWO	Duty Intelligence Watch Officer
DIWS	(1) Digital Imagery Workstation Suite; (2) Defense Indications and Warning System; (3) DOD Intelligence Warning System
DJ2	Deputy Director of Intelligence
DJS	Director, Joint Staff
DJSM	DJS Memorandum
DJTF	Deployable Joint Task Force
DJTFAC	DJTF Augmentation Cell
DLA	Defense Logistics Agency
DLAB	Defense Language Aptitude Battery
DLEA	Drug Law Enforcement Agency
DLED	Dedicated Loop Encryption Device
DLI	Defense Language Institute
DLIFLC	Defense Language Institute, Foreign Language Center
DLO	Defense Liaison Office
DLPT	Defense Language Proficiency Test
DLTV	Daylight Television
D&M	Detection and Monitoring

Page 3331 of 3957

DM	(1) Dissemination Manager; (2) Decompression Monitor
DMA	(1) Defense Mapping Agency; (2) Direct Memory Access
DMAAC	Defense Mapping Agency Aerospace Center
DMACSC	Defense Mapping Agency Combat Support Center
DMAHTC	DMA Hydrographic and Topographic Center
DMAI	Defense Mapping Agency Instruction
DMAL	Defense Mapping Agency Liaison
DMAR	Deferred Maintenance and Repair
DMB	DODIIS Management Board
DMC&GP	Defense MC&G Program
DMD	Digital Message Device
DMDG	Digital Message Device Group
DME	Distance Measuring Equipment
DMED	Digital Message Entry Device
DMFE	DAWS Message Front End
DMI	Directorate of Military Intelligence
DMOB	Defensive Missile Order of Battle
DMOS	Daily Maritime OPINTEL Summary
DMPC	Deployment Media Production Center Project
DMPI	Desired Mean Point of Impact
DMS	(1) Data Management System; (2) Defense Message System
DMSP	Defense Meteorological Satellite (or Support) Program
DMZ	Demilitarized Zone
DN	(1) Data Net; (2) Duplicate Negative; (3) Department of the Navy
DNA	(1) Defense Nuclear Agency; (2) Deoxyribonucleic Acid
DNAS	(1) DODIIS Network Access System; (2) Data Network Access System
DNC	(1) Director, Naval Communications; (2) Digital Nautical Chart
DNCC	Data Network Control Center
DND	Department of National Defence (Canada)
DNI	Director of Naval Intelligence
DNSIX	DODIIS Network Security for Information Exchange
DNVT	Digital Non-Secure Voice Terminal
DO	Director of Operations
DOA	(1) Department of the Army; (2) Date of Arrival; (3) Director of Administration; (4) Dead on Arrival
DOAT	JAC Counterterrorism/Counterintelligence Analysis Branch
DOB	(1) Depth of Burst; (2) Date of Birth; (3) Defense Order of Battle
DOC	Department of Commerce
DOCC	(1) Defense Communications Agency Operations Center Complex; (2) Deep Operations Coordination Cell; (3) DISA Operational Control Complex
DOCEX	(1) Document Exploitation; (2) Document Exploitation Center
DOCKLAMP	Defense Attache System Message Channel
DOCS	DSCS Operations Control System

Page 3332 of 3957

DoD, DOD	(1) Department of Defense; (2) Date of Death; (3) Date of Departure
DODCI	DoD Computer Institute
DODCSC	Department of Defense Computer Security Center
DODD	DoD Directive
DODEX	DoDIIS Extended
DODFCIP	DoD Foreign Counterintelligence Program
DODFDCO	Department of Defense Foreign Disclosure Coordinating Office
DODFIP	DoD Futures Intelligence Program
DODIIS	DoD Intelligence Information System
DODIIS SCINET	DoDIIS Sensitive Compartmented Information Network
DODIMS	DoD Intelligence Management System
DODIPP	DoD Intelligence Production Program
DODNACC	Department of Defense National Agency Check Center
DODSATCOM	DoD Satellite Communications Program
DOD SAT COM	DOD Satellite Communications
DODSI	Department of Defense Security Institute
DODSPECREP	DoD Special Representative
DOD TCSEC	DOD Trusted Computer System Evaluation Criteria
DOE	Department of Energy
DOF	Disposition of Forces
DOI	(1) Date of Information; (2) Duration of Illumination; (3) Director of Intelligence; (4) Imagery Division (JAC); (5) Director of Operations and Intelligence; (6) DSSCS Operating Instruction; (7) Date of Intercept
DOJ	Department of Justice
DOMS	Directorate of Military Support
DOMSAT	Domestic Satellite
DON	Department of the Navy
DOO	Daily Operations Order (NATO)
DOPS	DIA Outline Plotting System
DOS	(1) Department of State; (2) Date of Separation; (3) Disk Operating System; (4) Direct Operating System
DOSCOM	Division Support Command
DoSIP	Department of State Intelligence Program
DOSTN	Department of State Telecommunications Network
DOT	Department of Transportation
DP	(1) Duplicate Positive; (2) Development Program; (3) Displaced Person; (4) Delegated Production; (5) Directorate of Production; (6) Data Processing; (7) Decision Point; (8) Director of Personnel
DPAC	Defense Program Analysis Center
DPAE	Director, Program Analysis and Evaluation
DPAS	(1) Digital Patch and Access System; (2) Defense Priorities and Allocations System
DPC	Defense Planning Committee (NATO)
DPF	Digital Processing Facility

Page 3333 of 3957

DPG	Defense Planning Guidance
DPI	Desired Point of Impact
DPIC	(1) Decentralized Pacific Imagery Processing and Interpretation Center; (2) Defense Photographic Interpretation Center
DPICM	Dual-Purpose Improved Conventional Munitions
DPKO	Department of Peacekeeping Operations
DPL	Degausser Products List
DPM	Dissemination Program Manager
DPOB	Date, Place of Birth
DPOM	Directorate of Plans, Operations, and Mobilization
DPOMIS	Directorate of Plans, Operations, Mobilization, Intelligence, and Security
DPP	(1) Delegated Production Program; (2) Deliberate Planning Process; (3) Distributed Production Program
DPPC	Deployable Print Production Center
DPPDB	Digital Point Positioning Database
DPPG	Defense Policy and Planning Guidance
DPQ	Defense Planning Questionnaire (NATO)
DPRB	Defense Planning and Resources Board
DPRK	Democratic People's Republic of Korea
DPS	(1) Delegated Production System; (2) Data Processing Set; (3) Department of Public Safety
DPSK	Digital Pulse Shift Key
DR	(1) Director; (2) Dissemination Requirement; (3) Directorate of Resources; (4) Detection Radar
DRA	Defense Research Assessment
DRAM	Dynamic Random Access Memory
DRASH	Deployable Rapid Assembly Shelters
DRB	Defense Resources Board
DRC	(1) Defense Review Committee (NATO); (2) Defense Research Comment; (3) Data Reduction Center
DR&E	Defense Research and Engineering
DRIC	Defense Resource Identification Code
DRM	Defense Research Memorandum
DRO	Departmental Requirements Officer
DRP	Disaster Relief Program
DRS	(1) Data Relay Satellite; (2) DoD Imagery Requirements Structure; (3) Data Retrieval Subsystem; (4) Data Reconstruction System
DRSA	Defense Reconnaissance Support Activities
DRSEM	Deployable Receive Segment Engineering Model
DRSN	Defense Red Switch Network

Page 3334 of 3957

DRSP	(1) Defense Reconnaissance Support Program; (2) Defense Red Switched Program
DRU	Direct Reporting Unit
DRZ	Deep Reconnaissance Zone
DS	(1) Defense Suppression; (2) Direct Support
DS&T	Director of Science and Technology
DSA	(1) Defense Supply Agency; (2) Direct Service Activities (SIGINT); (3) Directed Search Area; (4) Division Support Area; (5) Defense Security Agency (ROK); (6) Digital Signature Algorithm
D&SA	Depth & Simultaneous Attack
DSAA	Defense Security Assistance Agency
D&SABL	Depth & Simultaneous Attack Battle Lab
DSARC	Defense Systems Acquisition Review Council
DSAT	(1) Developmental Submarine Analysis Terminal; (2) Defense Satellite
DSB	Defense Science Board
DSC	Defense Satellite Communications
DSCIS	Daily Space Command Intelligence Summary
DSCS	Defense Satellite Communications System
DSC-SLEP	Defense Satellite Communications System Service Life Enhancement Program
DSCSOC	Defense Satellite Communications System Operations Center
DSDIO	Director, Strategic Defense Initiative
DSE	(1) Direct Support Element; (2) Division Support Element
DSEC	Directorate of Security
DSFOB	Daily Strategic Forces Order of Battle
DSG	Defense Steering Group
DSI	Defense Simulation Internet
DSIATP	Defense Sensor Imagery Application Training Programs
DSIIB	Direct Support Imagery Interpretation Brief
DSIMS	Deployable SouthCom Intelligence Management System
DSI/TCCS	Defense Simulation Internet/Theater Command and Control System
DSM	Data Systems Modernization
DSN	(1) Defense Switched Network; (2) Deep Space Network
DSNET	Defense Integrated Secure Network
DSNET 1	Defense Integrated Secure Network 1 (SECRET level)
DSNET 2	Defense Integrated Secure Network 2 (TOP SECRET level)
DSNET 3	Defense Integrated Secure Network 3 (TS/SCI level)
DSO	Direct Support Operator/Operations
DSP	Defense Support Program
DSPO	Defense Special Projects Office
DSR	(1) Defense Source Register; (2) Data Service Request
DSRA	DODSPECREP-Alameda
DSRP	Defense Space Reconnaissance Program
DSRV	Deep Submergence Rescue Vehicle

Page 3335 of 3957

DSS	(1) Decision Support System; (2) Devices, Simulators and Simulations
DSSCC	Defense Special Security Communications Center
DSSCS	Defense Special Secure Communications System
DSSCS/DIN	Defense Special Security Communications System/Digital Intelligence Network
DSSR	Deep Space Surveillance Radar
DSSS	Defense Special Security System
DST	(1) Daylight Savings Time; (2) Decision Support Template; (3) Decision Support Tools; (4) Direct Support Team; (5) Digital Support Team
DSTE	Digital Subscriber Terminal Equipment
DSTF	Decision Support Task Force
DSTP	Director, Strategic Target Planning
DSTS	Deep Space Tracking System
DSU	(1) Direct Support Unit; (2) Disk Storage Unit; (3) Data Service Unit (DCTN)
DSV	Deep Submergence Vehicle
DSVT	(1) Digital Subscriber Voice Terminal; (2) Digital Secure Voice Terminal
DT	(1) Developmental Test; (2) Directorate for Science and Technology
DTA	Directorate of Threat Analysis
DTC	(1) Digital Tape Cassette; (2) Desktop Computer
DTC-2	Desktop Computer-2 (Navy)
DTD	Digital Terrain Data
DT&E	Developmental Test and Evaluation
DTE	Data Terminal Equipment
DTED	Digital Terrain Elevation Data
DTG	Date-Time Group
DTI	Doppler-Time-Intensity
DTIC	Defense Technical Information Center
DTIO	Deputy Target Intelligence Officer
DTIR	Defense Technical Intelligence Report
DTLOMS	Doctrine, Training, Leadership, Organization, Material, Soldiers
DTLS	Descriptive Top-Level Specification
DTM	(1) Data Transfer Module; (2) Digital Transfer Module; (3) Digital Target Materials
DTMF	Dual-Tone Multi-Frequency
DTNSRDC	David W. Taylor Naval Ship Research & Development Center
DTOC	Division Tactical Operations Center
DTOCSE	Division Tactical Operations Center Support Element
DTOLM	Doctrine, Training, Organization, Leader Development and Material
DTD	Data Transfer Device
DTP	Drug Testing Program

Page 3336 of 3957

DTS	(1) Diplomatic Telecommunications System/Service; (2) Data Transmission System; (3) Direct Transmission System; (4) Dedicated Transmission Service
DTSA	Defense Technology Security Administration
DTSG	Digital Technology Subworking Group
DTSS	Digital Topographic Support System
DTU	Data Transfer Unit
DTUC	Data Transfer Unit Cartridge
DUCA	Distributed Users Coverage Antennas
DUG	Deep Underground
DUPLEX	Simultaneous Transmit and Receive
DVO	Direct View Optics
DVM	Digital Voice Module
DVTC	Digital Voice Transmit Communications
D/TWP	Director, Tactical Warfare Programs
DTWS	Digital Topographic Work Station
DU	(1) Decision Unit; (2) Depleted Uranium
DUA	Directory User Agent
DUSD(AT)	Deputy Under Secretary of Defense (Advanced Technology)
DUSD(P)	Deputy Under Secretary of Defense (Policy)
DV	Distinguished Visitor
DVI	Digital Video Interactive
DVITS	Digital Video Imagery Transmission System
DVO	Defense Visit Offices
DWIO	Duty Watch Intelligence Officer (Canadian)
DWIP	Defense-Wide Intelligence Plan
DWS	Disaster Warning System
DWT	(1) Deadweight Ton; (2) Division Wing Team
DZ/LZ	Drop Zone/Landing Zone
DZ/LZ/RZ	Drop/Landing/Recovery Zone
DZS	Drop Zone Study

Page 3337 of 3957

E

e	Elipticity
E	Evaporites (soil type)
EA	(1) Emergency Action(s); (2) Electronic Attack; (3) Executive Agent
E&A	(1) Exploitation and Analysis; (2) Engineering and Administration
E3	(1) End-to-End Encryption; (2) Emergency and Extraordinary Expenses
EAC	(1) Emergency Action Console; (2) Echelons Above Corps
EACTPC	Echelon-Above-Corps Theater Production Center
EACIC	Echelon-Above-Corps Intelligence Center
EAD	(1) Echelon Above Division; (2) Earliest Arrival Date; (3) Extended Air Defense
EADSIM	Extended Air Defense Simulation
EAM	(1) Emergency Action Message; (2) Event Analysis Matrix
EAMA	African States Associated with the EEC
EAMAS	Emergency Action Message Authentication System
EAP	(1) Emergency Action Procedure; (2) Emergency Action Plan
EAS	Emergency Action System
EASTLANT	Eastern Atlantic Command (NATO)
EASTPAC	Eastern Pacific
EATTG	Enhanced Automated Tactical Target Graphics
EBS	Emergency Broadcast System
EC	(1) European Community; (2) Expenditure Center; (3) Electronic Combat
ECA	(1) Enemy Capability Assessment; (2) Earth Central Angle; (3) Enemy Courses of Action
ECAC	Electromagnetic Compatibility Analysis Center
ECB	Echelons Corps and Below
ECC	(1) Eurasian Communist Countries; (2) European Communist Countries; (3) European Community Commission
ECCM	Electronic Counter-Countermeasures
ECDB	EISS Consolidated Database
ECG	Emergency Coordination Group
ECI	External Communications Interface
ECM	(1) Electronic Countermeasures; (2) European Common Market
ECMA	European Computer Manufacturer’s Association
ECMC	Enhanced Crisis Management Capability
ECMO	European Collection Management Office
ECO	Electronic Collection Outstations
ECOA	Enemy Courses of Action
ECOWAS	Economic Community of West African States
ECP	(1) Emergency Communications Plan; (2) Entry Control Point
ECPL	Endorsed Data Encryption Standard Products List

Page 3338 of 3957

ECS	(1) Electronic Combat Support; (2) European Communications Satellite
ECSC	European Coal and Steel Community
ECSM	(1) Special Assistant for Security Matters; (2) Enhanced Capability Stand-Off Munition
ECSO	European Command Special Operations
ECU	Environmental Control Unit (GSM)
ED	(1) European Capability Datum; (2) EUCOM Directive
EDA	Emergency Dissemination Authority(ies)
E-DAY	Start Day of an Exercise
EDI	European Defense Initiative
EDL	Electric Discharge Laser
EDM	Engineering Development Model
EDMS	Electronic Dissemination Management System
EDN	Emergency Data Network
EDP	(1) Electronic Data Processing; (2) ELINT Data Processor
EDPSELINT	Data Processing System
E-DRB	Expanded Defense (Planning &) Resources Board
EDRE	Emergency Deployment Readiness Exercises
E&E	Escape and Evasion
EEA	Essential Elements of Analysis
EEC	(1) European Economic Community; (2) East European Countries; (3) Enhanced Explosives Charge
EECT	End of Evening Civil Twilight
EEFI	Essential Elements of Friendly Information
EEI	Essential Elements of Information
EELS	Early Entry Lethality and Survivability
EELV	Evolved Expendable Launch Vehicle
EENT	End Evening Nautical Twilight
EEO	Equal Employment Opportunity
EEOB	Enemy Electronic Order of Battle
EEOC	Equal Employment Opportunity Commission
EES	Emergency Evacuation Study
EFCS	Electronic Filmless Camera System
EFD	Electronic Fill Device
EFS	(1) Electronic Filing System; (2) Proper Name of System
EFTA	European Free Trade Association
EFTO	Encrypted for Transmission Only
EFVS	Electronic Fighting Vehicle System
EGA	Enhanced Graphics Adapter
EGADS	Electronic Generation, Accounting, and Distribution System
EGIS	East German Intelligence Service
EHF	Extremely High Frequency
EI	Effectiveness Index
EIA	Electronics Industry Association

Page 3339 of 3957

EIB	(1) European Investment Bank; (2) External Intelligence Bureau
EIC	Economic Intelligence Committee
EIDB	EISS Integrated Database
EIDS	Electronic Information Delivery System
EIF	(1) ECMC Interface Facility; (2) Enhanced Interface Facility
EIG	Explosive Incendiary Grenade
EIP	ELINT Improvement Program
EIRP	Effective Isotropic Radiated Power
EIS	Enhanced Imagery System
EISI	(1) Electrical Interface-SWPS/IDHS 2000; (2) Electrical IDHS-90/SWPS Interface
EISS	EUCOM Intelligence Support System
EITO	EUCOM Intelligence Training Office EKIP Enhanced Korean Information Package
EKMS	Electronic Key Management System
ELDO	(1) European Space Vehicle Launcher Development Organization; (2) European Launcher Development Organization
ELECTRO-OPINT	Electro-Optical Intelligence Element
ELECTRO-OPTINT	Electro-Optical Intelligence
ELEV	Elevation
ELF	Extremely Low Frequency
ELI	Emitter Location & Identification
Elm	Element
ELMT	Element
ELINT	Electronic Intelligence
ELISA	Electronic Intelligence Search & Analysis
ELNET	European Liaison Network
ELNOT	ELINT Notation
ELOS	Extended Line of Sight
ELS	Emitter Location System
ELSEC	Electronic Security
ELSET	(1) Element Set; (2) Proper Name of System
ELT	(1) Emergency Locator Transmitter; (2) Electronic Light Table
ELT 3000	Electronic Light Table for UNIX-based system
ELV	Expendable Launch Vehicle
EM	(1) Electromagnetic; (2) Enlisted Member; (3) Environmental Monitoring
E-Mail	Electronic Mail
EMA	European Monetary Agreement
EMAP	Electromagnetic Analysis Program
EMATS	Emergency Message Automatic Transmission System
EMC	Electromagnetic Compatibility
EMCS	ELINT Mission Control System
EMCON	Emission Control
EMCP	Electromagnetic Compatibility Program

Page 3340 of 3957

EMD	Engineering and Manufacturing Development
E&MD	Engineering and Manufacturing Development
EMGTN	Equivalent Megatonnage
EMHS	EUCOM Message Handling System
EMI	Electromagnetic Interference
EMIDS	Experiment for Management Information Data Systems
EMINT	Emissions Intelligence
E-MIPE	Enhanced MIPE
EMIS	Early Mission Identification System
EMIT	Emergency Message Initiation Terminal
EMP	Electromagnetic Pulse
EMR	Electromagnetic Reconnaissance
EMSEC	Emanations/Emissions Security
EMT	(1) Emergency Management Team; (2) Equivalent Megatonnage
EMTR	Eastern Missile Test Range
EMUT	Enhanced Manpack UHF Terminal
En	Enemy
ENDEX	End Date of an Exercise
E-NET	Ethernet
Engr	Engineer
ENL	Enlisted
ENMCC	Expanded National Military Command Center
ENSCD	Enemy Situation and Correlation Division
ENSCE	Enemy Situation Correlation Element
ENSIT	Enemy Situation
ENTNAC	Entrance National Agency Check
EO	(1) Electro-Optical; (2) Executive Order; (3) Escape Orbit; (4) End Office
EOA	Early Operational Assessment
EOB	(1) Electronic Order of Battle; (2) Executive Office Building; (3) Enemy Order of Battle
EOBS	Electronic Order of Battle Server
EOC	Emergency Operations Center
EOD	(1) Explosive Ordnance Disposal; (2) Erasable Optical Disks
EOINT	Electro-Optical Intelligence
EOP	Emergency Operating Procedures
E-OPTINT	Electro-Optical Intelligence
EORSAT	ELINT Ocean Reconnaissance Satellite
EOS	Earth Observation Satellite
EOSAT	Earth Observation Satellite
EOSS	Electro-Optic Sensor System
EOTDA	Electro-Optical Tactical Decision Aids
EOW	Electro-Optic Warfare
EP	(1) ELINT Processor; (2) Electronic Protection
EP-3	U.S. Navy Reconnaissance Aircraft

Page 3341 of 3957

EPA	(1) Environmental Protection Agency; (2) Evasion Plan of Action
EPAC	Eastern Pacific
EPAMS	Exercise Planning and Message System
EPAT	Earliest Possible Arrival Time
EPDS	(1) Electronic Processing and Dissemination System; (2) ELINT Processing and Dissemination System
EPF	Exploitation Products File
EPIC	El Paso Intelligence Center
EPIRB	Emergency Position-Indicating Radio Beacon
EPL	(1) ELINT Parameters List; (2) Evaluated Products List
EPLRS	Enhanced Position Location and Reporting System
EPMO	European Production Management Office
EPR	(1) Extended Planning Annex; (2) Enlisted Performance Report
EPROM	Erasable Programmable Read-Only Memory
EPS	(1) ELINT Processing System; (2) Electronic Publication System; (3) Exploitation Problem Set; (4) Encapsulated Postscript
EPW	(1) Earth Penetrator Weapon; (2) Enemy Prisoner of War
EPWG	Exploitation Plans Working Group
EPUU	Enhanced PLRS User Units
EQV	Equivalent
ER	(1) Enhanced Radiation; (2) Electronic Reconnaissance; (3) Eastern Region; (4) EAGLE REACH
ERA	(1) Extended Range Ammunition; (2) Equal Rights Amendment
ERADCOM	Electronic Research and Development Command
ERAST	Environmental Research Aircraft and Sensor Technology
ERBM	Extended Range Ballistic Missile
ERCS	Emergency Rocket Communications System
ERADCOM	Electronic Research and Development Command
ERDAS	Earth Resources Data Analysis System
ERF	Early Reinforcing Force
ERIN	Electronic Radio Intercept Network (USCS)
ERINT	Extended Range Intercept Missile
ERIR	Electronic Reconnaissance Intercept Report
ERIS	Exo-atmospheric Reentry Vehicle Interception System
EROS	Earth Resources Observational System
ERP	Effective Radiated Power
ERPHO	Earth Resources Photographic Satellite
ERRS	Emergency Regional Reporting System
ERS	(1) Emergency Relocation Site; (2) Earth Resources Satellite
ERSSO	Emergency Reaction Special Security Officer
ERT	Executive Reference Time
ERTM	Electronic Intelligence Request Tasking Message
ERTS	Earth Resources Technology Satellite
ERTZ	Equipment Radiation TEMPEST Zone
ERW	Enhanced Radiation Weapon

Page 3342 of 3957

ES	(1) Emplacement Site; (2) Exploitation Support; (3) Electronic Warfare Support; (4) Expert System; (5) Electronic Support
ESA	(1) European Space Agency; (2) Electronically Steered Antenna
ESAA	European Special Activities Area (U.S. Air Force)
ESAC	El Salvador Analysis Cell
ESAF	European Special Activities Facility
ESAMS	Enhanced Surface-to-Air Missile Simulation
ESAR	Enhanced Synthetic Aperture Radar
ESC	Electronic Security Command (U.S. Air Force)
ESD	(1) Electronic Systems Division; (2) Ephemeris Support Data; (3) Exploitation Support Section (JSIPS)
ESF	(1) Environmental Scale Factor; (2) Extended Superframe Formatted
ESG	(1) Electronic Security Group; (2) Exploitation Steering Group
ESI	Extremely Sensitive Information
ESIAC	Electronic Satellite Image Analysis Center
ESJ	Escort Jamming
ESM	(1) Electronic Warfare Support Measures: (2) Electronic Support Measures; (3) Electronic Security Measures
ESMC	Eastern Space and Missile Center
ESMT	External Supply Management Tools
ESP	Emergency Special Measures
ESR	ELINT Summary Report
ESRO	European Space Research Organization
ESS	(1) Electronic Security Squadron; (2) ELINT Support System; (3) Exploitation Support Segment; (4) Exercise Support Sub-system; (5) Electronic Switching System; (6) Exploitation Support Section (JSIPS)
ESSA	(1) Expert System for Situation Assessment; (2) Environmental Satellite Service Administration
ESSM	Electronic Shop, Shelter-Mounted
Est	Estimated
ESV	Earth Satellite Vehicle
ESW	Electronic Security Wing
ET	(1) Enhanced Terminal; (2) Earth Terminal; (3) Embedded Training
ETA	(1) Estimated Time of Arrival; (2) Equivalent Target Area
ETAC	Enlisted Terminal Attack Controllers
ETAP	Education Training Awareness Program
ETAWG	ELINT Technical Analysis Working Group
ETC	(1) Estimated Time of Completion; (2) Et Cetera
ETD	(1) Estimated Time of Departure; (2) Effective Transfer Date
ETDS	Elapsed Time Distribution System
ETF	Enhanced Tactical Fighter
ETHICS	European Theater High Capacity Intelligence Communications System
ETI	Estimated Time of Impact

Page 3343 of 3957

ETIBS	Enhanced Tactical Information Broadcast Service
ETII	External-to-Internal Interface
ETIWCS	European Theater Intelligence Warning and Communications System
ETL	(1) Endorsed Tools List; (2) Engineer Topographic Laboratories
ETO	(1) European Theater of Operations; (2) Earth-To-Orbit
ETP	(1) Extended Tether Program; (2) Enhanced Thermal Protection
ETPL	Endorsed TEMPEST Products List
ETR	(1) Estimated Time of Return; (2) Eastern Test Range
ETRAC	Enhanced Tactical Radar Correlator
ETRO	Estimated Time Return to Operation
ETS	(1) European Telephone System; (2) Estimated Time of Separation; (3) Expiration of Term of Service; (4) Earth Technology Satellite; (5) Engineer Test Satellite
ETSC	Electronic and Telecommunications Subcommittee
ETSS	Electronic Telecommunications Switching System
ETTP	EUCOM Tactics, Techniques and Procedures
ETUT	Enhanced Tactical User Terminal
EU	Expenditure Unit
EUCI	Endorsed for Unclassified Cryptographic Information
EUCOM	U.S. European Command
EUCOM/JIC	(1) U.S. European Command/Joint Intelligence Command; (2) EUCOM Joint Intelligence Center
EUDAC	European Defense Analysis Center
EUF	ECME User Facility
EUL	Economically Useful Life
EUMETSAT	European Meteorological Satellite (Organization)
EURATOM	European Atomic Energy Community
EUSA	Eighth U.S. Army (Korea)
EUSC	Effective United States Controlled
EUTE	Early User Test & Evaluation
EUTELSAT	European Telecommunications Satellite (Organization)
EUV	Extreme Ultraviolet
EUVE	Extreme Ultraviolet Explorer
EV	Enforcement Vector
EVA	Extra-Vehicular Activity
EVC	DoD Evasion Chart
EVO	Event Verification Officer
EVR	Enemy Vulnerability Report
EVS	Electronic Visual Communications
EW	(1) Electronic Warfare; (2) Early Warning
EW/GCI	Early Warning/Ground Control Intercept
EWAC	Electronic Warfare Anechoic Chamber
EWAS	Electronic Workorder Accounting System

Page 3344 of 3957

EWC	(1) Electronic Warfare Center; (2) Electronic Warfare Coordinator
EWCC	Electronic Warfare Coordination Center
EWCM	Electronic Warfare Coordination Module
EWCS	Electronic Warfare Control System
EWIR	Electronic Warfare Integrated Reprogramming
EWIRS	Electronic Warfare Integrated Reprogramming System
EWMIS	Electronic Warfare Management Information System
EWMS	EW Mission Summary
EWO	(1) Electronic Warfare Officer; (2) Emergency War Order
EWOPFAC	Electronic Warfare Operating Facility
EWR	(1) Early Warning Radar; (2) Electronic Warfare Reprogramming
EWRL	Electronic Warfare Reprogrammable Library
EWS	Electronic Warfare Support
EWSE	EW Support Element
EWSM	Electronic Warfare Support Measures
EWSO	EW Staff Officer
EXCRIT	Exercise Critique System
EXDEF	Exercise Deficiency Program
EXCAP	Exercise Capability (simulator)
EXCOM	Community Executive Committee
ExDir/ICA	Executive Director for Intelligence Community Affairs
EXDIS	Exclusive Distribution (Pneumatic Tube Message Precedence)
EXEC	Executive
EXERTAS	Exercise Timeline Analysis System
EXFIL	Exfiltration
EXO	Exoatmosheric
EXOPLAN	Exercise Operations Plan
EXPER	Experience
EXPL	Exploitation
EXPLAN	Exercise Plan
ExPReS	Expoitation Process Reengineering Study
EXRAND	Exploitation Research and Development (COMIREX)
EXSCEN	Exercise Scenario System
EXSUBCOM	Exploitation Subcommittee (COMIREX)
EXSUM	Executive Summary
EXTAC	Experimental Tactics

F

F	(1) Fahrenheit; (2) Frequency
FA	(1) Frontal Aviation (FSU); (2) Field Artillery; (3) Forward Area; (4) Functional Architecture; (5) Frequency Agile; (6) Full Accounting; (7) Feasibility Assessment
FAA	(1) Federal Aviation Agency; (2) Federal Aviation Administration; (3) Foreign Assistance Act
FAAD C3I	Forward Area Air Defense Command, Control, Communications and Intelligence
FAADS	Forward Area Air Defense System
FAAR	Forward Area Alerting Radar
FAARP	Forward Area Armament and Refuel Point
FAAS	Foreign Affairs Administrative Support
FAC	(1) Forward Air Control (Controller); (2) Facilities
FACP	(1) Forward Air Control Post; (2) Forward Air Control Party
FACSFAC	Fleet Air Control and Surveillance Facility
FAD	(1) Fleet Air Defense; (2) Force Activity Designator; (3) Field Arbitrary Designators
FADOC	Future Air Defense Operation Concept
FADS	Foreign Area Data System
FAE	Fuel Air Explosive
FAF	Fast Access Format
FAFIC	Federal Armed Forces Intelligence Center (FRG)
FAI	Fuel Air Incendiary Concussion Bomb
FAIO	Field Artillery Intelligence Officer
FAISA	FORSCOM Automated Intelligence Support Activity
FAISS	FORSCOM Automated Intelligence Support System
FALD	Field Administration and Logistics Division
FAM	Functional Area Model
FAME	FORSCOM Automated Modernization Effort
FAMP	Foreign Army Materiel Production
FAMS	Fleet Ocean Surveillance Information Center Analytical Maritime Summary
FAMSIM	Family of Simulation
FANS	Friendly Allied Nation Support Network
FANT	French Atmospheric Nuclear Test
FAO	(1) Foreign Area Officer; (2) Forward Area of Operations; (3) Food and Agricultural Organization (UN)
FAPC	Food and Agriculture Planning Committee (NATO)
FARP	Forward Area Refuel Point
FARRFAA	Air Replacement Radar
FARRP	Forward Area Rearming and Refueling Point
FAS	(1) (U.S.) Foreign Agriculture Service; (2) Frequency Assignment Subcommittee
FAST	(1) Fleet Antiterrorist Support Teams; (2) Forward Area Support Team; (3) Forward Area Support Terminal
FAST-I	Forward Area SID and TRAP-Improved

Page 3346 of 3957

FAST/I2	Improved FAST/I
FASTC	Foreign Aerospace Science and Technology Center (archaic, now NAIC)
FASTFAX	Tactical Digital Facsimile
FASTL	Future Analytic Strategic Target List
FAV	(1) Field Assistance Visit; (2) Fast Attack Vehicle
FAX	Facsimile
FB	Fighter Bomber
FBA	Fighter Bomber Attack
FBH	Force Beachhead
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FBM	Fleet Ballistic Missile
FBR	Fast Breeder Reactor
FBS	(1) Forward-Based Systems; (2) Federal Border Service
FC	(1) Fire Control; (2) Fractional Coverage
FCA	Foreign Counterintelligence Activity
FCB	Functional Control Board
FCC	(1) Fleet Command Center; (2) Federal Communications Commission; (3) Fighter Control Center; (4) Fire Coordination Center
FCE	Forward Control Element
FCFS	First Come, First Served
FCG	Foreign Clearance Guide (military)
FCG2	FORSCOM G2
FCI	Foreign Counterintelligence
FCIAD	FORSCOM Component Intelligence Architecture Document
FCIP	Foreign Counterintelligence Program
FCISD	FORSCOM Component Intelligence Strategy Document
FCITP	Foreign Counterintelligence and International Terrorism Program (FBI)
FCITTP	FORSCOM Component Intelligence Tactics, Techniques and Procedures
FCLP	FORSCOM Command Language Program
FCO	Facility Control Office
FCRC	Federal Contract Research Center
FCS	(1) Fire Control System; (2) Flight Control System; (3) (U.S.) Foreign Commercial Service
FCSE	Forward Control Support Element
FCT	Foreign Comparative Test
FCZ	Forward Combat Zone
FD	Functional Design
F/d	Ratio of focal-length to diameter (of reflector type antennas)
FDB	Fleet Database
FDBM	Functional Data Base Manager
FDBPS	Fleet Data Base Production System

Page 3347 of 3957

FDC	Fire Direction Center
FDDAC	Foreign Denial and Deception Analysis Committee
FDDI	Fiber Distributed Data Interface
FDDS	Flag Data Display System
FDIU	Fill Device Interface Unit
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FDO	Foreign Disclosure Officer
FDOA	Frequency Difference of Arrival
FDR	Foreign Disclosure Representative
FDT&E	Force Development Test & Experimentation
FDU	Force Design Update
FDW	Forward Deployed Workstation
FDX	Full Duplex
FEA	Front End Analysis
FEAF	Far Eastern Air Forces
FEBA	Forward Edge of the Battle Area
Fed	Federal Reserve System
FEDS	Front End Distribution System
FEDSIM	Federal Computer Performance Evaluation and Simulation Center
FEL	Free Electron Laser
FEMA	Federal Emergency Management Agency
FEMD	Far East Military District
FEMP	Front End Message Processors
FEP	(1) Front End Processor; (2) FLTSATCOM EHF Package
FERS	Federal Employees Retirement System
FET	Field Effect Transistor
FETVD	Far East Theater of Military Operations
FEWS	Future Early Warning System
FEWSG	Fleet Electronic Warfare Support Group
FF	Frigate
FFA	Free-Fire Area
FFAR	Folding-Fin Aerial Rocket
FFED	FIREFINDER Elevation Data
FFG	Guided-Missile Frigate
FFGH	Guided-Missile Aviation Frigate
FFGN	Nuclear-Powered Guided-Missile Frigate
FFH	Aviation Frigate
FFHGN	Nuclear-Powered Guided-Missile Aviation Frigate
FFHN	Nuclear-Powered Aviation Frigate
FFL	Corvette
FFLG	Guided-Missile Corvette
FFM	Full Face Mask
FFN	Fleet Flash Net

Page 3348 of 3957

FFR	Radar Picket Frigate
FFS	(1) Fixed Field Site; (2) Formatted File System
FFT	Training Frigate
FGHQ	Fighter Group Headquarters (Canada)
FGN	Foreign
FH	Frequency Hopping
FH/DS	Frequency Hopping/Direct Sequence
FI	(1) Finished Intelligence; (2) Foreign Intelligence
FI&SS	Foreign Intelligence and Security Service(s)
FIA	Foreign Intelligence Agency
FIC	(1) Fleet Intelligence Center; (2) FORSCOM Intelligence Center
FICEURLANT	Fleet Intelligence Center, Europe and Atlantic
FICM	Fleet Intelligence Collection Manual
FICPAC	Fleet Intelligence Center, Pacific
FID	(1) Foreign Internal Defense; (2) Force Integration Division
FIDB	Fundamental Intelligence Database
FIE	Foreign Intelligence Element
FIG	Figure
FIIC	Force Imagery Interpretation Center
FIIU	Force Imagery Interpretation Unit
FIM	Force Integration Master Planner
FIN	(1) Fixed-Site Intelligence Network; (2) Financial
FINPLAN	Financial Plan
FIO	Foreign Intelligence Officer
FIP	(1) Force Improvement Plan; (2) Federal Information Processing
FIPC	Foreign Intelligence Priorities Committee
FIPS	(1) Federal Information Processing Standard; (2) Fleet Intelligence Production System
FIR	Field Investigative Region
FIRCAP	Foreign Intelligence Requirement Capabilities and Priorities
FIRE	Fused Intelligence Report in Europe
FIRF	Future Information Requirements Forecast
FIRMS	Foreign Intelligence Relations Management System
FIROPS	Freedom of Air Operations
FIRST	Fleet Intelligence Reserve Support Team
FIRSTEURLANT	Fleet Intelligence Reserve Support Team, Atlantic
FIRSTPAC	Fleet Intelligence Reserve Support Team, Pacific
FIS	(1) Foreign Instrumentation Signals; (2) Foreign Intelligence Service
FISA	Foreign Intelligence Surveillance Act
FISAP	FMFPac Intelligence Sub-Architecture Plan
FISINT	(1) Foreign Instrumentation and Signature Intelligence; (2) Foreign Instrumentation Signals Intelligence
FISS	Foreign Intelligence and Security Services
FIST	(1) Fleet Imagery Support Terminal; (2) Fire Support Team

Page 3349 of 3957

FIST-T	Transportable FIST
FITCPAC	Fleet Intelligence Training Center, Pacific
FITD	FORSCOM Intelligence Training Detachment
FITWING	Fighter Wing
FLA	Foreign Launch Assessment
FLAGE	Flexible Lightweight Agile Guided Experiment
FLC	Foreign Language Committee
FLEETSATCOM	Fleet Satellite Communications
FLENUMOCEANCEN	Fleet Numerical Oceanography Center (U.S. Navy)
FLEX	Force-Level Execution System
FLI	Force-Level Information
FLIR	Forward-Looking Infrared (Radar)
FLO	Foreign Liaison Office
FLOT	Forward Line of Troops
FLR	Forward-Looking Radar
FLRA	Federal Labor Relations Authority
FLSG	Force Logistics Support Group
FLT	Fleet; Flight
FLTBCST	Fleet Broadcast
FLTCINC	Fleet Commander in Chief
FLTSAT	Fleet Satellite
FLTSATCOM	Fleet Satellite Communications System
FLTSEVOCOM	Fleet Secure Voice
FM	(1) Frequency Modulation; (2) Foreign Materiel; (3) File Maintenance; (4) Factory Marking(s); (5) Functional Manager; (6) Field Manual; (7) From; (8) Comptroller
FMA	(1) Foreign Materiel Acquisition; (2) Foreign Media Analysis
FMAO	Foreign Materiel Acquisition Operation
FMAR	Foreign Materiel Acquisition Requirement
FMAS	Foreign Media Analysis Subsystem
FMC	(1) Field Maintenance Center; (2) Force Mobile Command
FME	Foreign Materiel Exploitation
FMEC	Foreign Materiel Exploitation Catalogue
FMEP	Foreign Materiel Exploitation Program
FMF	Fleet Marine Force(s)
FMFLANT	Fleet Marine Force, Atlantic
FMFM	Fleet Marine Field Manual
FMFPAC	Fleet Marine Force, Pacific
FMIB	Foreign Materiel Intelligence Board
FMIG	Foreign Materiel Intelligence Group
FMIS	Force Management Information System
FMLM	French Military Liaison Mission
FMOCC	Fleet Mobile Operations Command Center
FMP	Foreign Materiel Program
FMPCP	Foreign Military Personnel Contact Program

Page 3350 of 3957

FMPRB	Foreign Military Program Review Board
FMRL	Foreign Materiel Requirements List
FMs	Defense Intelligence Functional Managers
FMS	Foreign Military Sales
FMSF	Foreign Military Sales Financing
FMTV	Family of Medium Tactical Vehicles
FN	Foreign National
FNOC	Fleet Numerical Oceanographic Center
FNU	First Name Unknown
FO	Forward Observer
F/O	Fiber-Optics
FOA	(1) Field Operating Agency; (2) Forward Operating Area
FOAMP	Foreign Aerospace Materiel Production
FOAP	Foreign Aircraft Production
FOB	(1) Forward Operating Base; (2) Foreign Order of Battle
FOBS	Fractional Orbital Bombardment System
FOC	(1) Final Operational Capabilities; (2) Full Operational Capability; (3) FORSCOM Operations Center; (4) Full Operating Capacity
FOCI	Foreign Owned, Controlled or Influenced
FOCUS	(1) Interagency Review of Defense Attache Offices; (2) FORSCOM Objective Communications System
FOD	Foreign Object Damage
FOFA	Follow-on Forces Attack
FofF	Field of Fire
FOG	Fiber-Optics Guided
FOGM	Fiber-Optic Guided Missile
FOI	Freedom of Information
FOIA	Freedom of Information Act
FOL	(1) Forward Operating Location; (2) Family of Loudspeakers
FOLAN	Fiber-Optic Local Area Network
FOLPEN	Foliage-Penetrating
FOM	Figure of Merit
FOMA	Foreign Military Assistance
FOMCAT	Foreign Materiel Catalogue
FOMP	Foreign Missile Production
FONS	Fleet Operational Needs Statement for Intelligence
FOP	Forward Observation Post
FORDTIS	Foreign Disclosure Technical Information System
FORECON	Force Reconnaissance
FORGE	Force Generation
FORMAT	Foreign Materiel
FORMDEPS	FORSCOM Mobilization and Deployment Planning System
FORMICA	Foreign Military Intelligence Collection Activity
FORMMS	Foreign Materiel Management System

Page 3351 of 3957

FORSCOM	U.S. Forces Command
FORSTAT	Force Status and Identity Report
FORT	Force Trends Data Base
FORTRAN	Formula Translator
FOSCAS	Foreign Ship Construction and Shipyards
FOSD	Family of Sabotage Devices
FOSIC	Fleet Ocean Surveillance Information Center
FOSIC-E	Fleet Ocean Surveillance Information Center, Europe
FOSICLANT	Fleet Ocean Surveillance Intelligence Center, Atlantic
FOSICPAC	Fleet Ocean Surveillance Information Center, Pacific
FOSIF	Fleet Ocean Surveillance Information Facility
FOSIF Rota	Fleet Ocean Surveillance Information Facility, Rota
FOSIF/WESTPAC	Fleet Ocean Surveillance Information Facility, Western Pacific
FOTARS	Follow-On Tactical Reconnaissance System
FOT&E	Follow-On Test and Evaluation
FOTELSYS	Foreign Telecommunications Systems
FOTRS	Follow-On Tactical Reconnaissance System
FOUO	For Official Use Only
FOV	Field of View
FP	(1) Fire Position; (2) Field Post; (3) Force Package
FPA	(1) Federal Preparedness Agency; (2) Focal Plane Array; (3) Force Projection Army
FPB	Fast Patrol Boat
FPE	Force Planning Estimate
FPF	Final Protection Fire
FPI	(1) Foreign Positive Intelligence; (2) Federal Process Improvement
FPIR	Force Protection Information Report
FPL	Fire Protective Line
FPN	Field Post Number
FPO	Fleet Post Office
fps	Feet Per Second
FPTOC	Force Projection Tactical Operations Center
FPU	Floating Point Unit
FQ&P	Flying Qualities and Performance
FRAG	Fragmentary Order
FRAGO	Fragmentary Order
FRD	(1) Federal Research Division (Library of Congress); (2) Formerly Restricted Data; (3) Functional Requirements Document
FREQ	Frequency
FRG	Federal Republic of Germany
FRIES	Fast Rope Insertion Extraction System
FRIF	Finished Recurring Intelligence File
FROG	Free Rocket Over Ground
FROKA	First Republic of Korea Army

Page 3352 of 3957

FROSS	Foreign Reliance on Space Systems
FRPG	Facility Reference Point Graphic
FRR	Frequency Resource Records
FRS	(1) Fleet Readiness Squadron; (2) Federal Research Service; (3) Forward Recording Site
FRY	Former Republic of Yugoslavia
FRYM	Former Republic of Yugoslavia-Macedonia
FS	(1) File Server; (2) Fire Support
F3S	Field Station Support System
FSAIS	FICEURLANT SCI Analyst Information System
FSB	(1) Fleet Satellite Broadcast (of FLTSATCOM); (2) Forward Staging Base; (3) Fire Support Base
FSBS	Fleet Submarine Broadcast System
FSCC	Fire Support Coordination Center
FSCL	Fire Support Coordination Line
FSCOORD	Fire Support Coordinator
FSD	(1) Field Support Division; (2) Forward Support Detachment
FSE	Fire Support Element
FSHB	Fallout Safe Height of Burst
FSI	Foreign Service Institute
FSIC	Forward Sensor Interface and Control
FSK	(1) Field Station, Korea; (2) Frequency Shift Keying
FSM	Federated States of Micronesia
FSO	(1) Foreign Service Officer; (2) Fire Support Officer
FSOC	Fairchild Satellite Operations Center
FSOF	Forward Special Operations Facility
FSP	Fire Support Plan
FSRS	Functional Security Requirements Specification
FSS	(1) Fast Sealift Ship; (2) FAISS SID System; (3) Fixed Satellite Services
FSSG	Force Service Support Group (USMC)
FSST	Forward Space Support in Theater
FST	(1) Future Strategic Targets; (2) Future Soviet Tank
FSTC	Foreign Science and Technology Center (archaic; now NGIC)
FSTS	Federal Security Telephone Service
FSU	Former Soviet Union
FSV	Fire Support Vehicle
FSVS	Future Secure Voice System
FSWDS	Fixed-Site Warning & Detection System
FT	(1) Fort; (2) Foot
FT-1	Fractional T-1
FTA	(1) Field Training Area; (2) Functions, Tasks, and Activities
FTAM	File Transfer Access Management
FTC	(1) Fast Time Constant (ECCM); (2) Federal Trade Commission
FTD	Foreign Technology Division (USAF)

Page 3353 of 3957

FTDB	Foreign Technology Data Base
FTI	Fixed Target Indicator
FTL	Future Target List
FTLS	(1) Future Target List-Strategic; (2) Formal Top-Level Specification
FTM	Full-Time Manning
FTP	File Transfer Protocol
FTPS	FORSCOM Topographic Production System (Facility)
FTR	Fighter
FTS	(1) Fleet Telecommunications System; (2) Federal Telecommunications System; (3) Federal Telephone System; (4) Flight Training Squadron
FTS 2000	Federal Telephone System 2000
FTSC	Fleet Technical Support Center
FTU	Forecast Tactical Unit
FTX	Field Training Exercise
FU	Forecast Unit
FUD	Full Unit Designator
FUE	First Unit Equipped
FUNT	French Underground Nuclear Test
FUSS	Fleet Undersea Surveillance System
FUWOB	Forward Unconventional Warfare Operations Base
FV	Fighting Vehicle
FVS	Foreign Visits System
FW	(1) Fighter Wing; (2) Fixed-Wing
FWAIS	Free-World Air Intelligence Study
FWAOB	Free-World Air Order of Battle
Fwd	Forward
FWE	Foreign Weapons Evaluation
FWIC	Fighter Weapon School Intelligence Course
FWVP	Fallout Wind Vector Plot
FY	Fiscal Year
FYDP	(1) Fiscal Year Defense Program/Plan; (2) Five-Year Defense Program; (3) Future Years Defense Program
FYI	For Your Information
FYIP	Five-Year Intelligence Plan
FYMOP	Five-Year Master Objectives Plan
FYP	Five-Year Plan (FSU)
FYROM	Federal Yugoslav Republic of Macedonia

Page 3354 of 3957

G

G	Gain
G1	Assistant Chief of Staff, G1 (Personnel)
G2 or G-2	(1) Assistant Chief of Staff, G2 (Intelligence); (2) Army or Ground Directorate of Intelligence; (3) General Corps Staff Intelligence Officer
G3	Assistant Chief of Staff, G3 (Operations and Plans)
G4	Assistant Chief of Staff, G4 (Logistics)
G5	Assistant Chief of Staff, G5 (Civil Affairs)
G6	Director(ate) of C4
G8	Director(ate) of Resource Management
GA	Ground Attack
GaAs	Gallium Arsenide
GACC	Ground Attack Coordination Center
GAD	Guards Artillery Division
GADT	Ground/Air Defense Threat
GAF	Ground Alert Facility (of PAC ABNCP)
GAFIA	German Armed Forces Intelligence Agency
GALE	Generic Area Limitation Environment
GALS	FSU Satellite (“Horizon”)
GAMO	Ground and Amphibious Military Operations
GAO	General Accounting Office
GAS	(1) Gray Area Systems; (2) Getaway Special
GAT	(1) Government Acceptance Test; (2) Guidance, Apportionment, and Targeting
GATT	General Agreement on Tariffs and Trade (UN)
GB	(1) Gigabyte; (2) Guardband
GBCS(-L or -H)	Ground-Based Common Sensor (-Light or -Heavy)
GBI	Ground-Based Interceptor
GBL	Ground-Based Laser
GBMD	Global Ballistic Missile Defense
GBR	Ground-Based Radar
GBS	Global Broadcast System
GBU	Guided Bomb Unit
GC	Gun Camera
GCA	Ground Controlled Approach
GCC	(1) Government Control Center; (2) Ground Component Commander; (3) Gulf Cooperation Council; (4) Global Control Center
GCCS	(1) Ground Command and Control System; (2) Global Command and Control System
GCDCAL	Great Circle Distance Calculator
GCE	Ground Combat Element
GCI	Ground-Controlled Intercept
GCN	Ground Communications Network
GCNTTY	Ground Communications Network Teletype

Page 3355 of 3957

GCP	Ground-Controlled Processor
GCP-E	Ground-Controlled Processor-ELINT
GCS	(1) Graphics Compatibility System; (2) Ground Control Station; (3) Global Connectivity Services; (4) Global Communications System
GCSS	Global Combat Support System
GDA	Gimbaled Dish Antenna
GDBI	Generic Data Base Interface
GDBMS	Generic Data Base Management Server
GDIC	General Defense Intelligence Community
GDIP	General Defense Intelligence Program
GDIPP	General Defense Intelligence Proposed Program
GDL	Gas Dynamic Laser
GDOP	Geometric Dilution of Precision
GDP	(1) General Defense Plan; (2) Gross Defense Product; (3) Ground Defense Position; (4) Gross Domestic Product
GDPS	Ground Data Processing System
GDRS	Ground Data Reduction System
GDS	(1) General Declassification Schedule; (2) FSU Guards; (3) Group Decision Support
GDSS	Global Decision Support System
GDT	Ground Data Terminal
Gen	General
GEM	Ground Effects Machine
GEN	(1) Generation; (2) General
GENIC	German National Intelligence Cell (NATO)
GENREP	General Reports
GENSER	General Service (Communications)
GEO	Geosynchronous Earth Orbit
GEODIS	Geographic Display
GEODSS	Ground-Based Electro-Optical Deep-Space Surveillance System
GEOFILE	(1) Geographic Locations Code File System; (2) Geolocation File (JOPES)
GEOREF	Global Reference System, a worldwide position reference system that may be applied to any map or chart graduated in latitude and longitude regardless of projection.
GEOSAT	Geological Satellite
GEP	Ground Entry Point
GEPS	Generic Electronic Publishing System
GES	Ground Entry Station
GFAC	Ground Forward Air Controller
GFCP	Generic Front-End Communications Package
GFE	Government Furnished Equipment
GFTD	Global Force Trends Data Base
GFR	Gap Filler Radar
GGI&S	Global Geospatial and Information Services
GHz	Gigahertz

Page 3356 of 3957

GIGSTER	NSA Video Teleconferencing System
GIIPS	Geographic Installation Intelligence Production Specifications
GIITS	General Intelligence Imagery Training System
GIN	Greenland-Iceland-Norway
GIPD	(1) General Intelligence Production Detachment; (2) General Intelligence Production Division
GIPMIS	General Intelligence Production Management Information System
GIPS	Geographic Installation Intelligence Production Specifications
GIPSY	Graphics Information or Presentation System
GIS	Geographical Information System
GIST	Graphical Intelligence Support Terminal
GITAC	General Intelligence Training Advisory Committee
GITC	General Intelligence Training Center
GITS	General Intelligence Training System
GIUK	Greenland-Iceland-United Kingdom
GKNT	State Committee for Science and Technology (FSU)
GKS	Graphics Kernel System
GL	Grenade Launcher
GLCM	Ground-Launched Cruise Missile
GLLD	U.S. Ground Laser Locator Designator (for COPPERHEAD)
GLMX	Geological Multi-Source Exploitation (System)
GLOBIXS	Global Information Exchange System
GLOMR	Global Low-Orbiting Message Relay
GLONASS	Global Navigation Satellite System
GM	Guided Missile
GMD	Global Missile Defense
GMF	Ground Mobile Forces
GMFP	Global Military Force Policy
GMFSC	Ground Mobile Force Satellite Communications
GMI	(1) General Medical Intelligence; (2) General Military Intelligence
GMIPP	General Military Intelligence Production Plan
GMIT	Ground Military Intelligence Team (ROK)
GMRD	Guards Motorized Rifle Division (FSU)
GMS	(1) Ground Mobile System; (2) Geostationary Meteorological Satellite; (3) Ground Mission Supervisor
GMT	Greenwich Mean Time (Zulu)
GMTI	Ground Moving Target Indicator GNAS Gateway Network Access System
GNC	Global Navigation Chart
GND	Ground
GNP	Gross National Product
GNS	Global Network Segment
GNST	Glossary of Naval Ship Types
GO()	Government of (Name of Country)

Page 3357 of 3957

G-O	Office of Law Enforcement and Defense Operations (USCG)
G-OINS	Intelligence Division (USCG/G-O)
G-OIS	Investigations and Security Division (USCG/G-O)
GOB	Ground Order of Battle
GOC	(1) General Officer Commanding (UK); (2) Government of Canada; (3) Global Operations Center
GOCO	Government Owned Contractor Operated
GOES	Geostationary Operational Environmental Satellites
GOLDS	General On-Line Display System
GOLDWING	Army HF Radio; HF communications system for meteorological and other operations
GOMS	Geostationary Operational Meteorological Satellite
GOP	Generated Option Plan
GOR	General Operational Requirement
GORB	General Officer Review Board
GOS	Grade of Service
GOSC	General Officer Steering Committee
GOSIA	Government Open System Interconnect Architecture
GOSIP	Government Open Systems Interconnected Profile
GOSPLAN	State Planning Committee (FSU)
GOSSNAB	State Committee for Material-Technical Supply (FSU)
GOTS	Government Off-the-Shelf
GP	(1) Group; (2) General Purpose
GPALS	Global Protection Against Limited Strikes
GPEE	General Purpose Encryption Equipment
GPF	(1) General Purpose Forces; (2) Ground Processing Facility
gph	Gallons Per Hour
GP NAF	General Purpose Numbered Air Force
GPNDS	Global Positioning & Nuclear Detection System
GPO	Government Printing Office
GPS	(1) Global Positioning System; (2) Grid Producing Source; (3) Geographical Positioning System; (4) Ground Processing Stations
GPSCS	General Purpose Satellite Communications System
GR	(1) Graphical Reporting; (2) Gateway Router
GRAD	Graduate
GRANITE SENTRY	Proper Name of System
GRID	Brand of Portable PC
GRIPF	GUARDRAIL Integrated Processing Facility
GRD	Ground Resolved Distance
GREEN FLAG	ACC live-fly electronic combat exercise
GRG	Gridded Reference Graphic
GRO	Gamma Ray Observatory
GROFIS	Ground Forces Intelligence Study
GRP	Glass Reinforced Plastic
GRT	Gross Registered Tonnage

Page 3358 of 3957

GRU	FSU General Staff Intelligence Organization
GS	(1) General Staff, (2) General Support; (3) Geological Survey; (4) General Schedule; (5) General Service; (6) Government Service (Federal Civil Service); (7) Ground Station; (8) Government Civilian
GSA	General Services Administration
GSD	(1) Ground Sample Distance; (2) Graphical Situation Display
GSE	Ground Support Equipment
GSF	(1) Ground Support Fighter (FSU); (2) Group of Soviet Forces; (3) Ground Station Facility
GSFC	Goddard Space Flight Center
GSFG	Group of Soviet Forces Germany
GSFM	Group of Soviet Forces Mongolia
GSICS	General Support Interim Contractor Support
GSM	(1) Ground Support Module (JSTARS); (2) Ground Station Module
GSOAF	GGI&S Special Operations Applications Facility
GSP	General Strike Plan
GSR	(1) General Support Reinforcing; (2) Ground Surveillance Radar
GSRS	U.S. General Support Rocket System
GSS	(1) Global Support System; (2) General System Specification
GST	(1) Ground Sensor Terminal; (2) Ground Station Terminal; (3) Ground Support Terminal
GSTS	Ground-Based Surveillance and Tracking System
GSTN	General Switched Telephone Network
GSU	Geographically Separated Unit
G/T	Ratio of Antenna Gain to Noise Temperature
GTA	Government Training Aid
GTAB	Global Transportation Analysis Bulletin
GTD	Guards Tank Division (FSU)
GTN	Global Transportation Network
GTS	Global Telecommunications Service
GTC	Gas Turbine Compressor
GTTC	Goodfellow Technical Training Center
GUI	Graphics User Interface
GW	(1) Guided Weapon; (2) Gateway; (3) Guerrilla Warfare
G/W	Gateway
GWC	Global Weather Control
GWEN	Ground Wave Emergency Network
GWIC	Great Wall Industries Corporation (China)
GWIP	Global Weather Intercept Program
GWP	General Work Plan
GW/R	Gateway/Router
GWS	Gaps, Weaknesses, and Shortfalls (also GW&S)
GYRO	Gyroscope or Gyroscopic
GZ	Ground Zero

Page 3359 of 3957

H

H	Symbol for the magnetic field of the propagated radio wave
H_2O	Critical life-essential liquid, commonly known as water
HA	Humanitarian Assistance
HAA	Helicopter Alighting Area
HAB	(1) High Altitude Burst; (2) High Altitude Bombing; (3) High Air Burst; (4) Hardened Aircraft Bunker
HAC	(1) House Appropriations Committee; (2) Historical Area Coverage
HACC	Humanitarian Assistance Coordination Center
HAE	High-Altitude Endurance
HAHO	High-Altitude High-Opening
HAIS	Hawaiian Air Intelligence System
HAL	Helicopter Light Attack
HALE	High-Altitude Long-Endurance
HALO	High-Altitude Low-Opening
HANE	High-Altitude Nuclear Effects
HANG	Hawaii Air National Guard
HARDLOOK	Special Data Analysis Product of NAVSPACECOM/N24
HARDS	High-Altitude Radiation Detection System
HARM	High-Speed Anti-Radiation Missile (AGM-88A)
HARV	Harassment Vehicle (Drone)
HAS	Hardened Aircraft Shelter
HASC	House Armed Services Committee
HATS	Heuristic Automated Transportation System
HATMD	High-Altitude Theater Missile Defense
HAV	(1) High Acceleration Vehicle; (2) Heavy Armored Vehicle (non-tactical)
HAWS	Hawaii Area Wideband System
HAZCON	Hazardous Condition
HAZMAT	Hazardous Materials
HB	High Burst
HBWP	Host-Based Word Processing
HC	HUMINT Committee
HCA	Humanitarian and Civic Assistance
HCC	HUMINT Contingency Cell
HCF	High Command of Forces
HCI/DV/AEX	Human-Computer Interface/Data Visualization/Automated Expansion
HCR	HUMINT Collection Requirement
HCS	Helicopter Combat/Search and Rescue
HCU	High Capacity Computer Unit
HD	Horizontal Ground Distance
HDL	Harry Diamond Laboratories
HDM	Hierarchical Development Methodology

Page 3360 of 3957

HDO	Humanitarian Demining Operations
HDX	Half Duplex
HX	Half Duplex
HE	High Explosive
HEAT	High-Explosive AntiTank
HEC	Helicopter Element Coordinator
HEDI	High Endoatmospheric Defense Interceptor
HEF	Hostile Establishment File
HEI	High-Explosive Incendiary
HEL	High-Energy Laser
HELIP	HAWK European Limited Improvement Program
HELRATS	High Energy Laser Radar Acquisition & Tracking System
HELSTF	High-Energy Laser Systems Test Facility
HELW	High-Energy Laser Weapons
HELWING	Helicopter Wing
HEMP	High-Altitude Electromagnetic Pulse
HEMT	High-Electron-Mobility Transistor
HEO	(1) High-Earth-Orbit; (2) Highly Elliptical Orbit
HEP	High-Explosive Plastic
HERO	(1) Hazards of Electromagnetic Radiation To Ordnance; (2) Historical Evaluation and Research Organization
HERT	Headquarters Emergency Relocation Team
HES	Hardcopy Exploitation Systems
HESS	Hangul English Support System
HEST	High-Explosive Simulation Technique
HET	Heavy Equipment Transporter
HF	(1) High Frequency; (2) Height Finder; (3) Hydrogen Fluoride
HFE	Human Factors Engineering
HFA	High-Frequency Antenna
HF/DF	High-Frequency Direction-Finding
HFE	Heavy-Fuel Engine
HFEA	Human Factors Engineering Assessment
HFP	Host Front-End Protocol
HH	Hand-Held
HHC	Headquarters and Headquarters Company
HHD	Headquarters and Headquarters Detachment
HHS	(1) Headquarters and Headquarter Services; (2) Hasty Hide Shelter
HHW	Higher High Water
HIL	High Interest List
HI-PAR	High-Performance Precision-Approach Radar
HI-RES	High-Resolution
HIC	High-Intensity Conflict
HICOM	High Command (CINCPACFLT Voice Network)
HIDSS	Helmet-Integrated Display & Sight System

Page 3361 of 3957

HIFAR	High-Frequency Fixed-Array Radar
HIMAD	(1) High- to Medium-Altitude Defense; (2) High to Medium Altitude Adjustment
HIMS	HUMINT Information Management System
HIP	Howitzer Improvement Program
HIRMS	Human Intelligence Requirements Management System
HIROCC	Hawaiian Islands Regional Operational Control Center
HIS	(1) Honeywell Information System; (2) Hostile Intelligence Services
HISP	Hostile Intelligence Service Profiler System
HIT	High-Interest Track
HITS	(1) Human Intelligence Tasking System; (2) Hawaii Information Transfer System
HJ	HONEST JOHN (U.S. Surface-to-Surface Rocket)
HL	Hand-Launched
HLA	Helicopter Landing Areas
HLA/DZ	Helicopter Landing Area/Drop Zone
HLA/DZS	Helicopter Landing Area/Drop Zone Study
HLLV	Heavy-Lift Launch Vehicle
HL-UAV	Hand-Launched Unmanned Aerial Vehicle
HLW	Higher Low Water
HLZ	Helicopter Landing Zone
HM	Helicopter Mine Warfare
HMC	HUMINT Management Center
HMCII	Higher Military Command, Interior and Islands (Greece)
HMF	Handbook of Military Forces
HMI	(1) Host-Message Interface; (2) Human-Machine Interface
HMMWV	High-Mobility Multipurpose Wheeled Vehicle
HMS	(1) Her Majesty’s Ship; (2) HUMINT Management System
HMTV	Head-Mounted Thermal Vision
HN	Host Nation
HNAF	Host Nation Armed Forces
HNIS	Host Nation Intelligence Support
HNS	Host Nation Support
HNSC	House National Security Committee
HOB	Height of Burst
HOBO	Homing Optical Bomb
HOC	(1) History of Coverage; (2) HUMINT Operations Cell
HOCNET	HUMINT Operational Communications Network
HOE	Homing Overlay Experiment
HOIS	Hostile Intelligence Service(s)
HOJ	Home on Jam
HOL	High-Order Language
HOM	(1) Head of Media; (2) Head of Mission
HOTA	HUMINT Operational Tasking Authority

Page 3362 of 3957

HOTOL	Horizontal Takeoff & Landing
HOTPHOTOREP	Hot Photographic Interpretation Report
HOTSIT	Hot Situation Message
how	Howitzer
HP	(1) Headquarters Pamphlet; (2) Horsepower
HPA	High-Power Amplifier
HPG	Hardcopy Products Group
HPM	High-Power Microwave
HPT	(1) High-Payoff Target; (2) High-Priority Target
HPSC	High-Performance Computing Research System
HPSCI	House Permanent Select Committee on Intelligence
HQ/HQS	Headquarters
HQDA	Headquarters, Department of the Army
HQJTF	Headquarters, Joint Task Force
HQMC	Headquarters, U.S. Marine Corps
HQMRHITS	Quarterly Management Report
HQ USAF	Headquarters, Department of the Air Force
HR	(1) High Resolution; (2) Humanitarian Relief Service
hr	Hour
HR/MR	Human Readable/Machine Readable (Data)
HRC	Human Resources Committee
HRCS	High-Resolution Camera System
HRMS	Human Intelligence Requirements Management System
HRPT	High-Resolution Picture Transmissions
HRR	High-Resolution Radar
HRS	(1) Hours; (2) Humanitarian Relief Service
HRTV	High-Resolution Television
HRU	Hardcopy Reconstruction Unit
HRV	High-Resolution Visible Range Instruments
HS	(1) Helicopter Squadron; (2) Home Station
HSD	HUMINT Support Detachment
HSE	HUMINT Support Element
HSE-E	HSE-Europe
HSE-SOCOM	HSE-USSOCOM
HSI	(1) Human Systems Integration; (2) Hyperspectral Imagery
H-SIP	H-Camera Spectral Improvement Program
HSLLADS	High Speed Low Level Aerial Delivery System
HSMS	Human Sources Management System
HSS	Health Service Support
HTACC	Hardened Tactical Air Control Center
HTKP	Hard-Target Kill Potential
HTLD	High-Technology Light Division
HTOHL	Horizontal Take-off and Horizontal Landing
HTML	Hypertext Markup Language
HUD	Heads-Up Display

Page 3363 of 3957

HULTEC	Hull-to-Emitter Correlation
HUMINT	Human Resources Intelligence
HUMMV	High Utility Mobile Mechanized Vehicle
HUMRO	Humanitarian Relief Operations
HUS	Hardened Unique Storage
HUSK	Hardened Unique Storage Key
hv	Heavy
HVA	High Value Asset
HVAC	High-Voltage Air Conditioning
HVAP	High-Velocity Armor-Piercing
HVAPFSDS	High Velocity Armor-Piercing Fin-Stabilized Discarding-Sabot
HVAT	High-Velocity Antitank
HVF	Highly Volatile Fuel
HVIT	High Volume Information Transfer
HVT	High-Value Target
HW	(1) High Water; (2) Hardware
HWAS	High Wycombe Air Station
HWC	Hobart Walk-in Cooler
HW/SW	Hardware/Software
HWY	Highway
Hz	Hertz

Page 3364 of 3957

I

i	Inclination
I2	Intelligence Information
IA	(1) Imagery Analyst; (2) Intelligence Assistant; (3) Initial Assessment; (4) Intelligence Analyst; (5) Intelligence Agent
IAA	Interagency Agreement
I&A	(1) Imagery and Analysis; (2) Identifcation and Authentication
IAB	Imagery Analysis Branch
IAC	(1) Intelligence Analysis Center; (2) Intelligence Advisory Committee; (3) Intelligence Analyst Course (DIA); (4) Information Analysis Centers
IAD	(1) Intelligence Analysis Division; (2) Integrated Air Defense
IADB	Inter-American Defense Board
IADS	Integrated Air Defense System
IAEA	International Atomic Energy Agency
IAG	(1) Intelligence Analysis Group (formerly ITAD); (2) Imagery Analysis Group
IAGC	Instantaneous Automatic Gain Control
IAGS	Inter-American Geodetic Survey
IAIPS	Integrated Automated Intelligence Processing System
IAM	Imagery Analysis Memorandum
IAMP	Imagery Acquisition and Management Plan
IAMS	Individual Aerial Mobility System
IAN	Imagery Analysis Notice
IAP	International Airport
IAPF	Inter-American Peace Force
IAR	Imagery Analysis Report
IAS	(1) Intelligence Access System; (2) Interactive Applications System; (3) Intelligence Analysis System
IAS WS	IAS Work Station
IASSA	INSCOM Automated Systems Support Activity
IAT	Intelligence Augmentation Team
IATA	International Air Transport Association
IAW	In Accordance With
IAWG	Interagency Working Group
IAWS	Improved Analyst Workstation
IBAC	Identity-Based Access Control
IBs	Issue Books
IBBS	Interim Brigade/Battalion Simulation
IBD	Intelligence Baseline Document
IBDTF	IBD Transaction Format
IBE	Field-Initiated BE Number
IBERLANT	Iberian Atlantic Area
IBIS	Imaging Background Limited Infrared System
IBM	International Business Machines

Page 3365 of 3957

IBO	Intelligence Baseline Overview
IBOS	Intelligence Battlefield Operating System
IBS	(1) Interactive Beacon System; (2) Integrable Base Station; (3) Integrated Broadcast Service; (4) Intelsat Business Service; (5) Integrated Bridge System
IBSSIR	Background Signature Survey
IBTA	Integrated Battlefield Targeting Architecture
IBUR	Intelligence Bottom-Up Review
IC	(1) Intelligence Community; (2) Intelligence Collection; (3) Integrated Circuit; (4) Intelligence Center; (5) Irish Concern
IC/EC	Intelligence Community/Executive Committee
ICA	Intelligence Center Atlantic
ICAF	Industrial College of the Armed Forces
ICAO	International Civil Aviation Organization
ICAP	Improved Capabilities Program
ICARIS	Intelligence Communications Architecture and Requirements Information System
ICBM	Intercontinental Ballistic Missile
ICC	(1) Integrated Communications Center; (2) Intelligence Continuity Cell; (3) IMlNT Coordination Cell; (4) Intelligence Coordination Center (Coast Guard); (5) Initial Connectivity Capability
ICCC	International Council for Computer Communication
ICD	(1) Interface Control Document; (2) Intelligence Collection Division; (3) Initiative Communications Deception
ICDP	Intelligence Career Development Program
ICE	(1) Independent Cost Estimate; (2) Interface Control Element
ICEDEFOR	Iceland Defense Forces
ICES	International Cooperation in Ocean Exploration
ICF	(1) Intelligence Collection Flight; (2) Intelligence Contingency Funds; (3) Interconnect Facility
ICFTU	International Confederation of Free Trade Unions
ICIG	IDHSS CSSR Interface Guard
ICITAP	International Criminal Investigative Training and Assistance Program
ICL	Intelligence Coordination Cell
ICM	(1) Improved Conventional Munitions; (2) Intelligence Correlation Module; (3) Integrated Common Modules
ICMC	Intelligence Collection Management Course
ICOD	Intelligence/Information Cut-Off Date
ICOM	Integrated COMSEC (SINCGARS)
ICON	Image Communications and Operations Node
ICP	(1) Intelligence Collection Platform; (2) Interface Change Proposals; (3) Incremental Change Packages
ICPS	Intelligence Communications Processing Shelter
ICR	Intelligence Collection Requirement
ICRC	(1) Intelligence Contingency Readiness Center; (2) International Committee of the Red Cross
ICRS	Imagery Collection Requirements Subcommittee (COMIREX)

Page 3366 of 3957

ICS	(1) Intercommunications System; (2) Intelligence Community Staff
ICTF	Interagency Crisis Task Force
ICTT	(1) Improved Commander's Tactical Terminal; (2) Interim Commander's Tactical Terminal
ICU	Interface Control Unit
ICV	Infantry Combat Vehicle
ICW	In Coordination With
ICWG	(1) Interface Control Working Group; (2) Imagery Coordination Working Group
ID	(1) Identification; (2) Infantry Division; (3) Intelligence Division
IDA	Institute for Defense Analysis
IDAD	Internal Defense and Development
IDB	(1) Integrated Data Base; (2) Inter-American Development Bank
IDB-II	PC-Based Integrated Data Base
IDBM	Integrated Data Base Maintenance
IDBR	Integrated Data Base Retrieval
IDBTF	Intelligence Data Base Transaction Format
IDC	Interagency Defector Committee
IDCSP	Initial Defense Communications Satellite Program
IDEAS	Intelligence Data Element Authorization Standards
IDES	Installation Damage Expectancy Summary
IDEX	Imagery Data Exploitation System
IDEX II	Imagery Data Exploitation System II
IDF	(1) Israeli Defense Force; (2) Installation Data File
IDHS	Intelligence Data Handling System
IDHS	IDHS for the mid-1990s
IDHS-2000	Intelligence Data Handling System for the Year 2000
IDHS-II	Intelligence Data Handling System, Second Iteration
IDHSC	Intelligence Data Handling System Communications
IDHSC-II	Intelligence Data Handling System Communications, Version II
IDIMS	Interactive Digital Image Manipulation System
IDIQ	Indefinite Delivery, Indefinite Quantity
IDIRA	Introduction to Defense Intelligence Research and Analysis (DIA)
IDL	Interoperable Data Link
IDM	Improved Data Modem
IDMS	IPAC Document Management System
IDN	Integrated Data Network
IDNX	Integrated Digital Network Exchange
IDP	Intelligence Data Processor
IDPS	(1) Imagery Data Processing System; (2) Integrated Deployable Processing System; (3) Interim Deployable Processing System
IDS	(1) Intrusion Detection System; (2) Infrared Detection Set
IDSCS	Initial Defense Satellite Communications System
IDSCP	Initial Defense Satellite Communication Program

Page 3367 of 3957

IDSF	Intelligence Defector Source File
IDTT	Inactive Duty Training Travel
IDZ	Inner Defense Zone
IEA	International Energy Agreement
IEBL	Inter-Entity Boundary Line
IEC	(1) Imagery Exploitation Center; (2) Intelligence Exchange Conference
IED	(1) Improvised Explosive Device; (2) Imitative Electronic Deception
IEG	Imagery Exploitation Group
IEMATS	Improved Emergency Message Automated Transmission System
IEP	Independent Evaluation Plan
IEPG	Independent European Program Group
IEPR	Information Exchange and Processing Requirements Report
IER	Independent Evaluation Report
IES	Imagery Exploitation System
IESS	Imagery Exploitation Support Segment
IEW	Intelligence and Electronic Warfare
IEWCS	IEW Common Sensor
IEWD	Intelligence and Electronic Warfare Directorate
IEWFAM	IEW Functional Area Model
IEWSE	IEW Support Element
IEWTAC	IEW Technology Assessment Center
IEWTPT	IEW Tactical Proficiency Trainer
IF	(1) Interrogation Facility; (2) Identification Frequency; (3) Intermediate Frequency
IFAC	International Federation of Automatic Control
IFF	Identification, Friend or Foe
IFFN	Identification, Friend, Foe or Neutral
IFOR	Implementation Force (Operation JOINT ENDEAVOR)
IFOV	Instantaneous Field-of-View
IFPS	Interformation Position System
IFR	Instrument Flight Rules
IFRB	International Frequency Registration Board
IFS	Imagery File Server
IFTE	Integrated Family Test Equipment
IFV	Infantry Fighting Vehicle
IG	(1) Interagency Group; (2) Inspector General; (3) Intelligence Group (Air Force)
IGCP	Intelligence Guidance for COMINT Programming
IGD	Intelligence Guidance Document
IGR	Improved GUARDRAIL
IGRV	Improved GUARDRAIL V
IGS	Image Generation System
IGSM	Interim Ground Station Module
IGT	Interdepartmental Group on Terrorism

Page 3368 of 3957

IGY	International Geophysical Year
IHC	Intelligence Information Handling Committee
IHE	Insensitive High Explosive
IHFR	Improved High Frequency Radio
IHO	(1) International Hydrographic Organization; (2) In Honor of
IHR	In-Extremis Hostage Rescue
II	(1) Imagery Interpretation; (2) Imagery Interpreter
IIC	Imagery Interpretation Center
IICT	Interagency Intelligence Committee on Terrorism
IID	Integrated Information Display
IIDP	Integrated Intelligence Development Plan (USCINCEUR)
IIE	Installation Identification Element
IIF	Imagery Interpretation Facility
IIG	(1) Imagery Intelligence Group (formerly USAIIC); (2) Intelligence Inspector General
IIM	Interagency Intelligence Memorandum
IIN	Imagery Interpretation Note
IINCOMNET	Intratheater Intelligence Community Network
IINS	Imagery Information Need Statement
IIPL	Integrated Intelligence Priority List
IIR	(1) Imaging Infrared; (2) Intelligence Information Report; (3) Imagery Interpretation Report
IIRES	Imagery Interpretation, Reporting, and Exploitation System
IIRK	Interarea Interswitch Rekeying Key
IIRS	Imagery Interpretability Rating Scale
IIS	(1) Indirect Identification System; (2) IPAC Intelligence Summary; (3) Imagery Interpretation Segment
IISE	Intelligence Information System Enhancement
IISS	Intelligence Information Subsystem
IITLPC	Inter/Intra Team Low Power Communications
IITS	(1) Intra-Theater Imagery Transmission System; (2) Installation Information Transfer Systems
IIU	(1) Imagery Interpretation Unit; (2) Imagery Interface Unit
IJMS	Interim JTIDS Message Standard
ILAM	Improved Limpet Assembly Modular
ILC	International Lines of Communication
ILD	Injection Laser Diode
ILE	Intelligence Liaison Element
ILEA	International Law Enforcement Academy
ILO	Intelligence Liaison Officer
ILP	Intelligence Liaison Party
ILS	(1) Instrument Landing System; (2) Integrated Logistic Support
ILSA	Improved Lightweight Satellite Antenna
IM	(1) Information Management; (2) Intermodulation
IM/GD	Intelligence Management/Guidance Document

Page 3369 of 3957

IMA	(1) Institute for Military Assistance; (2) Intelligence Mobilization Augmentee; (3) Information Mission Area
I-MAE	Interim Medium Altitude Endurance UAV (formerly Tier I)
IMAF	1st Marine Amphibious Force
IMAP	Interim Mission Assessment Program
IMB	(USCENTCOM) Intelligence Management Board
IMC	The International Medical Corps
IMCO	Intergovernmental Maritime Consultative Organization
IMD	Intelligence Management Document
IMEF	First Marine Expeditionary Force
IMET	(1) International Military Education and Training; (2) Integrated Management Evaluation Team
IMETS	Integrated Meteorological System
IMF	International Monetary Fund
IMINT	Imagery Intelligence
IMIS	(1) Intelligence Management Information System; (2) Integrated Management Information System
IMLETT	International Maritime Law Enforcement Training Team
IMMP	Information Management Master Plan
IMNET	Imagery Network
IMOM	Intelligence Many-on-Many
IMOC	International Maritime Officer Course
IMP	(1) Interface Message Processor; (2) Input Message Processor; (3) Image Product; (4) Information Management Program
IMPs	Imagery Products
IMS	International Military Staff (NATO)
IMSAT	Imagery Satellite
IMSE	Imagery Management Support Element
IMSO	International Maritime Satellite Organization
IMTT	Intelligence Mobile Training Team
IN	(1) International Negotiations; (2) Intelligence; (3) Infantry; (4) Director of Intelligence (Air Force Component) (also A2)
INA	Information Not Available
INCA	(1) Intelligence Communications Architecture; (2) Integrated Nuclear Communications Assessment
INCOLLNOM	Intelligence Collection Requirement Nomination
INCOMNET	Intratheater Intelligence Communications Network
INCSEA	Incidents at Sea
INDICOM	(1) Indications Communication Network; (2) Indications and Warning Communications
INDICOMM	Indications Intelligence Communications
INEWS	Integrated Electronic Warfare System
inf	Infantry
INF	Intermediate-Range Nuclear Forces
INFIL	Infiltration
INFLIGHTREP	Inflight Reports
INFLTRPT	Inflight Reports

Page 3370 of 3957

INFO	Information
INFOSEC	(1) Information Security; (2) Information Systems Security
INGO	International Nongovernmental Organizations
INI	Initiation
INL	International Narcotics and Law
INMARSAT	International Maritime Satellite
INMS	Integrated Network Management System
INR	Bureau of Intelligence and Research (State Department)
INS	(1) Inertial Navigation System; (2) Immigration and Naturalization Service
INSAT	Indian Satellite
INSICOM	Integrated Special Intelligence Communications
INSCOM	U.S. Army Intelligence and Security Command
INST	Instruction
INSTA	Automated Installations File (DIAOLS)
INSTAL	Installation
instl	Installation
INSUM	Intelligence Summary
INT/INTEL	Intelligence
INTACS	(1) Integrated Tactical Communications System; (2) Integrated Tactical Communications Study
INTCP	Intercept
INTEL	Intelligence
INTELCAST	Intelligence Broadcast
INTELCOM	Worldwide Intelligence Communication
INTELDATA	Intelligence Data
INTELINK	Proper Name of System
INTELSAT	International Telecommunications Satellite Organization
Intelink	Command server/client system that allows secure SCI connectivity to all commands on the network, and access to available files without additional log-on.
INTELNET	Intelligence Network
Internet	International Network
INTI	CI database
intg	Interrogation
INTRA	International Travel by Selected Foreign Officials
Intranet	Internet with local scope
INTREP	Intelligence Report
INREQ	Intelligence Request
INTSUM	Intelligence Summary
INUT	Indian Nuclear Underground Test
IO	(1) Indian Ocean; (2) Intelligence Officer; (3) Information Objectives; (4) Intelligence Objective; (5) Intelligence Operations (Division); (6) Information Operations; (7) Information Objectives
I/O	Input/Output
IOA	Indian Ocean Area

Page 3371 of 3957

IOB	Intelligence Oversight Board
IOC	(1) Initial Operational Capability; (2) Intelligence Operations Center
IOCTL	Indian Ocean Conventional Target List
IOD	Intelligence Operations Division (USEUCOM)
IOF	Intelligence Operations Facility
IOIC	Integrated Operational Intelligence Center
IOM	Input/Output Module
IOMDWG	Interagency Offensive Missile Deployment Working Group
IONDS	Integrated Operational Nuclear Detection System
IOR	Individualized Operational Ration
IONDS	Integrated Operational Nuclear Detection System
IOS	(1) Intelligence Operations Specialist; (2) International Organization for Standards
IOSS	(1) Integrated Operational Support Study; (2) Intelligence Organization Stationing Study
IOT&E	Initial Operational Test and Evaluation
IP	(1) Initial Point; (2) Imagery Processing; (3) Intelligence Problem; (4) Instrumentation Point; (5) Immediate Permanent Incapacitation Dose; (6) Internet Protocol
IP/MP	Inphase/Midphase
IPA	(1) Intelligence Production Activity; (2) Imagery Product Archive
IPAT	Intelligence Planning/Programming Analysis Tool
IPB	Intelligence Preparation of the Battlefield/Battlespace
IPC	(1) Industrial Planning Committee; (2) Intelligence Producers' Council; (3) Intelligence Production Center
IPCP	Intelligence Production Campaign Plan
IPCS	Intelligence Producers Council Staff
IPD	(1) Intelligence Planning Document; (2) Intelligence Plans Division (USEUCOM); (3) Intelligence Production Division
IPDB	Intelligence Production Data Base
IPDS	Imagery Processing and Dissemination System
IPE	Intelligence Production Element
IPF	(1) Integrated Processing Facility; (2) Intelligence Processing Facility (Guardrail)
IPG	Implementation Planning Group
IPIR	(1) Immediate Photo Interpretation Report; (2) Initial Photographic Interpretation Report; (3) Initial Programmed Interpretation Report; (4) Initial Phase Interpretation Report
IPR	Integrated Personal Armor
IPIX	Interface Processor for Imagery Exchange

Page 3372 of 3957

IPM	(1) Interface Processor for Imagery Exchange; (2) Intelligence Programs Management
IPMA	Intelligence Production Management Activity
IPMO	Intelligence Program Management Office
IPL	Integrated Priority List
IPM	Interpersonal Messaging
IPOIC	Interagency Prisoner of War Ad Hoc Committee
IPOM	Intelligence Program Objective Memorandum
IPP	(1) Intelligence Producer Profile; (2) Impact Point Prediction
IPR	(1) Intelligence Production Requirement; (2) In Process Review; (3) Impulse Response; (4) Internet Protocol Route
IPRG	(1) Intelligence Priorities Review Group; (2) Intelligence Program Review Board
IPS	(1) Integrated Program Summary; (2) Intelligence Production System; (3) Imagery Processing Segment (CARS); (4) Intelligence Production Section; (5) Instructions Per Second; (6) Imagery Processing System
IPSC	Information Processing Standards for Computers
IPSG	Intelligence Program Support Group (now CISA)
IPSO	Internet Protocol Security Option
IPSP	Intelligence Priorities for Strategic Planning
IPT	Integrated Product Team
IPU	Inter-Parliamentary Union
IPW	Interrogation of Prisoners of War
IPWG	Intelligence Priorities Working Group
IPX	Internet Packet Exchange
IR	(1) Infrared; (2) Intelligence Information Report; (3) Illumination Rate; (4) Impulse Response; (5) Information Requirement; (6) Intelligence Requirement; (7) Initial Radiation; (8) Induced Radiation; (9) Information Ratio
I2R	Imaging Infrared
IRA	Intelligence-Related Activities
IRAC	Interdepartmental Radio Advisory Committee
IRBM	Intermediate-Range Ballistic Missile
IRC	(1) International Red Cross; (2) International Rescue Committee
IRCM	Infrared Countermeasures
IRCS	Improved Radar Calibration System
IR&D	Independent Research & Development

Page 3373 of 3957

IRD	(1) Independent Research & Development; (2) Intelligence Resources Division; (3) Intelligence Reserve Detachment
IRDB	Integrated Requirements Data Base
IRDC	Intelligence Research and Development Council
IRDHS	Imagery-Related Data Handling System (see AIRES)
IREMBASS	Improved Remotely Monitored Battlefield Surveillance System
IRDS	Infrared Detection System
IREMBASS	Improved-Remotely Monitored Battlefield Sensor System
IREPS	Integrated Refractive Effects Prediction System
IRF	(1) Imagery Readiness Facility; (2) Intelligence Readiness Facility
IRG	Interdepartmental Regional Group
IRGM	Infrared Guidance Module
IRINT	Infrared Intelligence
IRIS	Infrared Imaging System
IRISA	Imagery Report Index Summary
IRISF	Intelligence Report Index Summary File
IRK	Interswitch Rekeying Key
IRLS	Infrared Line Scanner
IRM	(1) Intelligence Requirements Management; (2) Information Resource Management
IRMS	Imagery Requirements Management System
IROF	Imagery Reconnaissance Objectives File
IROL	Imagery Reconnaissance Objectives List
IROP	(1) Imagery Reconnaissance Objectives Plan; (2) Infrared Optical Intelligence; (3) Imagery Requirements Objectives Program
IRPG	Installation Reference Points Graphics
IRPIA	Intelligence Information Report Photo Index
IRR	(1) Individual Ready Reserve; (2) Intelligence Requirement Request; (3) Intelligence Readiness Report
IRS	(1) Intelligence Research Specialist; (2) Internal Revenue Service; (3) Interface Requirements Specification; (4) Intelligence Requirements Subcommittee
IRSCOM	Imagery Requirements Subcommittee
IS	(1) Information Systems; (2) Intelligence Specialists; (3) Intelligence Squadron
I&S	(1) Intelligence and Security; (2) Intelligence and Surveillance

Page 3374 of 3957

ISA	(1) International Security Affairs; (2) Interservice Support Agreement; (3) Intelligence Support Activity; (4) Integration Support Activity; (5) International Support Agreement
ISAF	Israeli Air Force
ISAR	Inverse Synthetic Aperture Radar
ISARC	Intelligence, Surveillance, and Reconnaissance Cell
ISB	(1) Initial Staging Base; (2) Intermediate Staging Base; (3) Intelligence Systems Board; (4) Intelligence Support Base
ISC	(1) Information Systems Command; (2) Information Science Center; (3) Intelligence Support Cell
ISCO	Intelligence Support to Combined Operations
ISC/SC	Intelligence Specialist Chief/Senior Chief
ISD	(1) Intelligence Support Detachment; (2) Intelligence Security Division; (3) Intelligence Support Division
ISDB	Integrated Satellite Data Base
ISDN	(1) Integrated Services Data Network; (2) Intelligence Services Digital Network ISEIntelligence Support Element
ISEMS	Improved Spectrum Efficiency Modeling and Simulation
ISEW	Intelligence, Security, and Electronic Warfare
ISF	Intelligence Support Facility (U.S. Navy)
ISG	Intelligence Support Group (U.S. Navy)
ISHMRS	Improved SOF High Frequency Manpack Radio System
ISIC	Intelligence Support and Indications Center
ISID	Interim Secondary Imagery Dissemination System
ISIDS	Improved SIDS
ISINT	Instrumentation Signals Intelligence
ISIP	Intelligence Support Interface Program
ISIS	(1) Integrated Signals Intelligence System; (2) Interim SOCOM Intelligence Threat Data System
ISLES	Information Systems for Law Enforcement Support
ISM	Industrial Security Manual
ISMB	Intelligence Systems Management Board
ISO	(1) Information Systems Office; (2) International Standards Organization
ISOFAC	Isolation Facility
ISOPREP	Isolated Personnel Report
ISOS	Intelligence System of Systems
ISP	(1) Intelligence Support Plan; (2) Industrial Security Program; (3) Intelligence Support Processor; (4) Integrated Survey Program; (5) Intelligence Survey Program
ISP DCS	Integrated Survey Program Data Collection System
ISP CPE	Integrated Survey Program Central Production Element
ISPER	IPAC Special Reports
ISPO	Intelligence Support Program Office
ISPR	Information Systems Processing Request
ISPS	(1) ISP Server; (2) Improved SOF Power Sources
ISPT	Intelligence Support Processor Tool

Page 3375 of 3957

ISR	(1) Imagery Support Requirement; (2) Inter-Agency Source Registry; (3) Intelligence, Surveillance and Reconnaissance
ISRD	Information Systems Requirement Document
ISS	(1) Intelligence Support System; (2) Intelligence Support Sub-system; (3) Intelligence Support Staff; (4) Information Security System; (5) Information Systems Security
I&SS	Intelligence and Security Service
ISSA	(1) Information Systems Support Activity; (2) Inter-service Support Agreement
ISSM	Information Systems Security Manager
ISSO	(1) Information Systems Security Officer; (2) Intelligence Systems Support Office
ISST	ICBM SHF Satellite Terminal
IST	(1) Imagery Support Terminal; (2) Intelligence Support Team; (3) Intelligence System Team
ISTA	Intelligence, Surveillance, Target Acquisition
ISWG	Intelligence Support Working Group
ISYSCON	Integrated System Control
IT	Immediate Transient Incapacitation Dose
ITA	(1) Intelligence Terrain Analyzer; (2) International Telegraph Alphabet
ITAAS	Intelligence Training Army Area Schools
ITAC	(1) Intelligence and Threat Analysis Center (U.S. Army); (2) Intelligence Tracking Analysis and Correlation
ITACIES	Interim Tactical Imagery Exploitation System (U.S. Army)
ITACS	Integrated Tactical Air Control System
ITAR	International Traffic in Arms Regulations
ITAS	Improved Target Acquisition System
ITC	Interagency Training Center
ITCT	Improved Tactical Commander's Terminal
ITD	(1) Interim Terrain Data; (2) Individual Training Directorate; (3) International Training Division
ITDB	Intercept Tasking Data Base
ITDN	Integrated Tactical Data Network
ITEP	(1) Interim Tactical ELINT Processor (U.S. Army); (2) Integrated Threat Evaluation Program
ITF	Intelligence Task Force
ITFN	Intra-Task Force Network
ITG	Interdiction Target Graphic
ITIBS	Improved TIBS
ITIC-PAC	INSCOM Theater Intelligence Center-Pacific
ITII	Internal-to-Internal Interface
ITL	Interagency Telephone Laboratory
ITO	(1) International Trade Organization; (2) Integrated Tasking Order
ITOC	Interrogation Translation Operations Center
ITP	(1) Intelligence Town Plan; (2) Interrogation/Translation Platoon
ITS	Imagery Transmission System

Page 3376 of 3957

ITSS	Integrated Tactical Surveillance System
ITT	Interrogator Translator Team
ITU	(1) Interrogator-Translator Unit; (2) International Telecommunications Union
ITUT	Interim Tactical Users Terminal
ITW	(1) International Targeting Workstation; (2) Integrated Threat Warning
ITW&AA	Integrated Tactical Warning and Attack Assessment
IU	(1) Interface Unit; (2) Image Understanding
lUG	Intelligence Users' Guide
IUS	Inertial Upper Stage
IUSS	Integrated Undersea Surveillance System
IVAN	Intelligence Van
IVCS	Integrated Vehicle Communications System
IVD	Interactive Video Disk
IVIS	Inter-Vehicle Information System
IVSN	Initial Voice Switched Network
IW	(1) Information Warfare; (2) Intelligence Wing
I&W	(1) Indications and Warning; (2) Intelligence & Warning
IWC	Information Warfare Center
IWD	Intermediate Water Depth
IWG	Intelligence Working Group
IWO	Intelligence Watch Officer
IWS	(1) Intelligence Work Station; (2) Information Warfare Squadron
IWSDB	Integrated Weapon System Data Base
IWST	Information Warfare Support Team
IWT	Intelligence Watch Team
IWTS	Indications and Warning Training System
IWW	Inland Waterway
IX	Unclassified Miscellaneous Ship

Page 3377 of 3957

J

J3	Director(ate) of Operations
J4	Logistics Directorate
J5	Director(ate) of Plans, Policy, and Programs
J6	(1) Director(ate) of Command, Control, Communications; (2) Director(ate) of Command, Control, Communications, and Computer Systems
J7	Joint Operational Plans Staff
J8	Director(ate) of Resource Management
JA	Judge Advocate (General)
JAADS	Joint Allied Air Defense System
JAAT	Joint Air Attack Team
JAC	Joint Analysis Center
JACC/CP	Joint Airborne Communications Center/Command Post
JAD	Joint Assessment Data
JAEIC	Joint Atomic Energy Intelligence Committee
JAG	Judge Advocate General
JAI	Joint Administrative Instruction
JAIEG	Joint Atomic Information Exchange Group
JAIS	Japan Air Intelligence System
JAIS-PAC	Joint Area Information system-USPACOM
JAMIP	Joint Analytic Model Improvement Program
JAN	Joint Army-Navy
JANAF	Joint Army, Navy, Air Force Publication
JANAP	Joint Army/Navy Publication
JAO	Joint Area of Operations
JAOC	Joint Air Operations Center
JAOP	Joint Air Operations Plan
JAPC	Joint Attrition and Penetration Committee
JAR	JIC Analysis Report
JARCC	Joint Air Reconnaissance Control Center
JARIC	(1) Joint Aerial Reconnaissance Intelligence Center; (2) Joint Air Reconnaissance Interpretation Center (UK)
JAROC	(B) Joint Allied Refugee Operations Center (Berlin)
JARP	Joint Aerospace Reserve Program
JASDF	Japanese Air Self-Defense Forces
JASORS	Joint Advanced Special Operations Radio System
JASPO	Joint Airborne SIGINT Program Office
JASS	Joint Airborne SIGINT System
JAST	Joint Advanced Strike Technology Program
JATCCCS	Joint Advanced Tactical C3 System
JAWS	(1) Joint Analytical Workstation; (2) Joint Advanced Weapons System; (3) JDISS-Army Workstation
JBS	(1) Joint Base Station; (2) Joint Broadcast Service
J2C	CIA Liaison

Page 3378 of 3957

JC2WC	Joint C2 Warfare Center
JCAT	(1) Joint Crisis Action Team; (2) Joint Crisis Analysis Tool
JCC	Joint Coordination Center
JCCC	Joint Communications Control Center
JCCOC	Joint Communications & Control Operational Concept
JCCWC	Joint Command and Control Warfare Center
JCET	Joint/Combined Exercises for Training
JCEOI	Joint CEOI
JCF	Joint Communications Facility
JCISB	Joint Counterintelligence Support Branch
JCISOC	Joint CI Staff Officer's Course
JCMC	(1) Joint Crisis Management Capability; (2) Joint Crisis Management Center
JCMEC	Joint Captured Materiel Exploitation Center
JCMO	Joint Collection Management Office
JCMOTF	Joint Civil Military Operations Task Force
JCMPO	Joint Cruise Missile Project Office
JCMST	Joint Collection Management Support Tool (renamed JCMT)
JCMT	Joint Collection Management Tool
JCNJSIC	Center Cheyenne Mountain Air Force Base (CMAFB) Node
JCNICC	Joint Counternarcotics Intelligence Coordination Center
JCP	Joint Congressional Committee on Printing
JCPES	Joint Chiefs Planning and Execution System
JCPX	Joint Command Post Exercise
JCRC	Joint Casualty Resolution Center
JCS	Joint Chiefs of Staff
JCSAN	JCS Alert Network
JCSAR	Joint Combat Search and Rescue
JCSE	(1) Joint Communications Support Element; (2) Joint Contingency Support Element
JCSM	Joint Chiefs of Staff Memorandum
JCSS	(1) Japan Combat Support System; (2) Joint Communications Support Squadron
JCTG-ME	Joint Technical Coordinating Group for Munitions Effectiveness
J2D	DIA Liaison
JDA	(1) Joint Deployment Agency; (2) Japan Defense Agency; (3) Joint Duty Assignment
JDAC	Joint District Area Command
JDAL	Joint Duty Assignment List
JDAM	Joint Direct Attack Munition
JDC	Joint Debriefing Center
J-DEC	JICPAC-Detachment Japan
JDEC	Joint Document Exploitation Center
JDF	Joint Development Facility
JDGW	Joint Digital Geopositioning Workstation
JDIA	Joint Digital Intelligence Assessment

Page 3379 of 3957

JDIPC	Joint Deployable Imagery Production Center
JDISS	(1) Joint Deployable Intelligence Support System; (2) Joint Defense Intelligence Support Services
JDISS-C	Joint Deployable Intelligence Support System-CENTCOM
JDISS-E	JDISS-EUCOM
JDISS-S	Joint Deployable Intelligence Support System-SOCOM or SOCRATES
JDIVS	Joint Deployable Intelligence Video/Data System
JDMAG	Joint Deployable Maintenance Analysis Group
JDS	Joint Deployment System
JDSS	Joint Decision Support System
JDSIR	Joint Deployment System Incident Reporting System
JDSSC	Joint Data System Support Center
JEAP	(1) Joint Electronic Analysis Program; (2) Joint Electronic Analysis Position
JEC	Joint Economic Committee
JECC(G)	Joint Exercise Control Center (Group)
JECG	Joint Exercise Control Group
JECM	Joint Electronic Countermeasures
JEEP	Joint Emergency Evacuation Plan
JEIO	Joint Engineering and Interoperability Organization
JEFPROS	JAC EUCOM Force Protection Summary
JEIR	JAC EUCOM Intelligence Review
JEL	Joint Electronic Library
JEM	Joint Exercise Manual
JES	JDISS Embedded Support
JESS	Joint Exercise Support System
JET	JWICS Earth Terminal
JETDS	Joint Electronics Designation System
JEWC	Joint Electronic Warfare Center
JFACC	Joint Force Air Component Commander
JFC	(1) Joint Fusion Center; (2) Joint Force Commander
JFFC	Joint Force Fires Coordinator
JFFSC	Joint Force Fire Support Coordinator
JFI	Joint Force Integrator
JFIC	Joint Force Interdiction Coordinator
JFITL	Joint Force Integrator Task List
JFK CTRMA	John F. Kennedy Center for Military Assistance
JFLCC	Joint Force Land Component Commander
JLOTS	Joint Logistics Over the Shore
JFM	Joint Force Memorandum
JFMCC	Joint Force Maritime Component Commander
JFMO	Joint Frequency Management Office
JFSOCC	Joint Force Special Operations Component Commander
JGITSS	Joint General Intelligence Training System Subarchitecture

Page 3380 of 3957

JGSDF	Japanese Ground Self-Defense Forces
JIATF	Joint InterAgency Task Force
JIATF-E	Joint InterAgency Task Force - East
JIATF-W	Joint InterAgency Task Force - West
JIB	Joint Intelligence Bureau (Commonwealth Countries)
JIC	(1) Joint Intelligence Center; (2) Joint Interrogation Center; (3) Joint Intelligence Cell
JIC-E	Joint Intelligence Center-Europe
JIC-SOUTH	Joint Intelligence Center-U.S. SOUTHCOM
JIC-2000	Designation of JICSOUTH upon movement to CONUS
JICEUR	Joint Intelligence Center Europe
JICPAC	Joint Intelligence Center Pacific
JICREP	Joint Intelligence Center Report
JICTRANS	Joint Intelligence Center for Transportation
JIEO	Joint Interoperability Engineering Organization (DISA)
JIEP	Joint Intelligence Estimate for Planning
JIF	Joint Interrogation Facility
JIFF	Joint Interdiction of Follow-on Forces
JIIKS	Joint Imagery Interpretation Key Structure
JIIM	Joint Intelligence Information Management
JILE	Joint Intelligence Liaison Element
JIM	JESS Intelligence Model
JINTACCS	Joint Interoperability of Tactical Command and Control Systems
JINTC	Joint Intelligence Task Force
JIO	Joint Intelligence Organization
JIOC	Joint Intelligence Operations Center
JIPC	Joint Imagery Production Center
JIPTL	Joint Integrated Prioritized Target List
JISA	Joint Intelligence Support Architecture
JISAD	JTF Intelligence Support Architecture Document
JISC	(1) Joint Intelligence Support Center; (2) Joint Intelligence Support Concept
JISE	Joint Intelligence Support Element
JISI	Joint Intelligence System Integration
JISS	Japan Intelligence Support System
JITAP	Joint Intelligence Training Activity Pacific
JITC	Joint Interoperability Test Center (DISA)
JITF	Joint Integration Testing Facility
JIVA	Joint Intelligence Virtual Architecture
JLA	Joint Logistics Assessment
JLARG	Joint Logistics Assessment Review Group
JL-COE	Joint Logistics Center of Excellence
JLD	Joint Liaison Detachment
JLE	Jammer Locator Electronics
JLMIS	Joint Logistics Management Information System

Page 3381 of 3957

JLOTS	Joint Logistics Over the Shore
JLPPG	Joint Logistics and Personnel Policy and Guidance
JLRC	Joint Logistics Readiness Center
J4/LRC	Joint Logistics Readiness Center
JLREID	Joint Long-Range Estimating Intelligence Document (JSPS)
JLRSA	Joint Long-Range Strategic Appraisal
JLSP	Joint Logistics Steering Panel
JM	Joint Mission
JMA	(1) Joint Mobilization Augmentation; (2) Joint Mission Analysis
JMAT	Joint Mobility Assistance Team
JMC	Joint Movement Center
JMCC	(1) Joint MC&G Coordination Center; (2) Joint Mobile Command Center
JMCIS	Joint Maritime Command Information System
JMEM	Joint Munitions Effectiveness Manual
JMENS	Joint Mission Element Needs Statement
JMETL	(1) Joint Mission Essential Target List; (2) Joint Mission Essential Task List
JMI	JTIDS Modular AOC Integration System
JMIC	Joint Military Intelligence College
JMICS	JWICS Mobile Integrated Communications System
JMIE	Joint Maritime Information Element
JMIE/JEM	JMIE Support System and Modernization
JMINI	Joint UHF MILSATCOM Network Integrated
JMIP	Joint Military Intelligence Program
JMISE	Joint Military Intelligence Support Element
JMITC	Joint Military Intelligence Training Center
JMNS	Joint Mission Needs Statement
JMO	Joint Management Office
JMOCC	Joint Mobile Operations Command Center
JMP	(1) Joint Manpower Program; (2) Joint Mobilization Program
JMPAB	Joint Material Priorities Allocation Board
JMPP	Joint Munitions Production Panel
JMRR	Joint Military Readiness Review
JMSDF	Japan Maritime Self-Defense Force
JMSIP	Joint Modeling and Simulation Integration Program
JMSNS	Justification for Major System New Start
JMST	Joint Management Support Tool
JMTB	Joint Military Transportation Board
JMTG	(1) Joint Military Terminology Group; (2) Joint Master Training Guide
JMTK	Joint Mapping Tool Kit
JNACC	Joint Nuclear Accident Coordinating Center
JNAF	Yugoslavia National Air Force
JNC	Jet Navigation Chart

Page 3382 of 3957

JNC-A	Jet Navigation Chart-Air
JNIDS	(1) Joint National Intelligence Dissemination System; (2) Joint National Intelligence Development Staff
JNPE	Joint Nuclear Planning Element
JOA	Joint Operations Area
JOC	Joint Operations Center
JOC/INT	Joint Operations Center/Intelligence Team
JOG	Joint Operations Graphic
JOG-A	Joint Operations Graphic-Air
JOG-C	Joint Operations Graphic-Combined
JOG-G	Joint Operations Graphic-Ground
JOG-R	Joint Operations Graphic-Radar
JOIC	Joint Operational Intelligence Center/Cell
JOIN	Joint Operations Intelligence Network
JOINT REDTRAIN	Joint Readiness Training
Joint STARS	Joint Surveillance Target Attack Radar System
JOP	Joint Operating Procedure
JOPES	Joint Operations Planning and Execution System
JOPS	Joint Operational Planning System
JOS	Joint Operational Stocks
JOSE	Joint Operations Support Element
JOTS	Joint Operational Tactical System
JP	(1) Jet Petroleum; (2) Joint Publication
JPAM	Joint Program Assessment Memorandum
JPAT	Joint Planning and Assistance Team
JPD	Joint Planning Document
JPEA	Joint Planning and Exercise Activity
JPEC	Joint Planning and Execution Community
JPL	Jet Propulsion Laboratory
JPM	Joint Program Manager
JPMIE	Joint Program for Military Intelligence Education
JPMO	Joint Program Management Office
JPN	JSIC Peterson Node
JPO	Joint Project Office
JPOTF	Joint Psychological Operations Task Force
JPOTG	Joint Psychological Operations Task Group
JPPR	Joint Planning and Program Review
JPRS	Joint Publications Research Service
JPSD	Joint Precision Strike Demonstration
JPSS	Joint Planning Staff for Space
JPSIO	Joint Precision Strike Integration Office
JRA	Joint Rear Area
JRB	Joint Reconnaissance Board
JRC	(1) Joint Reconnaissance Center; (2) Joint Recovery Center
JRCB	Joint Reconnaissance Coordination Board

Page 3383 of 3957

JRCC	Joint Rescue Coordination Center
JRCP	Joint Readiness Command Program
JRDC	Joint Regional Defense Command
JRDOD	Joint Research and Development Objectives Document
JRFL	Joint Restricted Frequency List
JRIP	Joint Reserve Intelligence Program
JRMB	Joint Requirements and Management Board
JRO	Joint Reconnaissance Office
JROC	Joint Requirements Oversight Council
JROC-B	Joint Refugee Center, Berlin
JRS	Joint Reporting System/Structure
JRSC	Jam-Resistant Secure Communications
JRTC	(1) Joint Readiness Training Center; (2) Joint Regional Training Center
JRTC-IS	JRTC Instrumentation System
JRX	Joint Readiness Exercise
JRX MILES	JRX Milestone System
JS	Joint Staff
J/S	Ratio of received power level of a jamming signal and a desired signal
JSAJAC	Security Activity
JSAC	Joint State Area Command
JSAM	Joint Security Assistance Memorandum
JSAMSA	Joint Security Assistance Memorandum Supporting Analysis
JSB	Joint Synthetic Battlespace
JSC	(1) Lyndon B. Johnson Space Center; (2) Joint Spectrum Center
JSCP	Joint Strategic Capabilities Plan
JSCS	Joint Strategic Connectivity Staff
JSDF	Japanese Self-Defense Forces
JSEAD	(1) Joint Surveillance Enemy Air Defense; (2) Joint Suppression of Enemy Air Defenses
JSFC	Joint Space Fundamentals Course
JSIC	Joint SPACECOM Intelligence Center
JSIMS	Joint Simulation System
JSIOC	Joint Space Intelligence Operations Course
JSIOPC	Joint Space Intelligence Operations Policy Course
JSIP	Joint Services Imagery Processor
JSIPS	Joint Service Imagery Processing System
JSIPS-N	Joint Service Imagery Processing System-Navy
JSMB	Joint Space Management Board
JSO	(1) Joint Staff Office; (2) Joint Support Office
JSOA	(1) Joint Special Operations Agency; (2) Joint Special Operations Area
JSOACC	Joint Special Operations Air Component Commander
JSOC	(1) Joint Special Operations Center; (2) Joint Strategic Operations Center; (3) Joint Special Operations Command

Page 3384 of 3957

JSODC	Joint Special Operations Deception Course
JSOFI	Joint Special Operations Forces Institute
JSOIC	Joint Special Operations Intelligence Course
JSOIT	Joint Special Operations Intelligence Training
JSOIO	Joint Special Operations Intelligence Orientation
JSOP	Joint Strategic Objectives Plan
JSOPW	Joint Special Operations Planning Workshop
JSOR	Joint Service Operational Requirement
JSOSOC	Joint Special Operations Staff Officer Course
JSOTF	Joint Special Operations Task Force
JSOTFSO	Joint Special Operations Task Force South
JSOTP	Joint Special Operations Training Project
JSOW	Joint Standoff Weapon
JSPD	Joint Strategic Planning Document
JSPDSA	Joint Strategic Planning Document Supporting Analysis
JSPO	Joint System Program Office
JSPS	Joint Strategic Planning System
JSR	(1) Joint Strategy Review; (2) Joint Special Reports
JSRC	Joint Search and Rescue Center
JSS	(1) Joint Surveillance System; (2) JMIE Support System
JSST	(1) Joint Space Support Team; (2) Joint Special Support Team
JSTARS	Joint Surveillance and Target Attack Radar System
JSTPS	Joint Strategic Target Planning Staff
JSWG	(1) J-TENS Special Working Group; (2) Joint Service Working Group
JT	Joint
JTA	(1) Joint Task Analysis; (2) Joint Table of Allowances
JTAGS	Joint Tactical Ground Station
JTAO	Joint Tactical Air Operations
JTARS	Joint Tactical Aerial Reconnaissance System
JTASC	Joint Training, Analysis and Simulation Center
JTB	(1) Joint Transportation Board; (2) Joint Targets Board
JTC	(1) Joint Target Committee; (2) Joint Technology Center; (3) JFACC Target Cell
JTC3A	Joint Tactical Command, Control, and Communications Agency
JTCAE	Joint Tactical Control and Analysis Element
JTCB	Joint Targets Coordination Board
JTCG	Joint Technical Coordinating Group
JTCG(ME)	Joint Technical Coordinating Group (For Munitions Effectiveness)
JTC/SIL	Joint Technology Center/ Systems Integration Laboratory
JTD	Joint Table of Distribution (Manning Authorization for a Joint Organization)
JTDA	Joint Table of Distribution and Allowances
JTEB	Joint Test and Evaluation Board
J-TENS	Joint Tactical Exploitation of National Systems

Page 3385 of 3957

JTENS	Joint-Service Tactical Exploitation of National Systems
JTF	(1) Joint Tactical Fusion; (2) Joint Task Force
JTF-6	Joint Task Force-6
JTF-B	USSOUTHCOM JTF in Honduras
JTFCEM	Joint Task Force Contingency Engineer Manager
JTF-FA	Joint Task Force-Full Accounting
JTF-LOCE	Joint Tactical Fusion-Limited Operational Capability Europe
JTF-PM	Joint Task Force-Panama
JTFPO	Joint Tactical Fusion Program Office
JTF-PP	Joint Task Force PROVIDE PROMISE
JTF-SWA	Joint Task Force-South West Asia
JTFHQ	Joint Task Force Headquarters
JTFP	Joint Tactical Fusion Program
JTFPMO	Joint Tactical Fusion Program Management Office
JTFSO	Joint Task Force South
JTG	Joint Task Group
JTIC	Joint Transportation Intelligence Center
JTID	Joint Digital Team Information Device
JTIDS	Joint Tactical Information Distribution System
JTL	Joint Target List
JTMD	(1) Joint Theater Missile Defense; (2) Joint Table of Mobilization and Distribution
JTN	Joint Targeting Network
JTOSS	Joint Task-Organized Software Subsystem
JTP	Joint Training Plan
JTR	Joint Travel Regulation
JTRU	Joint Transportation Reserve Unit
JTSC	Joint Technology Steering Committee
JTSG	Joint Targets Steering Group
JTT	Joint Tactics Terminal
JTTP	Joint Tactics, Techniques and Procedures
JTWS	Joint Threat Warning System
JTX	Joint Training Exercise
JUAVTC	Joint UAV Training Center
JUDI	Joint Universal Data Interpreter
JULL	Joint Universal Lessons Learned
JULLS	Joint Universal Lessons Learned System
JUMPS	Joint Uniform Military Pay System
JUSMAG	Joint United States Military Advisory Group
JUWC	Joint Unconventional Warfare Command
JUWTF	Joint Unconventional Warfare Task Force
JVIDS	Joint Visual Integrated Display System
JWAC	Joint Warfare Analysis Center
JWARS	Joint Warfare Simulation
JWBCA	Joint Whole Blood Control Agency

Page 3386 of 3957

JWC	(1) Joint Warfare Center; (2) Joint Working Group
JWCA	Joint Warfighting Capability Assessment
JWFC	Joint Warfighting Center
JWG	Joint Working Group
JWICS	(1) Joint Warning Indications Communications System; (2) Joint Worldwide Intelligence Communications System
JWID	Joint Worldwide Interoperability Demonstration
J2X	JTF J2 Support Element

Page 3387 of 3957

K

K	Kelvin (absolute temperature scale)
KAC	Korea Analysis Center
KADIZ	Korean Air Defense Identification Zone
KAIS	Korean Air Intelligence System
KAK	Key-Auto-Key
KAL	Key Asset List
KALCC	Korean Airlift Control Center
KAPP	Key Asset Protection Program
KAWS	Korean Analyst Workstation
KB	(1) Kilobyte; (2) Knowledgeability Brief
Kbps	Kilobits Per Second (also KPS)
KBS	Knowledge-Based System
KBYTES	Kilobytes
KCG	Korean Consultative Group
KCIA	Korean Central Intelligence Agency
KCOIC	Korean Combat/Combined Operations Intelligence Center
KCSS	Korean Combat Support System
KDC	Key Distribution Center
KDEI	Key Defense Estimates Issues
KDIA	Korean Defense Intelligence Agency
KDII	Key Defense Intelligence Issues
KE	Kinetic Energy
KEK	Key Encryption Key
KELP	Kaleidoscope Elint Processor
KEW	Kinetic Energy Weapon
KG	(1) Kilogram; (2) Key Generator
KGB	Committee for State Security (FSU)
KH	Keyhole
KHA	Killed by Hostile Action
KHz	Kilohertz
KIA	Killed in Action
KIA-BNR	Killed in Action, Body Not Recovered
KIAS	Knots Indicated Air Speed
KIES	Kodak Imagery Exploitation System
KIEWS	Kodak Imagery Edit Workstation
KILLREP	Kill Report
KILLSUM	Kill Summary
KILOD	Killed in the Line of Duty
KIP	(1) Key Intelligence Position; (2) Key Indigenous Personnel
KIPPL	Key Intelligence Program Priorities List
KISS	Korean Intelligence Support System
KIWS	KISS Intelligence Workstation
KJ	(1) Kilojoules; (2) Key Judgments

Page 3388 of 3957

KM	Kilometer
KMASE	Key Management Application Service Element
KMC	Key Management Center
KM/HR	Kilometers Per Hour
KMODC	Key Management Ordering and Distribution Center
KMID	Key Management Identification Number
KMP	Key Management Protocol
KMPDU	Key Management Protocol Data Unit
KMR	Kwajalein Missile Range
KMS	Key Management System
KMSA	Key Management System Agent
KMUA	Key Management User Agent
KN	Knot
knots	Nautical Miles per hour
KP	Key Processor
KPH	Kilometers Per Hour
KPK	Key Production Key
KS	South Korea (ROK)
KSA	Knowledge, Skills, and Abilities
KSC	Kennedy Space Center
KSOS	Kernelized Secure Operating System
KT	(1) Kiloton; (2) Knot
KTAS	Knots True Airspeed
KTO	Kuwait Theater of Operations
KTTP	Korean Tactics, Techniques, and Procedures
Ku	A Satellite Frequency Band
KUSLO	U.S. Liaison Office-Kenya
KW	Kilowatt
KWH	Kilowatt Hours
KVG	Key Variable Generator

Page 3389 of 3957

L

LAAIB	Latin American Air Intelligence Brief
LAAM	Light Anti-Aircraft Missile
LAB	Laboratory
LABS	Laboratories
LAD	Launch Assist Device
LADD	Low Angle Drogue Delivery
LAEO	Low-Altitude Electro-Optical
LAEWWING	Light-Airborne Early Warning Wing
LAF	Launch Alert Folder
LAFTA	Latin America Free Trade Association
LAGEOS	Laser Geodynamic Satellite
LAI	(1) Light Armored Infantry; (2) Look-Down Air Intercept
LAL	Library Accessions List
LALO	Low-Altitude Low-Opening
LAM	Louisiana Maneuvers
LAMM	Land Armament and Manpower Model
LAMP	Lockwood Analytical Method for Prediction LAMPS (1) Light Airborne Multipurpose System; (2) LANTCOM Message Processing System
LAN	Local Area Network
LANDCENT	Land Forces Central Region
LANDSAT	Land Satellite (Commercial Multi-Spectral)
LANDSOUTH	Land Forces Southern Region
LANFORSIXTHFLT	Landing Force Sixth Fleet
LANL	Los Alamos National Laboratory
LANT	Atlantic
LANTAF	Atlantic Command Air Forces
LANTAREA	Atlantic Area
LANTCOM	Atlantic Command (now ACOM)
LANTCOMDIS	Atlantic Command Deployable Intelligence System
LANTCOM JIC	Atlantic Command Joint Intelligence Center (AIC)
LANTDAC	Atlantic Command Defense Analysis Center
LANTDIS	USACOM Deployable Intelligence System
LANTFLT	U.S. Atlantic Fleet
LANTIRN	Low-Altitude Navigation and Targeting Infrared System for Night
LANTIS	Atlantic Intelligence Supplement
LANUP	Local Area Network Upgrades
LANWAN	Local Area Network/Wide Area Network
LAR	Laser-Aided Rocket

Page 3390 of 3957

LARB	Light Amphibious Reconnaissance Battalion
LARS	Light Artillery Rocket System
LAS	Land Analysis System
LASA	Light Armed Surveillance Attack
LASER	Light Amplification by Stimulated Emission of Radiation
LASERFAX	Secure System for Transmitting Photos
LASH	Lighter Aboard Ship
LASINT	Laser Intelligence
LASTE	Low-Altitude Safety Targeting Enhancement
LAT	Latitude
LATAM	Latin America
LATIN	Atlantic Command Theater Intelligence Network
LATS	Large Aperture Tracking System
LATWING	Light Attack Wing
LAV	Light Armored Vehicle (non-tactical)
LAW	Light Antitank Weapon
LAWS	Long-Range Cruise Missile Analysis and Warning System
LB	Live Broadcast
Lb	Pound
L-BAND	1 to 2 GHz
LBR	Laser Beam Recorder
lbs (LB)	Pounds
LBSR	Lightweight Battlefield Surveillance Radar
LC	(1) Library of Congress; (2) Line of Contact
LCAC	Landing Craft, Air Cushion
LCC	(1) Amphibious Command Ship; (2) Logistics Coordination Center; (3) Launch Control Center; (4) Land Component Commander
LCC-IC	Amphibious Command Ship-Intelligence Center
LCD	Liquid Crystal Display
LCE	Liaison Coordination Element (Special Operations Liaison Team in Coalition Operations)
LCF	Launch Control Facility
LCM	(1) Medium Landing Craft; (2) Life Cycle Management
LCP	(1) Personnel Landing Craft; (2) Launching Control Post
LCPR	Ramped Personnel Landing Craft
LCS	Low-Cost Satellite
LCSMM	Life Cycle Support Management Model
LCSR	Swimmer Reconnaissance Landing Craft
LCU	(1) Utility Landing Craft; (2) Launch Correlation Unit
LCW	Special Warfare Support Craft
LCWS	Low-Cost Workstation
LD	(1) Line of Departure; (2) Laser Defense
LDC	(1) Less-Developed Country; (2) Local Data Concentrator; (3) Light-Weight Deployable Communication; (4) Land Defense of CONUS

Page 3391 of 3957

LDEF	Long Duration Exposure Facility
LDF	Lightweight Digital Facsimile
LDIS	Library Document Inventory System
LDM	Limited Distance Modems
LDMX	Local Digital Message Exchange
LDR	Low Data Rate
LDS	Laser Detection System
LDSD	Lookdown/Shootdown
LDT	Large Diameter Target
LDX	Long-Distance XEROX
LEA	Law Enforcement Agency
LEAD	(1) Low-Cost Encryption/Authentication Device; (2) List of Emerging Activations and Dispositions
LEAF	Law Enforcement Access Field
LEASAT	(1) Leased Satellite; (2) Leased System
LED	Light Emitting Diode
LEDS	Link 11 Display System
LEM	Land Engagement Model
LEN	Large Extension Node
LENSCE	Limited Enemy Situation Correlation Element
LEP	Linear Error Probable
LEPCU	Lightweight Environmental Protection Combat Uniform
LEO	Low Earth Orbit
LEO COM	Low Earth Orbit Data Communications
LERTCON	Alert Condition
LES	(1) Leading Edge Services; (2) Land Earth Station; (3) Limited Effects Submunition
LEW	Limited Effects Weapons
LEXIS	Meade Data Central Legal Service
LF	(1) Low Frequency; (2) Launch Facility; (3) Landing Force
LF6F	Landing Force 6th Feet
LFC	Large Format Camera
LFICS	Landing Force Integrated Communications System
LFM	Landing Force Manual
LFOC	Landing Force Operations Center
LFOV	Limited Field of View
LFR	Inshore Fire Support Ship
LFRSV	Launch-Fly-Recover Space Vehicle
LFS	Amphibious Warfare Fire Support Ship
LG	ACC Director of Logistics
LGB	Laser-Guided Bomb
LHA	Amphibious Assault Ship (General Purpose)
LHA-IC	Amphibious Assault Ship (General Purpose)-Intelligence Center
LHD	Multi-Purpose Amphibious Assault Ship
L-HOUR	Hour on C-Day when deployment begins

Page 3392 of 3957

LHR	Low Hop Rate
LHW	Lower High Water
LHX	Lightweight Helicopter
LIC	Low-Intensity Conflict
LIDAR	Light Detection and Ranging
LIGHTSAT	Lightweight Satellite
LIMDIS	(1) Limited Dissemination; (2) Limited Distribution
LIME	Laser-Induced Magnetic Emissions
LIMMER	Limited Control of Merchant Shipping
LIN	LANTCOM Intelligence Network
LINCS	Long-Range Intelligence Networked Communications Service
LIR	Launch and Impact Report
LISS	LANTCOM Intelligence Support System
LITE	Laptop Imagery Transmission Equipment
LITES	Laser Intercept and Technical Exploitation System
LITINT	Literature Intelligence
LIVID	Language Identification and Voice Identification
LIWA	Land Information Warfare Activity
LJ	Laser Jet
LKA	Amphibious Cargo Ship
LKG	Loop Key Generator
LL	(1) Landline; (2) Latent Lethal Dose
LLLTV/IR	Low-Light-Level TV/Infrared
LLSO	Low-Level Source Operations (CI/HUMINT)
LLTV	Low-Light-Level Television
LLNL	Lawrence Livermore National Laboratory
LLO	Land Liaison Office
LLW	Lower Low Water
LLVI	Low-Level Voice Intercept
LMBB	GENSER Intelligence Broadcast
LMCC	LOCE Mobile Correlation Center
LMD	Local Management Device
LMD-KP	Local Management Device/Key Processor
LME	Layer Management Entry
LMI	Layer Management Interface
LMR	Land Mobile Radio
LMRDFS	Lightweight Man-Transportable Radio Direction Finding System
LMS	(1) Local Monitor Station; (2) Least Means Squared
LMSR	Large Medium Speed RO/RO
LNA	Low Noise Amplifier
LNE	Liaison Element
LNG	Liquefied Natural Gas
LNIS	Atlantic Command Naval Intelligence Summary
LNO	(1) Limited Nuclear Option; (2) Liaison Officer

Page 3393 of 3957

LNU	Last Name Unknown
LO	(1) Liaison Officer; (2) Low Observables
LO/LO	Lift-On/Lift-Off
LOA	(1) Letter of Agreement; (2) Lead Operational Authority; (3) Letter of Assist
LOAC	Law of Armed Conflict
LOB	Line of Bearing
LOC(S)	(1) Line(s) of Communication; (2) Library of Congress; (3) Launch Operations Center; (4) Liaison Officer Coordinator; (5) Location; (6) ILS Localizer
LOCD	Lines of Communication Designators
LOCE	(1) Limited Operational Capability, Europe; (2) Linked Operations-Intelligence Centers Europe
LOCK	Logical Co-Processing Kernel
LOD	Low-Observable Demonstrations
LOFAR	Low-Frequency Analysis and Recording
LOG	Logistics
LOGCAP	Logistics Civil Augmentation Program
LOGEX	Logistics Exercise
LOGS	Logistics
LOI	(1) Letter of Instruction; (2) Location of Interest
LON	Longitude
LONG	Longitude
LORAD	Long-Range Air Defense
LORAN	Long-Range Navigation
LOROP	Long-Range Oblique Photography
LOROPS	(1) Long-Range Optical System; (2) Long-Range Oblique Photographic Sensor
LOS	(1) Line of Sight; (2) Law of the Sea
LOTS	(1) Lighter Over the Shore; (2) Logistics Over the Shore
LOW	(1) Laws of War; (2) Launch on Warning
LOX	Liquid Oxygen
LP	Listening Post
LPA	Amphibious Personnel Transport
LPAR	Large Phased-Array Radar
LPC	Linear Predictive Coding
LPD	(1) Amphibious Assault Transport Dock; (2) Low Probability of Detection
LPD/I	Low Probability of Detection/Intercept
LPF	Low Pass Filter
LPG	Liquefied Natural Gas
LPH	Amphibious Assault Ship (Helicopter)
LPI	(1) Low Probability Intercept; (2) Lines per Inch
LPO	Leading Petty Officer
LPR	Amphibious Transport (Small)
LPS	(1) Logistics Planning Study; (2) Large Processing Station

Page 3394 of 3957

LPSS	Amphibious Transport Submarine
LPT	Logistics Preparation of the Theater
LRA	Long-Range Aviation (FSU)
LRAA	Long-Range Air Army (FSU)
LRAACA	Long-Range Air-ASW Capable Aircraft
LRAAM	Long-Range Air-to-Air Missile
LRC	(1) Logistics Readiness Center; (2) Logistics Resupply Center; (3) Lesser Regional Contingency; (4) Limited Regional Conflict; (5) Limited Regional Contingency
LRCM	Long-Range Cruise Missile
LRCS	Light-Reaction Communications System
LRE	Launch and Recovery Element
LREO	Long Range Electro-Optical
LRINF	Longer Range Intermediate-Range Nuclear Forces
LRIP	Limited/Low-Rate Initial Production
LRL	Low-Cost Receive Location
LRM	Low-Rate Multiplexer
LRP	(1) Low-Rate Production; (2) Long-Range Plan; (3) Limited Response Package
LRR	Long-Range Reconnaissance
LRRP	Long-Range Reconnaissance Patrol
LRSC	Long-Range Surveillance Company
LRSO	Long-Range Surveillance Out-Post
LRSP	(1) Long-Range Surveillance Plan; (2) Long-Range Systems Plan
LRSPRAC	Long-Range Special Reporting and Coordination
LRSTIA	Long-Range Scientific and Technical Intelligence Assessment
LRSU	Long-Range Surveillance Unit
LRTNF	Long-Range Theater Nuclear Forces
LRU	Line-Replaceable Unit
LSA	(1) Logistics Support Analysis; (2) LAN Systems Administrator
LSB	Lower Sideband
LSC	Linear Shaped Charge
LSCS	Logistics Support Command, Somalia
LSD	(1) Landing Ship, Dock; (2) Lease Separation Distance
LSDV	Swimmer Delivery Vehicle
LSE	Logistic Support Element
LSG	Large-Scale Graphics
LSI	Large-Scale Integration
LSM	Medium Amphibious Assault Landing Ship
LSP	Launch Sequence Plan
LSS	Library Support System
LSSA	Logistic System Support Activity
LSSC	Light Seal Support Craft
LST	(1) Amphibious Vehicle Landing Ship; (2) Local Standard Time
LST-5C	Deployable Satellite Terminal

Page 3395 of 3957

LSV	Light Strike Vehicle
LT	(1) Light Table (2) Light
LTAC	Land Terminal Access Control
LTAS	Lightweight Tactical Army Satellite Communications System
LTBT	Limited Test Ban Treaty
Ltd	Limited
LTDP	NATO Long-Term Defense Program
LTDS	Laser Target Designator System
LTI	Lightweight Thermal Imager
LTID	Laser Target Interface Device
LTIOV	Latest Time Information of Value
LTMS	Light Table Mensuration System
LTOE	Living Table of Organization and Equipment
LUA	Launch Under Attack
LUT	Limited User Test
LVDS	Low-Volume Dissemination System
LW	Low Water
LWA	Light Weight Aircraft
LWIR	Long-Wavelength Infrared
LWM	Lightweight Motor
LWOP	Leave Without Pay
LWR	Lutheran World Relief, Inc
LWT	Amphibious Warping Tug
LZ	Landing Zone
LZCT	Landing Zone Control Team

Page 3396 of 3957

M

3M	Material, Maintenance, Management
M	(1) Meter; (2) Mach; (3) Mega (Million)
M1A1	M1A1 ABRAMS Tank
MA	Mission Assessment
MAA	Mission Area Analysis
MAAG	Military Assistance Advisory Group
MAAP	Master Air Attack Plan
MAB	Marine Amphibious Brigade
MAC	(1) Military Airlift Command (now AMC); (2) Mobile Inshore Undersea Warfare Attack Craft; (3) Multi-Array Correlator; (4) Missile Analysis Center; (5) Mandatory Access Control; (6) Message Authentication Code; (7) Military Areas of Coordination
MAC-IN	Military Airlift Command-Director of Intelligence
MACA	Military Assistance to Civil Authorities
MACCOM	MAC Communications (Network)
MACCS	Marine Aviation Command and Control System
MACDIS	Military Assistance to Civil Disturbances
MACLO	MAC Liaison Officer
MACOM	(1) Major Army Command; (2) Major Command
MACSAT	Multiple Access Communications Satellite
MAD	(1) Magnetic Anomaly Detector; (2) Mutual Assured Destruction
MADP	Military Attache for Defense Programs
MAE	(1) Mean Area of Effectiveness; (2) Medium Altitude Endurance UAV (formerly Tier II)
MAEO	Medium-Altitude Electro-Optical
MAE-UAV	Medium-Altitude Endurance Unmanned Aerial Vehicle
MAF	Marine Amphibious Force
MAFC	MAGTF All-Source Fusion Center
MAG	(1) Marine Aircraft Group; (2) Military Assistance Group; (3) Military Advisory Group; (4) Magnetic
MAGIC	Maritime Air-Ground Intelligence Cell
MAGIIC	Mobile Army Ground Imagery Interpretation Center
MAGIS	Marine Air-Ground Intelligence System
MAGR	Miniature Airborne GPS Receiver
MAG Tape	Magnetic Tape
MAGTF	(1) Marine Air-Ground Task Force; (2) Marine Amphibious Ground Task Force
MAINT	Maintenance
MAIS	Military Airlift Intelligence System
MAISRC	Major Automated Information System Review Council
MAJCOM	(1) Major Air Force Command; (2) Major Command
MAMS	MASINT Automated Management System
MAN	(1) Mandatory Modification; (2) Metropolitan Area Network

Page 3397 of 3957

MANPADS	Manportable Air Defense System
MANPRINT	Manpower and Personnel Integration
MAO	Major Attack Option
MAOC	Modular Air Operations Center
MAP	(1) Military Assistance Program; (2) Ministry of Aviation Industry (USSR); (3) Multiple Aim Point; (4) Master Attack Plan; (5) Materiel Acquisition Process
MAPREQ	Map Requisition System
MARAD	Maritime Administration
MARC	MAC ALCE Reaction Communications System
MARCENT	Marine Forces Central Command
MARCORSYSCOM	Marine Corps Systems Command
MARE	Mission Analysis Report-Electrical
MARECS	Maritime European Communications Satellite
MARDEZ	Maritime Defense Zone
MARDEZLANT	Maritime Defense Zone, Altantic
MARDIV	Marine Division
MARFOR	Marine Forces
MARFOREUR	Marine Forces Europe
MARFOR-K	Marine Forces Korea
MARFORCENT	Marine Forces, Central Command
MARFORLANT	Marine Forces Atlantic
MARFORPAC	Marine Forces Pacific
MARFORSOUTH	Marine Forces, Southern Command
MARG	(1) Marine Amphibious Readiness Group; (2) Marginal
MARINETERP	Westlant Maritime Intelligence Report
MARINTSUM	Maritime Intelligence Summary
MARISAT	Maritime Satellite (COMSAT)
Mark-Up	Detailed Budget Recommendation from a Congressional Committee
MARPAC	Marine Forces Pacific
MARREP	Maritime Report
MARS	(1) Man-hour Accounting and Reporting System; (2) Military Affiliate Radio System; (3) Monthly Aerial Reconnaissance Summary
MART	Mobile Autodin Record/Remote Terminal
MARV	Maneuverable Reentry Vehicle
MAS	(1) Military Airlift Squadron; (2) Measurement and Signature; (3) Message Analysis Server; (4) Military Agency for Standardization
MASDR	Measurement and Signature Data Requirements
MASH	Mobile Army Surgical Hospital
MASINT	Measurement and Signature Intelligence
MASS	(1) Matrix Analysis Subsystem; (2) Missile and Space Summary
MASST	Major Ship Satellite Terminal
MAST	(1) Mobile Ashore Support Terminal; (2) Manual Acquisition Satellite Track; (4) MILSTAR Advanced Satellite Terminals

Page 3398 of 3957

MAT	Medium Assault Transport
MATB	Multi-Spectral Analyst Test Bed
MATC	Armored Troop Carrier, Mini
MATDEV	Materiel Developer
MATRIX	Multi-source Automatic Target Recognition with Interactive Exploitation
MATS	Mobile Automatic Telephone System
MATSYM	Material Symbol
MATT	Multi-Mission Advanced Tactical Terminal
MATWING	Medium Attack Wing
MAU	Marine Amphibious Unit
MAVUS	Maritime Vertical Takeoff and Landing Unmanned Aerial Vehicle System
MAW	(1) Military Airlift Wing; (2) Marine Aircraft Wing
MAWTS	Marine Aviation Weapons and Tactics Squadron
MAXI	Modular Architecture for the Exchange of Intelligence
MB	(1) Megabit; (2) Meteor Burst; (3) Megabits
Mb	Megabyte
MBA	(1) Main Battle Area; (2) Multiple Beam Antennae
MBB	Modular Building Block (of EIF/ECMC)
MBC	Meteor Burst Communications
MBFR	Mutual and Balanced Force Reduction
MBITR	Multiband Inter Team Radio
MBO	Management by Objective
MBMR	Multiband Multimode Radio
MBPS	Megabytes per Second
MBRADIO	Multiband Radio
MBT	Main Battle Tank
MBYTES/Mbyte	Megabytes
MC	(1) Military Committee; (2) Mobility Corridor; (3) Joint Military Intelligence College; (4) Multi-Channel MC&G Mapping, Charting and Geodesy
MCA	(1) Maritime Collection Assets; (2) Military Capabilities Assessment; (3) Military Civil Action; (4) Mission Concept Approval
MCAR	Multi-Channel Acoustic Relay
MCAS	Marine Corps Air Station
MC ASI	Marine Corps Assistant Chief of Staff Intelligence
MCB	(1) Markings Center Brief; (2) Marine Corps Base
MCC	(1) Mobile Command Center; (2) Movement Control Center; (3) Mission Control Complex; (4) Military Coordination Center; (5) Mission Control Cell; (6) Mission Control Center
MCCB	Modification/Configuration Control Board
MCCC	Mobile Consolidated Command Center (USSPACECOM)
MCCP	Marine Corps Campaign Plan
MCCS	Mobile Command and Control System
MCCT	Mobile Command Communications Team
MCDN	Marine Corps Data Network

Page 3399 of 3957

MCDS	Multilateral Counterterrorism Data System
MCE	(1) Mission Control Element; (2) Modular Control Equipment
MCEB	Military Communications Electronics Board
MCG	(1) Magneto Cumulative Generator; (2) Minimum Character Grid; (3) Monitor Control Group; (3) Mapping, Charting, and Geodesy
MCG&I	Mapping, Charting, Geodesy, and Imagery
MCIA	Marine Corps Intelligence Activity
MCM	(1) Mine Countermeasures; (2) Military Committee Memorandum; (3) Multi-Command Manual; (4) Chairman of the Joint Chiefs of Staff Memorandum (Designator)
MCMIP	Marine Corps Master Intelligence Plan
MCO	MASINT Control Officer
MCOO	Modified Combined Obstacles Overlay
MCP	Mobile Command Post
MCR	Military Command Region
MCRB	Military Costing Review Board
MCRC	Master Control and Reporting Center
MCRD	Marine Corps Recruit Depot
MCRP	Mobilization Command Readiness Program
MCS	(1) Mine Countermeasures Support Ship; (2) Military Capabilities Study; (3) Maneuver Control System; (4) Master Control Station; (5) Mission Control Segment
MCSF	Mobile Cryptologic Support Facility
MCSFBN	Marine Corps Security Force Battalion
MCSP	Mobile Communications Support Package
MCST	Magnetic Card Selectric Typewriter (IBM)
MCT	Mobile Communications Terminal
MCTL	(1) Mediterranean Contingency Target List; (2) Military Critical Technologies List
MCU	Mobile Communications/Command Unit
MCW	Modulated Continuous Wave
MD	(1) Military District; (2) Map Distance; (3) Mission Director
MDA	Missile Defense Act of 1991
MDAP	Major Defense Acquisition Program
MDC	(1) Manipulation Detection Code; (2) Message Distribution Center
M-Day	Day on which mobilization begins
MDI	Multidiscipline Interaction
MDCI	Multidisciplinary Counterintelligence
MDCISUM	Multidisciplinary Counterintelligence Summary
MDDS	Modular Digital Dissemination System
MDID	MSE Data Interface Device
M-DITDS	Migration Defense Intel Threat Data System
MDJCS	Memorandum by the Director, Joint Staff for the Joint Chiefs of Staff
MDLX	Military Demarcation Line Extended

Page 3400 of 3957

MDPS	Mission Data Preparation System
MDO JAPAN	Military Defense Office, Japan
MDR	(1) MASINT Data Request; (2) Medium Data Rate
MDS	(1) Mission Dependent Segment; (2) Modular Dissemination System
MDT	Message Distribution Terminal
MDU	(1) Mine Disposal Unit; (2) Mission Data Update
MDW	Military District of Washington
MDZ	Maritime Defense Zone
ME	(1) Middle East; (2) Munitions Effectiveness
MEA	Munitions Effectiveness Assessment
MEAP	Military Economic Advisory Panel
MEB	Marine Expeditionary Brigade
MEBE	Middle East Basic Encyclopedia
MEC	Main Evaluation Center
MECD	Military Equipment Characteristics Document (NATO)
MECH	Mechanized
MECL	Mission Essential Circuits List
MECO	Main Engine Cutoff (Shuttle and Expendable Launch Vehicles)
MECS	Manual ELINT Collection System
Med	Mediterranean
MED	(1) Message Element Dictionary (JINTACCS); (2) Manipulative Electronic Deception; (3) Medical
MED-RES	Medium Resolution
MEDCAP	Medical Civic Action Project
MEDCOM	Medical Command
MEDEVAC	Medical Evacuation
MEDRETE	Medical Readiness Training Exercises
MEDINT	Medical Intelligence
MEECN	Minimum Essential Emergency Communications Network
MEF	(1) Marine Expeditionary Force; (2) Maximum Elevation Figure
MEFCG	MEF Command Group
MEFTL	Middle East Force Target List
MEIF	Master ELINT Intercept File
MECL	Mission Essential Circuits List
MELOS	Mediterranean Littoral OPINTEL Summary
MELT	Maximum Efficiency Language Training
MEM	Mission Effectiveness Model
MENA	Middle East (and) North Africa
MENS	Mission Element Needs Statement
MEO	Medium Earth Orbit
MEP	(1) Ministry of Electronics Industry (FSU); (2) Mission Enhancement Program (AWACS); (3) Management Engineering Plan
MER	(1) Maximum Effective Range; (2) Minimum Essential Requirements

Page 3401 of 3957

MERADCOM	Mobility Equipment Research and Development Command (U.S. Army)
MERCAST	Merchant Ship Broadcast System
MERCO	Merchant Ship Reporting and Control
MERCOSUR/MERCOSUL	Common Market of the South (South American Southern Cone Customs Union)
MERIT	Military Exploitation of Reconnaissance and Intelligence Technology
MERSHIP	Merchant Ship
MESA	Mechanically Steered Antenna
MET	(1) Mobile Exploitation Team; (2) Meteorology; (3) MILSTAR Engineering Development Model Terminal
METCOM	Control of Meteorological Information
METEOSAT	Meteorological Satellite
METL	Mission Essential Task List
METOC	Meteorological and Oceanographic
METSAT	Meteorology Satellite
METT-T	Mission, Enemy, Terrain, Troops and Time Available
MEU	Marine Expeditionary Unit
MEU(SOC)	Marine Expeditionary Unit (Special Operations Capable)
MEWSS	Mobile Electronic Warfare Support System
MEWSS PIP	Marine Electronic Warfare Support System-Product
MF	Medium Frequency
MFC	Multinational Force Commander
MF IDB	Mainframe Integrated Data Base
MFLOPS	Millions of Floating Point Operations per Second
MFO	Multinational Force and Observers
MFP	Major Force Program
MFP2	Major Force Program 2
MFR	(1) Memorandum for Record; (2) Mutual Force Reduction
MFS	(1) Ministry of State Security (East German); (2) Multifunction Switch
MFT	Mission, Functions and Tasks
MG	Machinegun
MGID	Military Geographic Information and Documentation
MGMT	Management
MGPS	Mobile Ground Processing System
MGR	Manager
MGRS	Military Grid References System
MGS	(1) Mission Ground Station; (2) Mobile Ground Station
MGT	(1) Mobile Ground Terminal; (2) Management
MHC	Coastal Mine Hunter
MHD	Magnet-to-Hydrodynamic
MHE	(1) Mechanized Handling Equipment; (2) Message Handling Enhancement; (3) Materiel Handling Equipment
MHOP	Multiple-Hop
MHS	Message Handling System

Page 3402 of 3957

MHV	Miniature Homing Vehicle
MHW	Mean High Water
MHz	Megahertz
mi	Miles
MI	(1) Military Intelligence; (2) Message Indicator
MIA	Missing in Action
MIB	(1) Military Intelligence Board; (2) Military Intelligence Battalion; (3) Management Information Base
MIBNLI	Military Intelligence Battalion, Low Intensity
MIBWG	Military Intelligence Board Working Group
MIC	(1) Mid-Intensity Conflict; (2) Multinational Intelligence Cell; (3) Monolithic Integrated Circuit; (4) Maritime Intelligence Center
MICEP	Military Intelligence Civilian Excepted Career Program
MICNS	Modular Integrated Communications and Navigation System
MICOM	Missile Command (U.S. Army)
MICON	Military ICON
micro	one millionth
MICFAC	Mobile Integrated Command Facility Ashore Center
MICS	MIIDS/IDB Interface to Client/Server
MICV	Mechanized Infantry Combat Vehicle
MID	(1) Military Intelligence Detachment (2) Military Intelligence Digest MIDB Modernized Integrated Data Base; Migratory Integrated Data Base
MID(S)	(1) Military Intelligence Detachments (Strategic); (2) Mobile Imagery Dissemination System
MIDAS	MAXI Intelligence Desktop Application Software
MIDE	Mean Installation Damage Expectancy
MIDEASTFOR	Middle East Force
MI DET	Military Intelligence Detachment
MIDL	Miniature Interoperable Data Link
MIDLANT	Mid-Atlantic
MIDPAC	Mid-Pacific
MIDMS	Machine Independent Data Management System
MIEF	Master Imagery Exchange Format
MIERS	Modernized Imagery Exploitation & Reporting System
MIES	Modernized Imagery Exploitation System
MIFASS	Marine Integrated Fire and Air Support System
MIG	(1) Mikoyan (FSU) Aircraft; (2) Military Intelligence Guide; (3) Military Intelligence Group
MIGP	Military Intelligence Group
MIIA	Medical Intelligence Information Agency (now AFMIC)
MIIDS	Military Intelligence Integrated Data System
MIIDS/IDB	Military Intelligence Integrated Data System/Integrated Database
MIIPS	Military Intelligence Information Processor Subsystem
MIJI	Meaconing, Intrusion, Jamming, and Interference

Page 3403 of 3957

MIJIFEEDER	Meaconing, Intrusion, Jamming, and Interference Report Feeder
MIL	Military
MILAN	International Antitank Guided-Missile System
MILCOM	Military Communications
MILCOMSAT	Military Communications Satellite
MILCON	Military Construction
MILDEP	Military Department
MILGP	Military Group
MILGRPS	Military Advisory Groups
mili	one thousandths
MILNET	(1) Military Logistics Equipment; (2) Military Network
MILOBS	Military Observer(s)
MILPERS	Military Personnel
MILSAT(COM)	Military Satellite (Communications)
MILSPEC	Military Specification
MILSTAR	(1) U.S. Military Communications Satellite Program; (2) Military Strategic and Tactical Relay
MILSTD	Military Standard
MIMES	Multi-Spectral Imagery Materials Exploitation System
MIMI	Multi-Level Interactive Man/Machine Interface
MIMIC	Monolithic Microwave/Millimeter Wave Integrated Circuit
MIMS	Multiple Independent Maneuvering Submissile
min	Minutes
MIN-O	Minimum Weapon for Damage
MINI-DISE	Compact Version of Deployable Intelligence Support Element
MINTERM	Miniature Terminal
MINURSO	United Nations Mission for the Referendum in Western Sahara
MINX	Multi-Media Information Exchange
MIPE	Mobile Intelligence Processing Element
MIO	(1) Missile Intelligence Officer; (2) Counter-Terrorism Database
MIP	(1) Management Implementation Plan; (2) Message Input Processor
MIPE	Mobile Intelligence Processing Element
MIPIR	(1) Multi-Mission Imagery Photographic Interpretation Report; (2) Multi-Source Photo Interpretation Report
MIPR	Military Interdepartmental Purchase Request
MIPS	Million Instructions per Second
MIR	(1) Mission Intercept Report; (2) Morning Intelligence Report
MIRA	Medium-Wave Infrared Acquisition Array
MIRACL	Mid-Infra-Red Advanced Chemical Laser
MIRADCOM	United States Army Missile Research & Development Command
MIRE	Mission Intercept Report-Electrical
MIRF	Mission Information Recording Facility
MIRGS	Multi-Intelligence Reconnaissance Ground Station
MIRS	Miniaturized Imagery Receive System

Page 3404 of 3957

MIRV	Multiple Independently-Targetable Reentry Vehicle
MIS	(1) Management Information System; (2) Military/Monthly Intelligence Summary; (3) Mission Integration Segment
MISE	Military Information Support Element
MISREP	Mission Report
MISSI	Multilevel Information System Security Initiative
MIST	(1) MCCS Intelligence Support Team; (2) Modular Interoperable Support Terminal; (3) Military Information Support Team
MISTE	Miniature Integrated Satellite Terminal Equipment
MIT	Mobile Interrogation Team (HUMINT)
MITASK	Mission Tasking
MITS	(1) Monthly International Terrorism Summary; (2) MAC Imagery Transmission System; (3) Multimedia-Intelligence Tracking Subsystem
MITT	Mobile Integrated Tactical Terminal
MITTS	Mobile Intelligence Tactical Transmission (System)
MIUW	Mobile Inshore Undersea Warfare
MIW	Mine Warfare
MJCS	Memorandum for the Joint Chiefs of Staff
MK-5O	Advance Lightweight Torpedo
MK V	Mark V Special Operations Craft
MLA	Multispectral Linear Array
MLBM	Modern Large Ballistic Missile
MLE	Mobile Logistics Element
MLLW	Mean Lower Low Water
MLM	Military Liaison Mission
MLNIS	Modified Atlantic Naval Intelligence Summary
MLO	Military Liaison Office
MLP	Multi-Line Phone
MLPP	Multilevel Precedence Preemption
MLRP	Marine Corps Long-Range Plan
MLRS	Multiple Launch Rocket System
MLS	(1) Microwave Landing System; (2) Multi-Level Security; (3) Multi-Level Simulcast
MLSATCOM	Military Satellite Communications
MLST	Mobile Logistics Support Team
MLW	Mean Low Water
MM	(1) Millimeter; (2) Million; (3) Manual Morse; (4) Minelayer
MMB	Miniature Multiband Beacon
MMI	Man/Machine Interface
MMIC	Monolithic Microwave Integrated Circuit
MMIS	Military Man in Space
MMP	MAGTF Master Plan
MMS	Multimission Modular Spacecraft
MMU	Manned Maneuvering Unit

Page 3405 of 3957

MMW	Millimeter Wave
MN	Multinational
MNAS	MAXI Network Access System
MNC	Major NATO Command (NATO)
MND	Multi-National Division
MNF	Multi-National Force
MNIC	Multinational Intelligence Cell
MNMIC	Modernized NMIC
MNS	Mission Needs Statement
MNTHS	Months
MNU	Middle Name Unknown
MO	Counter-Terrorism Database
MOA	(1) Memorandum of Agreement; (2) Military Operating Area
MOAF	Mission-Oriented Assessment Framework
MOB	(1) Main Operating Base; (2) Missile Order of Battle; (3) Mobilization
MOBDES	Mobilization Designee (now IMA)
MOBEX	Mobilization Exercise
MOBS	Multiple-Orbit Bombardment System
MOBSTA	Mobilization Station
MOBTDA	Mobilization Table of Distribution and Allowances
MOC	(1) Minister of Communications; (2) Mission Operations Center; (3) Mission Operations Chief
MOD	(1) Ministry of Defense; (2) Mobile Obstacle Detachment
MODA	Ministry of Defense and Aviation
MODCOM	Modular Communications
MODEMS	Modulation/Demodulation Equipment
MODS	Multiple Object Data System
MOE	Measure of Effectiveness
MOGAS	Motor Gasoline
MOICPAC	Maritime Operational Intelligence Center, Pacific
MOJT	Managed On-the-Job Training
MOL	Manned Orbital Laboratory
MOLINK	Moscow/Washington Emergency Communications Link
MOLNIYA	Soviet (FSU) satellite
MOM	Ministry of General Machine Building (FSU)
MOMCOMS	Man-on-the-Move Communications System
MOOTW	Military Operations Other Than War
MOP	(1) JCS Memorandum of Policy; (2) Ministry of Defense Industry (FSU)
MOPOT	Mobile PSYOP Transmitter
MOPP	Mission-Oriented Protective Posture
MOPS	Million Operations per Second
MORL	Manned Orbital Research Laboratory
mort	Mortar

Page 3406 of 3957

MORTREP	Mortar Bombing Report
MOS	(1) Military Occupational Specialty; (2) Maritime Operational Intelligence Summary; (3) Marine Observation Satellite
MOSFET	Metal-Oxide Semiconductor Field-Effect Transistor
MOSS	Manned Orbital Space Station
MOST	Mosaic Optical Sensor Technology
MOSW	Military Operations Short of War
MOT	Military Ocean Terminal
MOTIF	Maui Optical Tracking and Identification Facility
MOU	Memorandum of Understanding
MOUT	Military Operations in Urban Terrain
MOV	Military Owned Vehicle
MP	(1) Military Police; (2) Military Personnel
MP&B	Mission Planning and Briefing
MPA	(1) Maritime Patrol Aircraft; (2) Mission and Payload Assessment; (3) Mission Planning Agent
MPARE	Mission Planning, Analysis, Rehearsal, and Execution System
MPC	(1) Mobile Processing Center; (2) Manpower and Personnel Center; (3) Message Processing Center; (4) Media Production Center
MPDS	Message Processing and Distribution System
MPDT	Message Processing Distribution Terminal
MPEG	Motion Picture Experts Group
MPF	(1) Maritime Prepositioned Force; (2) Message Processing Facility; (3) Mission Planning Folder; (4) Media Production Center
MPF-E	Maritime Prepositioning Force Enhanced
MPI	Mean Point of Impact
MPM	Mission Planning Module
MPN	MSE Packet Network
MPP	Massively Parallel Processing
MPRS	Mission Planning and Rehearsal Segment
MPS	(1) Maritime Prepositioned Ships; (2) Message Processing System; (3) Master Personnel System; (4) Modular Printing System
MPSOC	Multi-Purpose Satellite Operations Center
MPSS	Ministry of Communications Equipment Industry (FSU)
MPWS	Mobile Protected Weapon System
MQS	Military Qualification and Standards System
MR	(1) Military Region; (2) Medium Range; (3) Motorized Rifle
MRB	Motorized Rifle Battalion
MRBM	Medium-Range Ballistic Missile
MRC	(1) Movement Report Center; (2) Military Region Command; (3) Motorized Rifle Company; (4) Major Regional Contingencies; (5) Major Regional Conflict
MRCA	Multirole Combat Aircraft
MRCS	Medium-Resolution Camera System

Page 3407 of 3957

MRD	(1) Mission Rehearsal Device; (2) Motorized Rifle Division
MRDBS	(1) MASINT Requirements Data Base System; (2) Measurement and Signature Intelligence Requirements Database
MRDFS	Man-Transportable Radio Direction-Finding System
MRDC	Missile Research and Development Command (U.S. Army)
MRF	Ministry of Radio Industry (FSU)
MRI	Military-Related Intelligence
MRK	Manual Remote (re)Keying
MRL	(1) Multiple Rocket Launcher; (2) Master Requirements List
MRLS	Multiple Rocket Launcher System
MRLOGAEUR	Minimum Required Logistics Augmentation Europe
MROC	(1) Multiple-Command Required Operational Capability; (2) Minimum Required Operational Capabilities
MRP	Mobilization Readiness Project
MRPE	Mobile Receive Processing and Exploitation
MRR	Motorized Rifle Regiment
MRS	Movement and Reinforcement Study
MRT	(1) Mobile Remote Terminal; (2) Miniature Receiver Terminal
MR-UAV	Medium-Range Unmanned Airborne Vehicle
MRV	Multiple Reentry Vehicle
MRVC	Multi-Rate Voice Card (Red Switch)
ms	Millisecond
MS	(1) Multispectral; (2) Mobilization Station
M&S	Modeling and Simulation
m/s	Meters per Second
MS-DOS	Microsoft Disk Operating System
MSA	(1) Military Strength Assessment; (2) Minimum Safe Altitude
MSAM	Medium Surface-to-Air Missile
MSB	Minesweeping Boat
MSC	(1) Military Sealift Command; (2) Coastal Minesweeper; (3) Major Subordinate Command (NATO); (4) Military Staff Committee
MSCD	Military Support to Civil Defense
MSCS	Multiple Source Correlation System
MSCT	Training Coastal Minesweeper
MSD	(1) Minesweeping Drone; (2) Mensuration Support Data
MSDF	Maritime Self-Defense Force (Japan)
MSE	Mobile/Multi Subscriber Equipment (Network) (U.S. Army)
MSEL	Master Scenario Events List
MSF	(1) Fleet Minesweeper; (2) Mobile Strike Force; (3) Medicines Sans Frontiers
MSG	(1) Marine Security Guard; (2) Military Support Group
Msg	Message
MSGGEN	Message Generator
MSH	Mine Hunter

Page 3408 of 3957

MSI	(1) Inshore Minesweeper; (2) Multi-Spectral Imagery; (3) Multisensor Interpretation
MSIC	Missile and Space Intelligence Center
MSID	Message Identifier
MSIP	(1) Multi-Spectral Image Processor; (2) Multisensored Intelligence Processor
MSK	Minimum Shift Keying
MSL	(1) Missile; (2) Mean Sea Level
MSM	(1) Minesweeper (River); (2) Ministry of Medium Machine Building (FSU)
MSN	Mission
MSO	(1) Ocean Minesweeper; (2) Marine Safety Office; (3) MILSATCOM Systems Office
MSP	Ministry of Shipbuilding Industry (FSU)
MSPB	Merit System Protection Board
MSPF	Marine Special Purpose Forces
MSR	(1) Patrol Minesweeper; (2) Main Supply Route; (3) Missile Site Radar
MSRT	(1) Mobile Subscriber Radio Telephone; (2) Mobile Subscriber Remote Terminal
MSS	(1) Message Support Subsystem; (2) Specialized Minesweeper; (3) Moored Sonobuoy System; (4) Mission-Management Support System; (5) Mission Support System; (6) Multispectral Scanner
MSSC	(1) Medium SEAL Support Craft; (2) Specialized Coastal Minesweeper; (3) MEU Service Support Group
MSSI	Master of Science of Strategic Intelligence
MSSP	Multi-Functional Smart Sensor Packages
MSSS	Maui Space Surveillance System
MST	(1) Mutual Security Treaty; (2) Maintenance Support Team; (3) Miniature Satellite Transceiver; (4) Multiband Satellite Terminal
MSTS	(1) Multisource Tactical System; (2) Multisource Transceiver System
MSU	(1) Major Subordinate Unit; (2) Ministry of the Soviet Union
MSW	MASINT Server/Workstation
MT	(1) Metric Ton; (2) Megaton; (3) Motor Transport; (4) Maintenance Trainer; (5) Machine Translation
MT-LB	Soviet (FSU) Tracked Vehicle
MTA	Maritime Threat Analysis
MTACCS	(1) Marine Tactical Command and Control System; (2) Marine Tactical Air Command Center System
MTAS	Multisensor Target Acquisition System
MTB	Motor Torpedo Boat
MTBF	Mean Time Between Failures
MTBSP	Mobilization Troop Basis Stationing Plan
MTCACS	Marine Corps Tactical Command and Control System
MTCR	Missile Technology Control Regime
MTDS	Military Tactical Data System
MTF	Message Test Format

Page 3409 of 3957

MTG	Master Training Guide
MTH	Memorandum To Holder
MTI	Moving Target Indicator
MTIB	Soviet (FSU) Amphibious Armored Tractor
MTIC	Military Target Intelligence Committee
MTIMS	Military Target Intelligence Management Structure
MTIT	Military Technical Intelligence Team
MTL	Mean Tide Level
MTLR	Moving Target-Locating Radar
MTL(S)	Material(s)
MTMC	Military Traffic Management Command
MTN	(1) Mountain; (2) M22 Tactical Network
MTO	Mission Type Order
MTO&E	Modified Table of Organization & Equipment
MTP	(1) Mission Training Plan; (2) Master Training Plan
Mtr	Motor
MTS	(1) Maritime Tactical Schools (NATO); (2) Man-Transportable SOCRATES; (3) Masked Target Sensor
MTST	Magnetic Tape Selectric Typewriter (IBM)
MTT	(1) Military Training Team; (2) Mobile Training Team
MTTR	Mean Time To Repair
MTZ	Motorized Infantry
MULE	Modular Universal Laser Equipment
MUSARC	Major United States Army Reserve Command
MUSIC	Multi-User Special Intelligence Communications
MUSE	MC&G Utility Software Environment
MUTES	Multiple Threat Emitter System
MUX	Multiplexer
Mvr	Maneuver
MV	Magnetic Variation
MVS	Multiple Virtual Storage
MVS/XA	Multiple Virtual System/Extended Architecture
MW	(1) Mine Warfare; (2) Millimeter Wave; (3) Microwave; (4) Missile Wing
MW/AA	Missile Warning/Attack Assessment
MWC	Missile Warning Center
MWDS	Missile Warning Display Subsystem
MWHQ	Mobile War Headquarters
MWIR	Medium Wavelength Infrared
MWL	Mean Water Level
MWR	Morale, Welfare, and Recreation
MWS	Missile Warning System
MWTGM	Millimeter Wave Terminal Guided Missile
MX	(1) Missile, Experimental; (2) Peacekeeper Ballistic Missile; (3) Mechanized; (4) Mexico; (5) Mission; (6) Maintenance

Page 3410 of 3957

N

N	North
N2	(1) Director of Intelligence (Naval Component); (2) Navy Staff Intellligence Officer
N/A	Not Applicable
NA	Navy
NAA	North Atlantic Alliance
NAADM	North American Air Defense Modernization
NAASW	Nonacoustic Antisubmarine Warfare
NAAWS	NATO Antiair Warfare System
NAB	(1) NATO Air Base Satellite (System); (2) Naval Amphibious Base; (3) Naval Air Base
NAC	(1) North Atlantic Council (NATO); (2) No Apparent Change; (3) National Agency Check; (4) Network Access Controller
NACA	National Advisory Committee for Aeronautics
NACAA	National Advisory Committee for Aeronautics and Astronautics
NACAM	National COMSEC Advisory Memorandum
NACC	Net Assessment Coordinating Committee
NACDF	National Area Coverage Data File
NACIC	National CI Center
NACIPB	National CI Policy Board
NACOB	National CI Operations Board
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NADGE	NATO Air Defense Ground Environment
NADS	North Atlantic Defense System
NAEW	NATO Airborne Early Warning (System)
NAF	(1) Numbered Air Force; (2) Naval Air Facility
NAFI	Non-Appropriated Fund Instrumentality
NAFIS	Naval Forces Intelligence Study
NAI	Named Areas of Interest
NAIC	National Aerospace Intelligence Center
NAK	Negative Acknowledge
NALE	Naval Liaison Element
NAM	(1) Non-Aligned Movement; (2) Naval Armaments Model
NAMSO	NATO Maintenance and Supply Organization
nano	one billionth
NAOB	Naval Air Order of Battle
NAOC	National Airborne Operations Center
NAOS	North Atlantic Ocean Station
NARA	National Archives and Records Administration
NARRS	NORTHAG Reconnaissance Reporting System

Page 3411 of 3957

NAS	(1) Naval Air Station; (2) Network Access System; (3) National Academy of Science
NASA	National Aeronautics and Space Administration
NASACOM	NASA Communications Network
NASF	NIC Analyst Support Facility
NASIC	North American Air Sovereignty Intelligence Capability
NASP	National Aerospace Plane
NAT	Not Air-Transportable
NAT'L	National
NATO	North Atlantic Treaty Organization
NATO ASWCS	Anti-Surface Warfare Combat System
NAV	(1) Navigation; (2) Navy
NAVAIR	Naval Air Systems Command
NAVAL AIRSHIP	Naval AIRSHIP Radar Surveillance System
NAVASTROGRU	Naval Astronautics Group
NAVATAC	Navy Antiterrorist Alert Center
NAVCAMS	Naval Communications Area Master Station
NAVCENT	U.S. Naval Forces Central Command
NAVCOMDET	Naval Communications Detachment
NAVCOMPARS	Naval Communications Processing and Routing System
NAVCOMTELCOM	Naval Computer and Telecommunications Command
NAVCOMSTA	Naval Communication Station
NAVDAC	Naval Data Automation Command
NAVELEX	Naval Electronic Systems Command
NAVEUR	U.S. Naval Forces, Europe
NAVFAC	(1) Naval Facility; (2) Naval Shore Facilities
NAVFOR	Naval Forces
NAVFORK	Naval Forces Korea
NAVIDS/SIS	Navigational Aids/Selective Identification System
NAVINTCOM	Naval Intelligence Command
NAVLGRU	Naval Liaison Group
NAVMACS	Navy Modular Automated Communications System
NAVMIC	Naval Maritime Intelligence Command
NAVMAP	Navy Missile Analysis Program
NAVMARINTCEN	Naval Maritime Intelligence Center
NAVMAT	Naval Material Command
NAVNET	Navy Data Network
NAVOCEANCOMDET	Naval Oceanography Command Detachment
NAVOCEANO	Naval Oceanographic Office
NAVOCFORMED	Naval On-Call Force for the Mediterranean (NATO)
NAVOPINTCEN	Naval Operations Intelligence Center
NAVPGSCHOOL	Naval Postgraduate School
NAVRADSTA	Naval Radio Station
NAVRES	Naval Reserve
NAVS	Navigators

Page 3412 of 3957

NAVSAT	Navigation Satellite
NAVSATCOMFAC	Naval Satellite Communications Facility
NAVSEA	Naval Sea Systems Command
NAVSEC	Naval Ship Engineering Center
NAVSECGRU	Naval Security Group
NAVSECGRUACT	Naval Security Group Activity
NAVSECGRUCOM	Naval Security Group Command
NAVSECSTA	Naval Security Station
NAVSO	Naval Forces, South
NAVSOC	Naval Special Operations Command
NAVSOF	Naval Special Operations Forces
NAVSOUTH	Naval Forces, Southern Command
NAVSPACECOM	Naval Space Command
NAVSPASUR	Naval Space Surveillance Activity
NAVSPAWAR	Naval Space and Warfare Systems Command
NAVSPECWARCEN	Navy Special Warfare Center
NAVSPECBOATRON	Navy Special Boat Squadron
NAVSPECWARCOM	Naval Special Warfare Command
NAVSPECWARDEVGRU	Naval Special Warfare Development Group
NAVSPECWARGRU	Naval Special Warfare Group
NAVSPECWARUNIT	Naval Special Warfare Unit
NAVSPOC	Naval Space Operations Center
NAVSTA	Naval Station
NAVSTAR	Navigation and Satellite Timing and Ranging
NAVSTAR USER EQUIP	NAVSTAR User Equipment
NAVSUPACT	Naval Support Activity
NAVTECHINTCEN	Naval Technical Intelligence Center
NAVTELCOM	Naval Telecommunications Command
NAVWARCOL	Naval War College
NAWAS	National Attack Warning System
NAWC-AD	Naval Air Warfare Center-Aircraft Division
NAWS	NORAD Attack Warning System
NB	Naval Base
NBC	(1) Nuclear/Biological/Chemical; (2) National Broadcasting Corporation
NBCE	Nuclear, Biological, Chemical Element
NBCWRS	NORAD - Nuclear, Biological, and Chemical Warning Reporting
NBK	Non-Battle Killed
NBRG	National Basic Reference Graphic
NBS	National Bureau of Standards
NC	(1) No Change; (2) Node Center; (3) Narrow Coverage
NCA	National Command Authority(ies)
NCAPS	Naval Controls and Protection of Shipping
NCB	Nuclear Contingency Branch

Page 3413 of 3957

NCC	(1) Naval Component Command; (2) Navy Command Center; (3) Net Control Center
NCCD	Nuclear Command and Control Document
NCCOSC	Naval Command, Control, and Ocean Surveillance Center
NCCS	Naval Command and Control System
NCDU	Naval Combat Demolition Unit
NCEUR	NSA/CSS Europe
NCIC	National Crime Information Center
NCIS	(1) Non-Communications Intercept System; (2) National Counterintelligence Strategy; (3) Naval Criminal Investigative Service
NCIS-E	NCIS-Europe
NCISFO	NCIS Field Office
NCISRA	NCIS Resident Agent
NCISRU	NCIS Resident Unit
NCMA	National Command and Military Authority
NCMC	National Collection Management Cell
NCMP	Navy Capabilities and Mobilization Plan
NCO	Non-Commissioned Officer
NCOA	(1) Non-Commissioned Officers' Academy; (2) Non-Commissioned Officers' Association
NCOC	NORAD Combat Operations Center
NCOES	Non-Commissioned Officers' Educational System
NCOIC	Non-Commissioned Officer in Charge
NCOS	Naval Control of Shipping
NCP	Nuclear Contingency Plan
NCPS	Nuclear Contingency Planning System
NCR	(1) National Capital Region; (2) NSA/Cryptologic Support Service Representative; (3) National Cryptologic Representative; (4) NSA/Central Security Service Representative
NCS	(1) National Communications System; (2) NMIC Control Subsystem; (3) Naval Control of Shipping; (4) Network Control Station; (5) Node Center Switch; (6) National Cryptologic School; (7) Net Control Station
NCSC	(1) Navy Command Support Center; (2) National Computer Security Center
NCSE	NIST Communications Support Element
NCSO	Naval Control of Shipping Office
NCSRT	Non-Communications Signal Recognition Trainer
NCTAMS	Navy Computer and Telecommunications Area Master Station
NCTC	Naval Computer and Telecommunications Center
NCTR	Non-Cooperative Target Recognition
NCTS	Naval Computer and Telecommunications Station
NCWA	NATO Civil Wartime Agency
NCWG	National Correlation Working Group
NCWR	Non-Codeword Reporting
ND	Deputy CINCNORAD

Page 3414 of 3957

NDA	Nondisclosure Agreement
NDAA	Non-Developmental Airlift Aircraft
N-Day	Days Before D-Day
NDB	Non-Direction Beacon
NDCDB	National Digital Cartographic Database
NDCP	Navy Decision Coordinating Paper
NDD	Nuclear Detection Device
NDDS	Nuclear Detonation Detection System
NDGZ	National Desired Ground Zero
NDHQ	National Defense Headquarters (Canada)
NDI	Non-Developmental Item
NDIC	National Drug Intelligence Center
NDL	(1) Network Data Language; (2) National DGZ List
NDOC	National Defense Operations Center
NDP	(1) National Disclosure Policy; (2) Naval Doctrine Publication
NDPC	National Disclosure Policy Committee
NDPO	National Disclosure Policy Office(r)
NDRF	National Defense Reserve Fleet
NDS	(1) Nuclear Detection Satellite; (2) NPIC Data System; (3) Nuclear Detection System
NDU	National Defense University
NEA	(1) Northeast Asia; (2) National Education Association
NEACP	National Emergency Airborne Command Post
NEADS	Northeast Air Defense Sector
NEANMCC	Navy Element Alternate National Military Command Center
NEC	(1) Naval Enlisted Code; (2) Northern European Countries; (3) Navy Enlisted Classification
NEIC	USAFE NATO Equipment Interpretation Course
NEMVAC/NISH	Non-combatant Emergency Evacuation/NEO Intelligence Support Handbook
NEL	National Exploitation Laboratory
NEO	Noncombatant Evacuation Operation
NEOPACK	NEO Package
NEPA	National Environmental Policy Act
NEREP	Nuclear Execution and Reporting Plan
NES	Network Encryption System
NESDIS	National Environmental Satellite Data and Information Service
NESEA	Naval Electronic Systems Engineering Activity
NESN	NATO English-Speaking Nations
NESP	Navy EHF SATCOM Program
NET	(1) Not Earlier Than; (2) New Equipment Training
NETS	Nationwide Emergency Telecommunications Service
NETT	New Equipment Training Team
NEXIS	Meade Data Center News Service
NF	No Foreign Dissemination, NOFORN

Page 3415 of 3957

NFA	(1) New Fighter Aircraft; (2) No Forwarding Address; (3) No-Fire Area
NFAC	National Foreign Assessment Center
NFCS	Nuclear Forces Communications Satellite
NFD	No Foreign Dissemination
NFDP	National Foreign Disclosure Policy
NFE	Network Front End
NFI	(1) Not Further Identified; (2) No Further Information
NFIB	National Foreign Intelligence Board (formerly USIB)
NFIC	National Foreign Intelligence Council
NFIP	National Foreign Intelligence Program
NFL	New Foreign Launch
NFM	Near-Full-Motion
NFS	Network File System
NFSN	NATO French-Speaking Nations
NFWS	Navy Fighter Weapons School
NFZ	Nuclear Free Zone
NG	National Guard
NGA	NATO Guidelines Area
NGAZ	NATO Gazetteer
NGB	National Guard Bureau
NGF	Northern Group of Forces (Soviet Forces in Poland)
NGFS	Naval Gunfire Support
NGIC	National Ground Intelligence Center
NGL	Natural Gas Liquids
NGO	Non-Governmental Organization(s)
NGS	National Ground Site
NHCD	National HUMINT Collection Directive(s)
NHCP	National HUMINT Collection Plan
NHO	Naval Hydrographic Office
NHRTC	National HUMINT Requirements Tasking Center
NIA	National Imagery Agency
NIAC	(1) National Information & Analysis Center; (2) Naval Intelligence Automation Command
NIAG	NATO Industrial Advisory Group
NIC	(1) Naval Intelligence Command; (2) National Intelligence Council; (4) Naval Intelligence Cell; (5) National Intelligence Cell/Community
NICCIA	National CI Coordinating Authority
NICKA	Nickname and Exercise Term System
NICOLS	NIC On-Line System
NICS	NATO Integrated Communications System
NICSCOA	NATO Integrated Communications System Central Operating Authority
NID	National Intelligence Daily
NIDS	NMCC Information Display System

Page 3416 of 3957

NIE	National Intelligence Estimate
NIEO	New International Economic Order
NIETB	National Imagery Exploitation Target Base
NIETS	National Imagery Exploitation Tasking Study
NIEX	No-notice Interoperability Exercise
NIG	National Input Group
NIHS	NAVEUR Intelligence Highlights Summary
NII	National Information Infrastructure
NIIC	NORAD Intelligence Indications Center
NIIDTS	Naval Intelligence Imagery Data Transmission System
NIIRS	National Imagery Interpretability Rating Scale
NILS	Naval Intelligence Locating Summary
NIM	NORAD Intelligence Memorandum
NIMA	National Imagery and Mapping Agency
NIO	National Intelligence Officer
NIP	(1) Notice of Intelligence Potential; (2) National Intelligence Priorities; (3) NATO Interoperability Plan
NIPIR	Nuclear Immediate Photo Interpretation Report
NIPRNET	Unclassified-but Sensitive (N) Internet Protocol Router Network
NIPS	(1) NMCC Information Processing System; (2) Naval Intelligence Processing System
NIPSSA	Naval Intelligence Processing Systems Support Activity
NIPSTRAFAC	Naval Intelligence Processing Systems Training Facility
NIS	(1) National Intelligence Summary; (2) National Intelligence Survey; (3) Naval Investigative Service; (4) NATO Identification System; (5) NPIC Information System (former NDS); (6) Newly Independent States; (7) National Imagery Segment; (8) National Input Segment; (9) NIPCImagery System; (10) Network Information System
NISAC	National Industrial Security Advisory Committee
NISAM	Naval Intelligence Systems Architecture Manual
NISC	Naval Intelligence Support Center (U.S. Navy) (now NIC)
NISCOM	Naval Investigative Service Command
NISHQ	Naval Investigative Service Headquarters
NISO	Naval Investigative Service Office
NISP	Nuclear Weapons Intelligence Support Plan
NISR	National Intelligence Situation Report
NIST	(1) National Intelligence Support Team; (2) National Institute of Standards and Technology
NIT	National Intelligence Topic
NITF	National Imagery Transmission Format
NITFS	NITF Standard
NIU	Network Interface Unit
NKIL	North Korea Installation List
NKSR	Nonkernel Security Related Software
NLC	National Logistical Command
NLI	Natural Language Interface

Page 3417 of 3957

NLM	Netware Loadable Module
NLP	Natural Language Processing
NLOS	Non-Line-of-Sight Weapon System
NLS	Non-Lethal Submunitions
NLT	Not Later Than
NLZ	No-Loan Zone
NM	Nautical Mile
NMC	(1) Naval Materiel Command; (2) NATO Military Council
NMCC	National Military Command Center
NMCC(A)	National Military Command Center (Alternate)
NMCS	National Military Command System
NMCSSC	National Military Command Systems Support Center
NMD	National Military Defense
NMI	No Middle Initial
NMIC	(1) National Military Intelligence Center (archaic, now NMJIC); (2) National Maritime Intelligence Center
NMICC	NATO Maritime Intelligence Coordination Center
NMICSS	NMIC Support System
NMIS	National Military Intelligence Support
NMIST	National Military Intelligence Support Team
NMITC	(1) Navy-Marine Corps Intelligence Training Center; (2) National Military Intelligence Training Center
NMJCC	National Military Joint Command Center
NMJIC	National Military Joint Intelligence Center
NMN	No Middle Name
NMOSS	NATO Maritime Operational Support System
NMRL	National MASINT Requirements List
NMS	National Military Strategy
NMSD	National Military Strategy Document
NMIC	National Military Intelligence Center
NMICC	National Military Intelligence Collection Center
NMJIC	National Military Joint Intelligence Center
NN	Neural Network
NNA	Neutral and Non-Aligned
NNAG	NATO Naval Armaments Group
NNBIS	National Narcotics Border Interdiction System
NNICP	National Nuclear Intelligence Collection Plan
NNWS	Non-Nuclear Weapons States
NOAA	National Oceanic and Atmospheric Administration
NOB	(1) Naval Order of Battle; (2) Nuclear Order of Battle
NOBS	Naval Operations Bases
NOBTS	Naval Order of Battle Textual Summary

Page 3418 of 3957

NOC	(1) Naval Operations Center; (2) Network Operations Center NOCONTRACT Not Releasable to Contractors or Contractor Consultants
NOD	Night Observation Device
NOE	Nap-of-the-Earth
NOFORN	Not Releasable to Foreign Nationals
NOIAN	National Operations and Intelligence Analysts Net
NOIC	Naval Operational Intelligence Center
NOIWON	National Operations and Intelligence Watch Officers Network
NOK	Next Of Kin
NOMS	Nuclear Operations Monitoring System
NOPF	Naval Ocean Processing Facility
NOR	Norway
NORAD	North American Aerospace Defense Command
NORD	Nordic
NORIP	NORAD Intelligence For Planning Document
NORLANT	North Atlantic
NORMIB	NORAD Missile Intelligence Bulletin
NORSAR	Norwegian Seismic Array
NORSIB	NORAD Weekly Space Intelligence Bulletin
NORTHAG	Northern Army Group
NORTIC	NORAD Tactical Intelligence Cell
NOSC	Naval Ocean Systems Center
NOSG	Naval Operations Support Group
NOSIC	Naval Ocean Surveillance Information Center
NOTAL	Not To All (message distribution restriction)
NPA	New People's Army
NPB	Neutral Particle Beam
NPE	Nuclear Planning and Execution
NPES	Nuclear Planning and Execution System
NPGS	Naval Postgraduate School
NPHR	National Foreign Intelligence Plan for Human Resources
NPIC	National Photographic Interpretation Center
NPR	Nuclear Posture Review
NPS	Nuclear Planning System
NPT	Non-Proliferation (of Nuclear Weapons) Treaty
NR	(1) Research Submarine (Nuclear); (2) Naval Reserve; (3) Non-Recurring; (4) Number
NRAD	NCCOSC Research, Development, Test and Evaluation Division
NRC	National Research Council
NRCC	NORAD Region Combat Center
NRDL	Naval Radiological Defense Laboratory
NRF	Naval Reserve Force
NRFI	Non-Recurring Finished Intelligence
NRI	Net Radio Interference

Page 3419 of 3957

NRIP	Naval Reserve Intelligence Program
NRIS	National Radar Interpretability Scale
NR JOIC	Northwestern Region Joint Operational Intelligence Cell
NRL	(1) Naval Research Laboratory; (2) NUWEP Reconnaissance List; (3) National Receive Location
NRO	National Reconnaissance Office
NROSS	Navy Remote Ocean Surveillance Satellite
NRP	(1) National Reconnaissance Program; (2) Net Radio Protocol
NRT	(1) Near Real Time; (2) Net Registered Tonnage
NRTEM	Near-Real-Time Exploitation Module
NRTI	Near-Real-Time Information
NRTS	Naval Reconnaissance and Technical Support
NSA	(1) National Security Agency; (2) National Shipping Authority; (3) National Standards Association; (4) Naval Support Activity
NSAD	Network Security Architecture and Design
NSA/CSS	National Security Agency/Central Security Service
NSAM	National Security Action Memorandum
NSARC	Navy Systems Acquisition Review Council
NSC	(1) National Security Council; (2) Naval Supply Center
NSC/DC	Deputies Committee of the NSC
NSCID	National Security Council Intelligence Directive
NSCIG	National Security Council Interdepartmental Group
NSD	National Security Directive
NSDD	National Security Decision Directive
NSDM	National Security Decision Memorandum
NSE	(1) Naval Support Element; (2) National Support Element
nsec	Nanosecond
NSEP	National Security Emergency Preparedness
NSF	National Science Foundation
NSFS	National Surface Fire Support
NSG	Naval Security Group
NSGA	Naval Security Group Activity
NSGC	Naval Security Group Command
NSGD	Naval Security Group Detachment
NSI	National Security Information
NSIC	Naval Security and Investigative Command
NSN	National Stock Number
NSNF	Non-Strategic Nuclear Forces
NSO	(1) Non-SIOP Option; (2) Network Security Officer
NSOC	(1) National Security Operations Center (formerly National SIGINT Operations Center); (2) Naval Special Operations Command
NSOF	Naval Status of Forces
NSP	NORAD/USSPACECOM
NISPC	National In-Service Production Centers
NSPG	National Security Planning Group

Page 3420 of 3957

NSRB	National Security Resources Board
NSRDB	National SIGINT Requirements Data Base
NSRDC	Naval Ship Research and Development Center
NSRL	National SIGINT Requirements List
NSRS	National SIGINT Requirements System
NSS	(1) NMIC Support System; (2) National Seismic Station; (3) National Security Strategy; (4) Network Support Server
NSSD	National Security Study Directive
NSSM	(1) Navy Spread Spectrum Modem; (2) National Security Study Memorandum
NSST	(1) Navy Space Command Space Support Team; (2) National Special Support Teams
NSTAC	National Security Telecommunications Advisory Committee
NSTD	(1) National Strategic Target Database; (2) Non-System Training Device
NSTG	Nuclear Strike Target Graphic
NSTGFE	Naval Scientific and Technical Group, Far East
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory/information Memorandum
NSTISSC/D/I/P	National Security Telecommunications and Information Systems Security Committee/Directive/Instruction/Policy
NSTL	National Strategic Target List
NSTS	NSA/CSS Secure Telephone System
NSV	Netted Secure Voice
NSVN	NATO Secure Voice Network
NSW	Naval Special Warfare
NSWC	(1) Navy Surface Weapons Center; (2) Navy Special Warfare Command
NSWDG	Naval Special Warfare Development Group
NSWG	Naval Special Warfare Group
NSWP	Non-Soviet Warsaw Pact
NSWTG	Naval Special Warfare Task Group
NSWTG/U	Naval Special Warfare Task Group/Unit or (Unconventional)
NSWTU	Naval Special Warfare Task Unit
NSWU	Naval Special Warfare Unit
NTA	National Tasking Authority
NTB	(1) National Targeting Base; (2) Nuclear Test Ban
NTBS	National Target Base Server
NTC	(1) National Territorial Command; (2) National Tasking Center; (3) Naval Training Center; (4) Network Terminal Concentrator; (5) National Training Center
NTCB	Network Trusted Computing Base
NTCC	Naval Telecommunications Center
NTCS-A	Naval Tactical Communications System-Afloat
NTDI	NATO Target Data Inventory
NTDS	Naval Tactical Data System
NTF	National Test Facility

Page 3421 of 3957

NTI	(1) National Tactical Interface; (2) Near-Term Initiative
NTIA	National Telecommunications & Information Administration/ Agency
NTIB	NATO Tactical Intelligence Broadcast
NTIC	Naval Technical Intelligence Center
NTIS	National Technical Information Service
NTISSAM	National Telecommunications and Information Systems Security Advisory/information Memorandum
NTISSC/D/I/P	National Telecommunications and Information Systems Security Committee/Directive/Instruction/Policy
NTM	National Technical Means
NTMWG	Nuclear Test Monitoring Working Group
NTP	National Tasking Plan
NTPC	National Telemetry Processing Center
NTPR	Nuclear Targeting Policy Review
NTPS	Near-Term Maritime Pre-Positioning Ships
NTS	(1) Nuclear Test Site; (2) Naval Telecommunications System
NTSC	National Television Standard Code/Committee
NTSDS	National Target/Threat Signatures Data System
NTSS	National Time-Sensitive System
NTU	New Threat Upgrade
NTZ	No Transgression Zone
NUAC	Nicaragua Analysis Cell
NUCAP	Nuclear Capabilities Data Base
NUCDEF	Nuclear Defense
NUCDETS	Nuclear Detonation Detection & Reporting System
NUCINT	Nuclear Intelligence
NUCREP	Nuclear Damage Report
NUCWPN	Nuclear Weapon(s)
NUICCS	NORAD/USSPACECOM Integrated Command and Control System
NUDET	(1) Nuclear Detection; (2) Nuclear Detonation
NUIS	NORAD/USSPACECOM Intelligence Systems
NURAD	Nuclear Radiation Detection
NUREP	Nuclear Weapons Report
NUSC	Naval Underwater Systems Center
NUT	Naval Upper Tier
NUTEX	Nuclear Tactical Exercise
NUWEAMP	Nuclear Weapons Employment and Acquisition Master Plan
NUWEP	Nuclear Weapons Employment Policy/Plan (NCA)
NVDEP	Network Virtual Data Entry Protocol
NVDET	Network Virtual Data Entry Terminal
NVG	Night Vision Goggles
NVIS	(1) Near-Vertical Incidence Skywave; (2) Night Vision Imaging System
NVS	Night Vision System

Page 3422 of 3957

NW	(1) Nuclear Warfare; (2) Northwest (region)
NWB	Nuclear Weapons Branch
NWC	(1) National War College; (2) Naval War College; (3) Naval Weapons Center; (4) NORAD Weather Center
NWFZ	Nuclear Weapons Free Zone
NWIP	Naval Warfare Information Publication
NWIS	Naval Weaponeering Information Sheet
NWL	Naval Weapons Laboratory
NWP	Naval Warfare Publication
NWR	Northwest Region
NWRS	Nuclear Weapons Requirement Study
NWS	(1) Nuclear Weapons State; (2) North Warning System; (3) National Weather Service
NWSS	Nuclear Weapons Storage Site
NWWCSS	Naval Worldwide Command Support System
NX	Non-Expendable

Page 3423 of 3957

O

O/A	On or About
OA	(1) Office Automation; (2) Operations Analysis; (3) Operational Area
OAC	Objective Architecture Center
OAD	(1) Operational Availability Date; (2) Objective Architecture Document
OAD-2	Objective Architecture Document, 2nd Iteration
OADR	Originating Agency's Determination Required
OALAN	Office Automation Local Area Network
OAMP	Optical Airborne Measurements Program
OAP	(1) Organizational Assessment Package; (2) Offset Aim Point
OAPEC	Organization of Arab Petroleum-Exporting Countries
OAS	(1) Organization of American States; (2) Offensive Air Support
OASA(RDA)	Office of the Assistant Secretary of the Army (Research, Development, and Acquisition)
OASD	Office of the Assistant Secretary of Defense
OASD(C3I)	OASD (Command, Control, Communications, and Intelligence)
OASIS	(1) Operational Application of Special Intelligence Systems; (2) Office Automation System for Intelligence Support
OATS	(1) Operations Analysis for Tactical Support; (2) Online AIF Transaction System
OAU	Organization of African Unity
OB	Order of Battle
OBC	Optical Bar Camera
OBE	Overtaken By Events
OBI	Observable Human Resources Intelligence
OBI-OC	OBI Operations Center
OBIS	Order of Battle Intelligence System
Obj	Object
OBP	On-Board Processing
OBO	Official Business Only
OBS	(1) Ocean Baseline System; (2) Orders of Battle System; (3) Observations (Optical Tracking)
OBSS	(1) Off-Board Sensor Systems; (2) Operational Briefing Support System
OBSUM	Order of Battle Summary
OBU	OSIS Baseline Upgrade
OC	(1) Dissemination and extraction of Information Controlled; (2) Optical Carrier
O&C	Operations & Control
OCA	(1) Ocean Control Authority; (2) Operational Control Authority; (3) Offensive Counterair
OCAC	Operational Control and Analysis Center
OCAM	Afro-Malagasy and Mauritian Common Organization

Page 3424 of 3957

OCAR	Office, Chief of Army Reserve
OCCIS	Operational Command and Control Information System
OCCULT	Optical Covert Communications Using Laser Transceivers
OCEANLANT	Ocean Atlantic Area (NATO)
OCJCS	Office of the Chairman, Joint Chiefs of Staff
OCM	Operational Coordination Message
OCMA	Objective Collection Management Architecture
OCMC	Overhead Collection Management Center
OCNO	Office of the Chief of Naval Operations
OCOKA	Observation and Fields of Fire, Concealment and Cover, Obstacles, Key terrain, Avenues of Approach, and Mobility Corridors
OCONUS	Outside CONUS
OCR	(1) Office of Collateral Responsibility; (2) Optical Character Reader
OCS	(1) Officer Candidate School; (2) Offensive Counterspace
OCS3	Optical Carrier 3 Communications
OCSA	Office of the Chief of Staff of the Army
OCSURV	Ocean Surveillance
OCU	Operational Conversion Unit
OD	Operating Directive(s)
ODA	Operational Detachment Alpha
ODC	Office of Defense Cooperation
ODCSINT	Office of the Deputy Chief of Staff, Intelligence
ODCSLOG	Office of Deputy Chief of Staff for Logistics
ODCSPER	Office of Deputy Chief of Staff for Personnel
ODECA	Organization of Central American States
ODIN	Operations Dedicated Imagery Network (LOCE)
ODISC4	Office of Director Information Systems Command, Control, Communications, Computers
ODJS	Office of the Director, Joint Staff
ODP	(1) Officer Distribution Plan; (2) Office of Defense Planning
ODRP	Office of the Defense Representative - Pakistan
ODS	(1) Open Data Server; (2) Operation DESERT STORM; (3) Output Data Server
OE	Operational Effectiveness
OECD	Organization for Economic Cooperation and Development
OEE	Operational ELINT Exploitation
OEF	Operational Exploitation Facility
OEG	Operational Exposure Guide
OEIC	Overseas Economic Intelligence Committee
OER	(1) Officer Evaluation Report; (2) Officer Efficiency Report; (3) Operational ELINT Requirements
OET	Office of Emergency Transportation
OFC	Office
OFCO	Offensive Counterintelligence Operation
Off	Officer

Page 3425 of 3957

OFM	Office of Foreign Mission
OGOOI	Operations Group Operations Officer Intelligence (Air Force)
OGS	Overseas Ground Station
OGSI	Operations Group Support Intelligence (Air Force)
OHD	Over-the-Horizon Detection Radar
OHD-B	Over-the-Horizon Detection Radar-Backscatter
OI	(1) Operating Instruction; (2) Operational Interest
O&I	Operations & Intelligence
OIA	(1) Office of Imagery Analysis; (2) Operations Intelligence Automation
OIC	Officer in Charge
OICC	(1) Operational Intelligence Crisis Center; (2) Operational Intelligence Coordination Center
OICS	Operational Intelligence Collection System
OII	Operations-Intelligence Interface
OILO	Operations Intelligence Liaison Officer
OIP	(1) Offset Instrumentation Point; (2) Operator Interface Processor
OIR	Operational Intelligence Requirement
OISS	Operational Intelligence Support System
OIW	OII Workstation
OJCS	(1) Organization of the Joint Chiefs of Staff; (2) Office of the Joint Chiefs of Staff
OJT	On-the-Job Training
OL	Operating Location
OLC	Oak Leaf Cluster
OM	Operations Module
O&M	Operation and Maintenance
OMA	(1) Office of Military Affairs (CIA); (2) Operations and Maintenance, Army
OMAR	Operations and Maintenance Army Reserve
OMAT	Ocean Measurements and Array Technology
OMB	Office of Management and Budget
OMC	Office of Military Cooperation
OMC-K	Office of Military Cooperation-Kuwait
OMG	Operational Maneuver Group (FSU)
OMNG	Operation and Maintenance, National Guard
OMOB	Offensive Missile Order of Battle
OMV	Orbital Maneuvering Vehicle
ON	Original Negative (film)
ONA	Australia Office of National Assessments
ONC	Operational Navigation Chart
ONI	Office of Naval Intelligence
ONIR	Overhead Non-Imaging Infrared
ONLEXKED	On-Line Five Year Exercise Schedule System
ONOO	Outline NATO Operational Objective

Page 3426 of 3957

ONPG	Operational Nuclear Planning Group
ONR	Office of Naval Research
ONS	Operational Needs Statement
ONUC	United Nations Operations in the Congo
ONUMOZ	United Nations Operations in Mozambique
ONUSAL	United Nations Observer Mission in El Salvador
OOA	Out of Area
OOB	Order of Battle
OODA	Observation, Orientation, Decision and Action
OOK	On/Off Keying
OOP	Object Oriented Programming
OOTW	Operations Other Than War
OP	(1) Observation Post; (2) Operation; (3) Operational
OPA	Other Procurement Activity
OP3	Overt Peacetime PSYOP Program
OPCC	Offutt Processing and Correlation Center
OPCEN	Operations Center
OPCODES	Operational Codes
OPCOM	Operational Command
OPCON	Operational Control
OPDEC	Operational Deception
OPEC	Organization of Petroleum-Exporting Countries
OPELINT	Operational Electronic Intelligence
OPF	Orbiter Processing Facility
OPFAC	Operational Facilities
OPFIS	Operational Foreign Instrumentation Signals
OPFOR	Opposing Forces
OPG	Operations Planning Group
OPI	Office of Primary Interest
OPIC	(1) Overseas Processing and Interpretation Center; (2) Overseas Private Investment Corporation
OPIC-A	Overseas Processing and Interpretation Center - Asia
OPINT	Optical Intelligence
OPINTEL	Operational Intelligence
OPLAN	Operations Plan
OPM	Office of Personnel Management
Opn(s)	Operation(s)
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	OPNAV Instruction
OPNOTES	Operational Notes
OPORDER/OPORD	Operations Order
OPPAR	Opposing Army
OPR	Office(r) of Primary Responsibility; Officer Performance Report
OPREP	Operations Report
OPREPS	Operational Reporting System

Page 3427 of 3957

OPS/OPNS/OP	Operations
OPS/INTEL	Operations Intelligence
OPSDEPS	Operations Deputies (JCS)
OPSCO	Operations Coordinator
OPSCOM	Operations Committee
OPSCOMM	Operations Secure Communications
OPSEC	Operations Security
OPSKAN	Open Skies Advanced Notice
OPSNOTE	Operations Note
OPT	(1) Optional Modification; (2) Operations Planning Team
OPTEMPO	Tempo of Operations
OPTEVFOR	Operational Test and Evaluation Force
OPTINT	Optical Intelligence
OPTIR	Optical Infrared
OPUS	OBU Program Upgrade System
OR	(1) Operational Requirements; (2) Operationally Ready
ORBINT	Orbital Intelligence
ORBIT	System Development Corporation Data Search Service
ORCON	(1) Dissemination and Extraction of Information Controlled by Originator; (2) Originator Controlled
ORD	Operational Requirements Document
ORE	Operational Readiness Exercise
ORF	Official Representation Fund
Org	Organization
ORI	Operational Readiness Inspection
OS	(1) Operating System; (2) Cryptologic Officer
O&S	Operations & Support
OSA	Open Systems Architecture
OSAP	Ocean Surveillance Assessment Program
OSAS	Operational Space Application System
OSC	(1) Office of the Security Council; (2) Operational Support Company; (3) Operations Support Center; (4) On-Scene Commander
OSCAR	Optical Submarine Communications by Aerospace Relay
OSCARCP	Operations Support Center and Rear Command Post (Korea)
OSD	Office of the Secretary of Defense
OSD(C)	OSD (Comptroller)
OSF	Open Systems Foundation
OSI	(1) Operating Systems Incorporated (Contractor); (2) On-Site Inspection; (3) Off-Shore Islands; (4) Office of Special Investigations; (5) Open System Interconnect; (6) Office of Special Investigations; (7) Open System Interconnect
OSIA	On Site Inspection Agency
OSINT	Open Source Intelligence
OSIS	(1) Ocean Surveillance Information System; (2) Open Source Information Service
OSP	(1) Ocean Surveillance Product; (2) Operational Support Package

Page 3428 of 3957

OSPRA	Ocean Surveillance Pattern Recognition Algorithm
OSO	Operational Support Office
OSP	Operational Support Packages
OSS	(1) Operational Storage Site; (2) Operations Support Squadron; (3) Operations Support System
OSSC	On-Line System Support Center
OST	Outer Space Treaty
OSTP	Office of Science and Technology Policy
OT	(1) Overseas Territories; (2) Overtime; (3) Operational Test; (4) One Time; (5) Operations Team
OT&E	Operational Test and Evaluation
OTA	(1) Operational Tasking Authority; (2) Office of Technology Assessment
OTAD	Over-The-Air Key Distribution
OTAR	Over-The-Air Rekeying
OTAT	Over-The-Air Transmission/Transfer
OTAU	Over-The-Air Updating
OTC	(1) Officer in Tactical Command; (2) Over-the-Counter
OTCIXS	(1) Officer in Tactical Command Information Exchange Sub-system; (2) OTC Information Exchange System
OTE	See OT&E
OTEA	Operational Test and Evaluation Agency (U.S. Army)
OTH	Over-the-Horizon
OTH-B	Over-the-Horizon Backscatter
OTH-R	Over-the-Horizon Radar
OTH-T	Over-the-Horizon Targeting
OTIS	Operational Targeting Intelligence System
OTM	On the Move
OTP	One-Time Pad
OTS	(1) One-Time Source; (2) Officer Training School; (3) Oahu Telecommunications System
OTT	One-Time Tape
OTU	Operational Training Unit
OUO	Official Use Only
OUSDRE	Office of the Under Secretary of Defense, Research & Engineering
OUTS	Operational Unit Transportable System
OVOP	Overt Operational Proposal
OVPF	Object-Oriented Vector Product Format

Page 3429 of 3957

P

P	Peacetime
P2E2I	Pre-Planned Essential Elements of Information
P-3H	Land-Based Anti-Submarine Warfare Patrol Aircraft (re-engined)
P3I	Pre-Planned Product Improvement
PA	(1) Pulse Amplitude; (2) Probability of Arrival; (3) Public Affairs; (4) Preliminary Assessment; (5) Proper Authority
PAA	(1) Primary Aircraft Authorized; (2) Peer Access Approval
PA ANG	Pennsylvania Air National Guard
PAATS	Precision Approach Area Tracking System
PABX	Private Access Branch Exchange
PAC	Pacific
PACAF	Pacific Air Forces
PACCAAT	USPACOM Command and Control AUTODIN Access Terminal
PACCS	Post-Attack Command and Control System
PACE	Portable Acoustic Collection Equipment
PACFAST	Pacific Forward Area Support Team
PACFLT	Pacific Fleet
PACOM	U.S. Pacific Command
PACOPS	Pacific Air Force Operations
PACTAIS	Pacific Theater Air Intelligence System
PACTIDS	PACOM Theater Intelligence Data System
PACVTCN	Pacific Video Teleconferencing Network
PAD	Program Action Directive
PADAR	Passive Airborne Detection & Ranging
PA&E	Program Analysis and Evaluation
PAE	Peer Access Enforcement
PAF	Production Analysis and Fusion
PAI	Project Assignment Instruction
PAIDS	PACOM Area Imagery Distribution System
PAIS	(1) Personnel Authentication Identification System; (2) Prototype Advanced Indicator System; (3) Pacific Air Intelligence System
PAL	Permissive Action Link
PALAPA	Indonesian Satellite
PALS	Photo Area & Location System
PAM	(1) Payload Assist Module; (2) Penetration Augmented Munition
PAMIS	Psychological Operations Automated Management Information System
PANAMSAT	PAN American Satellite (Communications System)
PANMAN	Panama Metropolitan Area Network
PAO	(1) Product Activity/Operational Code; (2) Public Affairs Officer
PAOC	PACAF Air Operations Center

Page 3430 of 3957

PAR	(1) Precision Approach Radar; (2) Perimeter Acquisition Radar; (3) Phased-Array Radar; (4) Population at Risk; (5) Program Assessment Review
PARCS	(1) Perimeter Acquisition Radar Attack; (2) Perimeter Acquisition Characterization System
PARINT	Partial Intercept
PARIS	Pacific Army Intelligence System
PARMIS	Peacetime Airborne Reconnaissance Management Information System
PARPRO	(1) Peacetime Aerial Reconnaissance Program; (2) Preplanned Application of Reconnaissance Programs
PAS	(1) Plans and analysis Staff; (2) Pan American Satellite
PASEP	Passed Separately
PASS	(1) Photo Interpretation Analyst Support System; (2) PACOM IPAC Intelligence Computer System Analyst Support System; (3) PACOM ADP Server Site
PASS-E	USPACOM ADP Server Site-EASTPAC
PASSEX	Passing Exercise (Naval)
PASS-H	USPACOM ADP Server Site, Hawaii
PASS-J	USPACOM ADP Server Site, Japan
PASS-K	USPACOM ADP Server Site, Korea
PAT	(1) Payload Associated Transporter; (2) Planning Assistance Team; (3) Process Action Team
PATREP	Patrol Report
PATRIOT	Phased Array Tracking to Intercept of Target
PATRIOT PAC III	Phased Array Tracking to Intercept of Target Advanced Capability III
PATRON	Patrol Squadron (Navy)
PATWING	Patrol Wing
PAVE	USAF Programs Connected (Night) Avionics, Target Designators, Vision
PAWS	(1) Portable Analyst Work Station; (2) Prototype Analytical Workstation; (3) Portable ASAS Workstation
PAX	Passengers
PB	(1) Particle Beam; (2) Patrol Boat
PB(A)(H)	Patrol Boat (Air Cushion) (Hydrofoil)
PBAC	Program Budget Activity Committee
PBC	Program and Budget Committee
PBD	(1) Program Budget Decision; (2) Patrol Boat Drone
PBEIST	Planning Board for European Inland Surface Transport
PBL	Patrol Boat, Light
PBN	Public Broadcasting Network
PBOS	Planning Board for Ocean Shipping
PBR	(1) River/Roadstead Patrol Boat (Navy); (2) Precision Bombing Range
PBTN	Panama Backbone Transport Network
PBV	Post-Boost Vehicle
PBW	Particle Beam Weapon

Page 3431 of 3957

PBX	Private Branch Exchanges
PC	(1) Patrol Craft; (2) Positive Control; (3) Production Control; (4) Personal Computer; (5) Project Coordinator; (6) Parallel Computing; (7) Provide Comfort; (8) Patrol Coastal
PCA	Point of Closest Approach
PCAC	Primary Collection and Analysis Center
PCC	(1) POADS Computer Center; (2) Program Coordinating Committee
PCD	(1) Program Change Decision; (2) Positive Control Document
PCE	Patrol Escort
PCF(A)(H)	Fast Patrol Craft (Air Cushion) (Hydrofoil)
PCFS	Fire Support Patrol Craft
PCH	Patrol Craft (Hydrofoil)
PC II	PROVIDE COMFORT II
PCL	Parallel Communications Link
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PCN	(1) Production Control Number; (2) Packet Switching Node; (3) Personal Communications Networking
PCP	(1) Project Concept Proposal; (2) Program Change Proposal
PCR	(1) Performance and Cost Report; (2) Program Change Request
PCS	(1) Publication Control Sheet; (2) Permanent Change of Station; (3) Submarine Chaser; (4) Personal Communications System; (5) Primary Control Station
PCS/UPT	Personal Communications Services/Universal Personal Telecommunications
PCSF	Fire Support Patrol Craft
PCT	Training Patrol Craft
PCTN	Pacific Consolidated Telecommunications Network
PCTCS	Pentagon Center Telecommunications System
PCZ	Protected Communications Zone
PD	(1) Probability of Damage; (2) Presidential Directive; (3) Pulse Duration; (4) Passive Detection; (5) Point Detonation (Fuse)
PDA	Personal Digital Assistant
PDB	PSYOP Dissemination Battalion
PDC	Propaganda Development Center
PDD	Presidential Decision Directive
PDI	Principal Deputy for Intelligence
PDF	Panamanian Defense Force
PDL	Program Design Language
PDM	(1) Program Decision Memorandum; (2) Pulse Duration Modulation
PDMS	Point Defense Missile Systems
PDMT	Pursuit Deterrent Munition Trainer
PDOP	Position Dilution of Precision

Page 3432 of 3957

PDP	(1) Program Decision Paper; (2) Programmable Data Processor
PDR	Preliminary Design Review
PDS	(1) Passive Detection System; (2) Power Distribution System; (3) Production Deconfliction System; (4) Protected Distribution System PDSC PACOM Data Systems Center
PDSS	Post-Deployment Software Support
PDU	Protocol Data Unit
PDUSD(A&T)	Principal Deputy Under Secretary of Defense (Acquisition & Technology)
PE	(1) Probable Error; (2) Personnel Equipment; (3) Program Element; (4) Preliminary Exploitation; (5) Peace Enforcement
PEAD	Presidential Emergency Affairs Documents
PEAS	(1) Psychological Operations Effectiveness Analysis Subsystem; (2) PSYOP Effects Analysis System
PEC	(1) Pacific Command Electronic Intelligence Center; (2) Program Element Code
PEG	(1) Photo Exploitation Group; (2) Priority Exploitation Group; (3) Priorities for ELINT Guidance; (4) Program Element Group
PEH	Probable Error in Height
PEI	Production Enhancement Initiative
PEILS	PACOM Executive Intelligence Summary
PEM	(1) Purchased Equipment Maintenance; (2) Program Element Monitor
PEO	Peace Enforcement Operation
PEOC4I	Program Executive Officer for Command, Control, Communications, Computers, and Intelligence
PEP	Photographic Exploitation Products
PER	Personnel
PERIGEE	Perspective Image Generation and Exploitation System
PERINTREP	Periodic Intelligence Report
PERINTSUM	Periodic Intelligence Summary
PERM	Processless Electron Recording Media
PERMCERT	Permanent Certification
PERSCON	Personal Contact
PEO	Program Executive Officer
PEO-CCS	PEO Command and Control Systems
PERSEC	Personnel Security
PERT	Program Evaluation and Review Technique
PES	Positive Enable System
PESM	Passive Electronic Support Measures
PF	Protection Factor
PFADS	Psychological Operations Foreign Area Data Subsystem
PFD	Power Flux Density
PFIAB	President’s Foreign Intelligence Advisory Board
PFLP	Popular Front for the Liberation of Palestine
PFM	Production Functional Manager

Page 3433 of 3957

PFOD	Presumptive Finding of Death
PG	(1) Patrol Combatant; (2) Persian Gulf; (3) Precision Guidance
PGDR	Portable Data Reduction System
PGF	Patrol Ship
PGG	Guided-Missile Patrol Combatant
PGH	Patrol Gunboat (Hydrofoil)
PGIP	Postgraduate Intelligence Program
PGM	Precision-Guided Munitions
PGR	Reconnaissance Patrol Combatant
PGW	Precision Guided Weapon
PGSS	Publications and Graphics Subsystem
PHD	Phase History Data
PHIBGRU	Amphibious Group
PHIBRON	Amphibious Squadron
PHIGS	Programmer's Hierarchical Interactive Graphics
PHM	Patrol Combatant Missile (Hydrofoil)
PHOTOINT	Photographic Intelligence
PHOTORECON	Photographic Reconnaissance
PHS	Public Health Service
PHYSEC	Physical Security
PI	(1) Photographic Interpretation/Interpreter; (2) Principal Investigator
PIAC	PACOM Intelligence Architecture Committee
PIB	(1) PACOM Intelligence Board; (2) Photo Interpretation Brief
PIC	(1) Pacific Imagery Processing and Interpretation Center; (2) Parent Indicator Code; (3) Processing and Interpretation Center
PICON	Portable ICON
PIF	(1) Processing and Interpretation Facility; (2) Project Investment Fund
PIGS	Passive Infrared Guidance System
PIICS	PACOM - Intelligence Computer System
PILOT	Phased Integrated Laser Optics Technology
PIM	Path of Intended Movement
PIN	(1) Preliminary Imagery Nomination File; (2) Photographic Intelligence Note; (3) Personal Increment Number; (4) Plan Identification Number; (5) Personal Identification Number; (6) PACOM Intelligence Net
PINES	PACAF Interim National Exploitation Segment/System

Page 3434 of 3957

PIP	(1) Project Implementation Plan; (2) Product Improvement Package
PIR	(1) Photo Interpretation Report; (2) Priority Intelligence Requirement
PIRATE	Portable Imagery Receive and Transmission Equipment
PIREP	Pilot Report
Pixel	Picture Element
PJ	Pararescue Jumper
PK	(1) Probability of Kill; (2) Soviet (FSU) Light Machinegun; (3) Peacekeeping
PKA	Public Key Algorithm
PKC	Public Key Cryptography
PKK	Kurdistan Worker's Party
PKO	Peace-Keeping Operation
PKSD	Programmable Key Storage Device
PL	(1) Phase Line; (2) Plans and Operations Division; (3) Public Law
PLA	(1) Plain Language Address; (2) People's Liberation Army (China)
PLARS	Position Locating and Reporting System
PLGR	Precision Lightweight GPS Receiver
PLL	Prescribed Load List
PLNG	Planning
PLRS	Position Location Reporting System
PLO	Palestinian Liberation Organization
PLP	PSYOP Leaflet Payload
PLS	Pre-Launch Survivability
PLSDU	Physical Layer Service Data Unit
PLSS	U.S. Precision Location Strike System
PLT/Plt	Platoon
PM	(1) Preventive Maintenance; (2) Post Meridian (after noon); (3) Prime Mover; (4) Preventive Medicine; (5) Program Manager; (6) Prime Minister; (7) Provost Marshall; Project Manager; (8) Production Manager; (9) Peacemaking
PMATS	Program Management Automated Tool Set
PMB	Program Management Board
PME	Professional Military Education
PMF	Project Management File
PMGM	Program Manager's Guidance Memorandum
PMIS	(1) Personnel Management Information System; (2) PSYOP Management Information Subsystem
PMO	(1) Program Management Office; (2) Project Management Office
P Model	Preproduction Model
PMP	Program Management Plan
PMPTS	Program Management Performance Tracking System
PMR	Primary Mission Readiness
PMRP	Program Manager's Recommended Program

Page 3435 of 3957

PMS	(1) Project Management System; (2) Preventive Maintenance System; (3) Precision Mensuration Software
PMSP	Preliminary Message Security Protocol
PMTC	Pacific Missile Test Center (Navy)
PN	Packet Network
PNAF	Prime Nuclear Airlift Force
PNCC	PASS Network Control Center
PNEK	Post-Nuclear-Event Key
PNE(T)	Peaceful Nuclear Explosion (Treaty)
PNG	Persona Non Grata
PNL	Prescribed Nuclear Load
PNUTS	Possible Nuclear Underground Test Site
PNVS	Pilot Night Vision System
PO	(1) Petty Officer; (2) Peace Operations
POA&M	(1) Plan of Action and Milestones; (2) Plan of Attack and Milestones
POADS	Psychological Operations Automated Data System
POAS	Psychological Operations Automation System
POB	(1) Place of Birth; (2) Psychological Operations Battalion
POC	(1) Point of Contact; (2) Program of Cooperation; (3) Psychological Operations Company
POC/ET	Proof of Concept/Experimental Testbed
POCS	Portable Oxygen Charging System
POD	Port of Debarkation
POE	(1) Plan of Execution; (2) Point of Entry; (3) Port of Embarkation
POES	Polar Orbiting Environmental Satellite
POG	Psychological Operations Group
POI	Program of Instruction
POL	(1) Petroleum, Oils, and Lubricants; (2) Political
POL-MIL	Political-Military
POLAD	Political Advisor
POM	(1) Program Objective Memorandum; (2) Preparation for Overseas Movement
POMCUS	Prepositioned Organizational Materiel Configured in Unit Sets
POOS	Parachute Offset Oxygen System
POP	Point of Presence
POR	Preparation for Oversees Replacement
PORTS (JOPES)	(1) Portable Remote Telecommunications System; (2) Seaports Files; (3) Portable Receive and Transmit System
PORTS-1N	Portable Receive and Transmit System - 1N
PORTSREP	Ports Report File (JCS/J-3)
Pos	Position
POSIX	Preliminary Open System Interface Standard
Pos-Nav	Positioning and Navigation
POST	Prototype Ocean Surveillance Terminal

Page 3436 of 3957

POTBI	Places, Organizations, Things, Biographics, Intangibles
POTF	Psychological Operations Task Force
POV	Privately Owned Vehicle
POW	Prisoner of War
POWERR	Prototype Workstation for Electronic Warfare and Radio
PP	Preprogramed
PPO	Pilot and Payload Operator
PPBES	Planning, Programming, and Budgeting Execution System
PPBS	Planning, Programming, and Budgeting System
PPC	Printing and Publications Center
PPDB	Point Positioning Data Base
PPF	Photographic Processing Facility
PPGM	Planning and Programming Guidance Memorandum
PPI	Pulse Position Indicator
PPIF	Photographic Processing and Interpretation Facility
PPL	Preferred Products List
PPM	(1) Parts Per Million; (2) Pulse Position Modulation
PPMS	Power Pattern Measurement System
PPS	Precision and Positioning Service
PR	(1) Production Requirement; (2) Personnel Recover
PRA	(1) Permanent Restricted Area; (2) Population Reception Area (NATO)
PRAM	Allied Mine
PRB	Program Review Board
PRBAC	Partition Rule Base Access Control
PRC	(1) Policy Review Committee; (2) People's Republic of China
PRC(I)	Policy Review Committee (Intelligence) (now SIG(I))
PRCSO	Peacetime Reconnaissance and Certain Sensitive Operations
PRD	(1) Production Responsibilities Document; (2) Presidential Review Directive
PRDA	Photo Reconnaissance Damage Assessment
PREMSS	Photo Reconnaissance and Exploitation Management Support System
PREP/RAMP	Pre-Edit Processor/Report and Message Processor
PRF	Pulse Repetition Frequency
PRG	Program Review Group
PRGB	Point Reference Guild Book
PRI	(1) Pulse Repetition Interval; (2) Primary Rate Interface
PRIMAC	Production and Inventory Management and Control System
PRM	Presidential Review Memorandum
PROC	Processing/Process
PROCOMM	Terminal Emulation Software for DOS Workstations
PROD	Production
PROG	Program
PROM	Programmable Read-Only Memory

Page 3437 of 3957

PROPIN	Caution — Proprietary Information Involved
PRP	Portable Radio Program
PRPG	Preliminary Reference Point Graphic
PRS	PACOM Remote System
PRSCO	Peacetime Reconnaissance and Sensitive Collection Operations
PRT	Personal Rapid Transit
PRTB	Soviet (FSU) Mobile Rocket Technical Base
PRU	Photographic Reconnaissance Unit
PS	(1) Processing Station; (2) Processing Segmext; (3) Policy Support
Ps	Permanent snowfields
PSAA	Pacific Special Activities Area
PSAC	President's Scientific Advisory Committee
PSB	Harbor Patrol Boat
PSC	Principal Subordinate Command (NATO)
PSDU	Physical Layer Service Data Unit
PSI	(1) Pounds Per Square Inch; (2) Personnel Security Investigation
PSK	Phase Shift Keying
PSL	Protected Services List
PSN	(1) Packet Switching Node; (2) Public Switched Network; (3) Packet Switched Network
Psns	Positions
PSO	(1) Protective Structure Only; (2) Personnel Security Office; (3) Post Security Officer
PSP	(1) Pierced Steel Planking; (2) Planning Support Package
PSPS	PSYOP Studies Program Subsystem
PSR	(1) Post-Attack Status Report; (2) Periodic Status Report
PSRC	Presidential Selected Reserve Call-Up
PSS	Packet Switched Service
PST	Pacific Standard Time
PSTN	Public Switched Telecommunications Network
PSYOP	Psychological Operations
PSYOPGP	Psychological Operations Group
PSYWAR	Psychological Warfare
PT	(1) Torpedo Boat; (2) Part Time; (3) Physical Training
Pt	Peat
PTADB	Planning Terrain Analysis Data Base
PTG	Missile Attack Boat
PTGP	Part-Time Graduate Program
PTIAP	PACOM Theater Intelligence Architecture Program
PTL	Small Torpedo Boat
Ptl	Patrol
PTN	Pacific Tributary Network
PTP	(1) Probability to Penetrate; (2) Point-to-Point
PTR/P	Paper Tape Reader/Punch

Page 3438 of 3957

PTS	Predicasts Terminal System
PTSR	Postmobilization Training Support Requirement
PTSS	Passive Thermal Suppression Suit
PTT	(1) Training Torpedo Boat; (2) Postal, Telephone, and Telegraph; (3) Push to talk
PTTP	USPACOM Tactics, Techniques, and Procedures
PTTDS	Projected Target Trends Data Sheet (FTL)
PTTP	USPACOM Tactics, Techniques, and Procedures
Pub	Publication
PUG	Partially Underground
PUP	(1) Performance Upgrade Program; (2) Pop-Up Point
PV	Physical Vulnerability
PVDS	Physical Vulnerability Data Sheets
PVITS	Portable Video Imagery Transmission System
PVST	Port Visit
PVO	(1) Air Defense (FSU); (2) Private Voluntary Organization
PVTM	Physical Vulnerability Technical Memorandum
PW	(1) Prisoner(s) of War; (2) Pulse Width
PWDS	Protected Wireline Distribution System
PWHQ	Primary War Headquarters
PWI	PACOM Warning Intelligence
PWIPS	Pre-Launch Warning Intelligence Processing System
PWRS	Prepositioned War Reserve Stock
PZ	Pick-Up Zone

Page 3439 of 3957

Q

QA	Quality Assessment
Q&A	Question and Answer
QBE	Query by Example
QC	Quality Control
QEA	Quick Erect Antenna
QM	Quartermaster
Q-MESSAGE	Classified Message on Navigational Hazard
QOL	Quality of Life
QPQ	Quid Pro Quo
QPSK	Quadrature Phase Shift Keying
Q/R	Query/Response
QRA	Quick Reaction Alert
QRC	Quick Reaction Capability
QRF	Quick Response Force
QRG	Quick Response Graphic
QRLS	Quick Reaction Launch System
QRMP	Quick Response Multicolor Printer
QRP	Quick Reaction Package
QRRC	Quarterly Readiness Report to Congress
QRT	(1) Quick Reaction Task; (2) Quick Reaction Terminal
QRSA	Quick Reaction Satellite Antennae
QRSP	Quick Reaction Shuttle Payload
QSR	Quick Strike Reconnaissance
QSTAG	Quadripartite Standardization Agreement
QUICKSAT	Modified AN/FSC-78
QUIP	Quarterly Intelligence Production Listing

Page 3440 of 3957

R

R	(1) Rock Outcrops; (2) Receiver
RA	(1) Restricted Area; (2) Responsible Agency; (3) Resident Agent
RAAF	Royal Australian Air Force
RAAP	Rapid Application of Air Power
RAC	Resident Agent in Charge
RACE	Rapid Automatic Cryptographic Equipment
RAF	Royal Air Force
RABFAC	Radar Beacon Forward Air Controller
RAC	Research and Analysis Company
RACO	Rear Area Combat Operations
RAD	Radiation Absorbed Dose
RADAR	Radio Detection and Ranging
RADAREXREP	Radar Exploitation Report
RADAY	Radio Day
RADBN	Radio Battalion
RADC	Rome Air Development Center
RADCM	Radar Countermeasures
RADCOM	Radio Communications
RADCON	Radiological Control
RADIAC	Radioactive Detection, Indication, and Computation
RADINT	Radar Intelligence
RADREL	Radio Relay
RAF	Royal Air Force (U.K.)
RAG	(1) River Assault Group; (2) Regimental Artillery Group (FSU)
RAIDS	Rapid Access Imagery Dissemination System
RAILS	Relational Analyses of Internetted Linkages System
RAM	(1) Rolling Airframe Missile; (2) Random Access Memory; (3) Radar Absorbing Materials; (4) Reliability, Availability, and Maintainability
RAMP	Rating Maintenance Program
RAMPART	Radar Advanced Measurement Program for Analysis of Reentry Techniques
RAOC	(1) Rear Area Operations Center; (2) Regional Air Operations Center
RAOWG	Radar and Optical Intelligence Working Group
RAP	(1) Rocket Assisted Projectile; (2) Remedial Action Projects
RAPIDE	Relocatable Army Processors for Intelligence Data-Europe
RAPIER	Rapid Emergency Reconstitution
RAPTOR	Responsive Aircraft Program for Theater Operations
RAS	(1) Record Assigned Systems; (2) Replenishmest at Sea; (3) Regional Analysis Section; (4) Rear Area Security; (5) Remote Access Support
RASC	Required Automated Services Center

Page 3441 of 3957

RASS	Random Access Storage System
RAST	Regional Analyst Support Team
RATO	Rocket-Assisted Takeoff
RATT	Radio Teletypewriter/Teleprinter
RATV	Rescue All Terrain Vehicle
RAU	Radio Access Unit
RAWS	RAPIDE Analyst Workstation
RAWSII	Raw Statement of Intelligence Interest
RB/ER	Reduced Blast/Enhanced Radiation
RBIF	Red Basic Intelligence File
RBS	(1) Regional Broadcast System; (2) Remote Base Server
RC	(1) Radio-Controlled; (2) Required Capability; (3) Reserve Component; (4) Riverine Craft
RCA	(1) Riot Control Agent; (2) Royal Canadian Army; (3) Requirements Control Authority
RCAF	Royal Canadian Air Force
RCAS	Reserve Component Automated System
RCC	(1) Regional Control Center; (2) Rescue Coordination Center
RCF	Remote Collection facility
RCM	Radar Countermeasures
RCOC	Regional Communications Operations Center
RCMP	Royal Canadian Mounted Police
RCP	Remote Communications Processor
RCS	(1) Radar Cross Section; (2) Remote Collection System
RCSS	(1) Reconnaissance Cargo; (2) RC-135 Support Service
RCST	RC-135 Support Team
RCU	Reserve Component Unit
RCV	Receive
RCW	Reconfigurable Workstation
RCZ	Rear Combat Zone
RD	(1) Restricted Data; (2) Radius of Damage; (3) Replacement Detachment; (4) Readiness Division
R&D	Research and Development
RD&A	Research, Development, and Acquisition
RDA	Research, Development, Acquisition
RDAISA	United States Army Research, Development & Acquisition Information Systems Agency
RDB	Requirements Data Base
RDBMS	Relational Data Base Management System
RDC	Rapid Deployment Capability
RDD	Required Delivery Date
RDE	Radiation Detection Experiment
RDEC	Research Development Engineering Center
RDF	(1) Radio Direction Finding; (2) Rapid Deployment Force
RDI	Reconnaissance, Detection & Identification
RDIT	Rapid Deployment Imagery Terminals

Page 3442 of 3957

RDJTF	Rapid Deployment Joint Task Force
RDL	Recurring Document Listing
RDMSS	Rapidly Deployable Mobile SIGINT Systems
RDS	(1) Remote Display System; (2) Rapid Dissemination System
RDSS	Rapidly Deployed Surveillance System
RDT&E	Research, Development, Test and Evaluation
RDV	Rapid Deployment Vehicles
RE	Receive Element
READ	Readiness
READYCAP	Fighter Aircraft in Standby Condition
REC	Radio-Electronic Combat
RECA	Residual Capabilities Assessment
RECA(T)	Residual Capability Assessment (Team)
RECAP	Requirements and Capabilities System
RECAS	Residual Capabilities Assessment System
RECC	Regional Emergency Communications Coordinator
RECCE	Reconnaissance
RECCEXREP	Reconnaissance Exploitation Report
RECI	Radar Emitter Classification Identification
RECLAU	Reconnaissance Launch Report
RECON	Reconnaissance
RECONBN	Reconnaissance Battalion
RECONT	Reconnaissance Intentions Report
REDCOM	Readiness Command
REDCON	Readiness Condition
RED Cell	Rapid Exploitation and Dissemination Cell
RED FLAG	ACC Combat Flying Exercise at Nellis AFB
RED HORSE	Deployable Civil Engineering Group
REDTRAIN	Readiness Training
REFORGER	Return of Forces to Germany (Exercise)
RFC	Request for Collection
REG	Regulation
REGT/Regt	Regiment
REL	Releasable
RELCAN	Releasable to Canada
RELROK	Releasable to the Republic of Korea
REM	Route Evaluation Module
REMAB	Remote Marshalling Base
REMBASS	Remotely Emplaced Battlefield Surveillance System
REMS	Remote Employed Sensors
REMT	Regional Emergency Management Team
RENS	Reconnaissance, Electronic Warfare & Naval Intelligence System
REP	(1) Range Error Probable; (2) Reserve Exploitation Program; (3) Representative

Page 3443 of 3957

RES	Remote Earth Sensing
Res	Reserve
RESDAT	Restricted Data
RESTA	Reconnaissance, Surveillance & Target Acquisition
RETRANS	Retransmission
RETS	Remoted Target System
REUTERS	A News Service
REW(S)	Radio Electronic Warfare (Service)
REWSON	Reconnaissance, Electronic Warfare, Special Operations & Naval Intelligence Processing System
RF	(1) Radio Frequency; (2) Representative Fraction
RF-4	Designator for Reconnaissance Aircraft (USAF/USMC)
RFA	Restricted Fire Area
RFC	Request for Collection
RFD	Radio Frequency Distribution
RFE/RL	Radio Free Europe/Radio Liberty
RFI	(1) Radio Frequency Interference; (2) Request for Information
RFIS	Reserve Forces Intelligence School
RFL	Restrictive Fire Line
RFMETS	Radio Frequency Mobile Electronics Test Set
RFP	(1) Remaining Force Potential; (2) Radio Frequency Pulse; (3) Request for Proposal; (4) Request for Production
RFPI	Rapid Force Projection Initiative
RFPW	Radio Frequency Pulse Weapon
RFR	Request for Requirements
RFS	Request for Service
RFTB	Reserve Force Target Base
RFTL	Reserve Forces Target List
RGB	Red-Green-Blue
RGR	(1) Ranger; (2) Roger
RGS	Relay Ground Station
RGT	Regiment
RHAW	Radar Homing and Warning
RHIB	Rubber Hull Inflatable Boat
RI	Routing Indicator
RIB	Rigid Inflatable Boat
RIC	(1) Regional Intelligence Center; (2) Resource Identification Code
RIF	Reduction in Force
RII	Request for Intelligence Information
RIM	ROTHR Interface Module
RIMPAC	U.S. Naval Exercise
RIMS	Requirements Inventory Management System
RINT	Unintentional Radiation Intelligence
RIO	Radar Intercept Officer

Page 3444 of 3957

RIP	(1) Register of Intelligence Publications; (2) Reconnaissance Information Point
RIPL	Reconnaissance and Interdiction Planning Line (NATO)
RIPSO	Revised IP Security Option
RISC	Reduced Instruction Set Computer
RISOP	Red Integrated Strategic Operations Plan
RISP	Reserve Intelligence Support Project
RIT	Remote Imagery Transceiver
RITS	Remote Imagery Transceiver System
RJITF	Regional Joint Intelligence Training Facility
RL	(1) Rocket Launcher; (2) Radio Liberty; (3) Receive Location
RLG	Ring Laser Gyro
RM	(1) Requirements Management; (2) Resource Management
RMBUX	Rocky Mountain Basic UNIX
RMEC	Regional Military Emergency Coordinator
RMG	Resource Management Group
RMO	(1) Records Management Officer; (2) Requirements Management Office
RMS	(1) Requirements Management System; (2) Remote Monitoring System
RNAV	Area Navigation
RNO	Regional Nuclear Option
RNP	(1) Radio Navigation Point; (2) Remote Network Processor
RO	(1) Reporting Officer; (2) Radar Operation; (3) Receive Only; (4) Resident Office
RO/RO	Roll-On/Roll-Off (Ship)
ROB	Radar Order of Battle
ROC	(1) Required Operational Capability; (2) Republic of China; (3) Reconnaissance Operations Center; (4) Required Operational Capability; (5) Regional Operations Center
ROCC	Regional Operations Control Center
ROD	Reconnaissance Operations Division
RODCA	(1) Reporting of DoD HUMINT Collection Activities; (2) Message Caveat
ROE	Rules of Engagement
ROF	(1) Rate of Fire; (2) Remote Operating Facility
ROFA	Remote Operating Facility Airborne
ROIPB	Rear Operations Intelligence Preparation of the Battlefield
ROK	Republic of Korea
ROKA	Republic of Korea Army
ROKAF	Republic of Korea Air Force
ROKN	Republic of Korea Navy
ROKUSCFC	Republic of Korea and U.S. Combined Forces Command
ROM	Read Only Memory
RON	Remain Overnight
ROP	Remote Operating Position
RORSAT	Soviet (FSU) Radar Ocean Reconnaissance Satellite

Page 3445 of 3957

ROSE	Remote Optical Sensing of the Environment
ROSS	Refinement of SIGINT Support
ROT	Rotating Position
ROTC	Reserve Officer Training Corps
ROTHR	Relocatable Over-the-Horizon Radar
ROU	Radius of Uncertainty
ROW	Rest-of-World
RP	(1) Reference Point; (2) Release Point
RPA	Reserve Personnel Allotment
RPB	Regional Preparedness Board
RPC	(1) Regional Preparedness Committee; (2) Regional Reporting Center; (3) Remote Procedure Calls; (4) Rapid Positioning Capability
RPE	Reconnaissance Planning Element
RPG	(1) Soviet (FSU) Shoulder-Fired Antitank Grenade Launcher; (2) Report Program Generator
RPK	Soviet (FSU) Light Machinegun (similar in design to the AK rifle)
RPM	(1) Revolutions per Minute; (2) Rounds per Minute
RPT	Report
RPTG	Reporting
RPV	Remotely Piloted Vehicle
RQS	Rescue Squadron
RQT	(1) Reliability Qualification Tests; (2) Requirement
RQMTS	Requirements
RR	(1) Railroad; (2) Radio Relay
R&R	Rest and Recreation
RRC	Regional Reporting Center
RRDB	Rapidly Reconfigurable Data Base
RRF	(1) Ready Reserve Force; (2) Rapid Reaction Force (ACE)
RRG	Remote Receive Group
RRI	Response to Request for Information
RRICS	Rapid Response Imagery Capability System
RRII	Response to Request for Intelligence Information
RRM	Red Resource Monitoring
RRP	Rapid Reinforcement Plan
RRS	Remote Receive Station
RRT	Radio Receive/Transmitter
RRTP	Rail-to-Road Transfer Point
RS	Reconnaissance/Surveillance
R&S	Reconnaissance and Surveillance
RSB	PSYOP Regional Support Battalion
RSBN	Short-Range Navigation System (FSU)
RSDN	Long-Range Navigation System (FSU)
RSC	(1) Regional Support Commands; (2) PSYOP Regional Support Company
R&SC	Reconnaissance and Surveillance Center

Page 3446 of 3957

RSE	Ranger Support Element
RSI, R/S/I	Rationalization, Standardization and Interoperability
RSN	Red Switched Network
RSO	(1) Reconnaissance & Survey Officer; (2) Regional Security Officer
RSOC	Regional SIGINT Operations Center
RSOD	Remote Satellite Operations Demonstration
RSOG	Reserve Special Operations Group
RSR	(1) Resource Status Report; (2) Required Supply Rate; (3) Radar Service Request
RSSC	Regional Space Support Centers
RSSP	Reconnaissance Support Survivability Program
RST	(1) Recovery Support Team; (2) Regional Survey Team
RSTA	Reconnaissance, Surveillance, & Target Acquisition
RSW	Reflected Shockwave
RT	(1) Real Time; (2) Radio Telephone; (3) Relocatable Target; (4) Radius of Target
RTA	Residual Threat Assessment
RTAPS	Relocatable Target Adaptive Planning Support
RTASS	Remote Tactical Airborne SIGINT System
RTCE	Rapid Targeting Capability Europe
RTG	Reconnaissance Technical Group (TAC, USAFE, PACAF)
RTIC	(1) Regional Threat Information Cell; (2) Real-Time Information to the Cockpit
RTIP	Real-Time Interactive Processor
RTM	Receiver/Transmitter/Modem
RTOS	Real-Time Optical System
RTP	Rail Transfer Point
RTS	(1) Reconnaissance Technical Squadron; (2) Real-Time Simulator
RTS-I	Regional Training Site(s)-Intelligence
RTSP	Real-Time Signal Processor
RU	(1) Roundup; (2) Resident Unit
RUNT	Russian Underground Nuclear Test
RURPOP	Rural Population File
RV	(1) Reentry Vehicle; (2) Radius of Vulnerability; (3) Reconnaissance Vehicle
RVT	Remote Video Terminal
RW	(1) Radiological Warfare; (2) Rotary Wing; (3) Reconnaissance Wing
RWH	Radar Warning & Homing
RWI	Radio Wireline Interface/Integration
RWO	Reconnaissance Watch Officer
RWR	Radar Warning Receiver
RWS	Remote Workstation
RX	Receive
RZ	Recovery Zone

Page 3447 of 3957

S

S	Secret
/s/	Signature
S-1	Personnel Staff Officer
S-2	Intelligence Staff Officer; Brigade, Battalion, and Armored Cavalry
S-3	Operations Staff Officer
SA	(1) Logistics Staff Officer; (2) Special Access; (3) Situational Awareness (4) Signals Analysis; (5) Surface-to-Air; used to identify FSU Surface-to-Air Missiles, e.g., SA-7/GRAIL; (6) Situation Assessment; (7) Security Assistance; (8) Special Agent; (9) Stand Alone; (10) Secretary of the Army; (11) Systems Administrator; (12) Strategic Attack
SAA	(1) Special Area Assessments; (2) Strategic Air Army
SAAC	Strategic Analysis Applications Center
SAAM	Special Assignment Airlift Mission
SAASE	Standard Data Element-Based Automated Architecture Support Environment
SACC	Supporting Arms Coordination Center
SACCS	Strategic Air Command Automated Command & Control System
SACS	(1) Secure Access Control System; (2) STU-III Access Control System
SAE	Service Acquisition Executive
SAB	Subject as Above
SAC	(1) Strategic Air Command; (2) Scientific Advisory Committee; (3) Senate Appropriations Committee
SACDIN	SAC Digital Network
SACEUR	Supreme Allied Commander, Europe (NATO)
SACLANT	Supreme Allied Commander, Atlantic (NATO)
SACLANTREPEUR	SACLANT Representative in Europe
SACOM	Southern Area Command
SACOS	SAC Operational Staff
SACWARNS	(1) Strategic Air Command Indications and Warning; (2) SAC Warning System
SADARM	Sense and Destroy Armor
SADF	South African Defense Force
SADO	Senior Air Defense Officer
SADT	Structured Analysis Design Technique
SAEDA	Subversion and Espionage Directed Against the Army
SAF	(1) Soviet (FSU) Air Force; (2) Source Acquisitions File; (3) Secretary of the Air Force; (4) US Air Force Staff
SAFE	(1) Support for the Analysts' File Environment; (2) Selected Area for Evasion
SAFF	Safing, Arming, Fuzing, and Firing
SAF/O/T	Security Assistance Force/Organization/Team
SAG	(1) Study Advisory Group; (2) Surface Action Group; (3) Strategic Advisory Group

Page 3448 of 3957

SAGE	Semiautomatic Ground Environment (Radar)
SAI	Strategic Command Administrative Instruction
SAIB	Safe Area Intelligence Brief
SAID	Safe Area Intelligence Description
SAIS	Strategic Aerospace Intelligence System
SAL	(1) Strategic Arms Limitation; (2) Submarine Alerting and Locating
SALT	(1) Strategic Arms Limitation Talks; (2) Supporting Arms Liaison Team
SALUTE	Size, Activity, Location, Unit, Time, Equipment (spot report format)
SAM	(1) Surface-to-Air Missile; (2) Summary Assessment Matrix
SAMOB	Surface-to-Air Missile Order of Battle
SAMSO	Space And Missile System Organization
SAMT	State of the Art Medium Terminals
SAO	(1) Special Access/Activities Office; (2) Select Attack Option; (3) Special Access Only; (4) Security Assistance Organization; (5) Security Assistance Office
SAOB	FSU Air Order of Battle
SAOC	(1) Space Actions Officers Course; (2) Sector Air Operations Center
SAOCS	Submarine/Aircraft Optical Communications System
SAP	(1) Special Access Program; (2) System Acquisition Plan
SAPAS	Semiautomatic Population Analysis System
SAR	(1) Search and Rescue; (2) Synthetic Aperture Radar; (3) Special Access Required; (4) Sea-Air Rescue
SARC	Surveillance and Reconnaissance Center
SARDA	Secretary of the Army for Research, Development and Acquisition
SARP	Storage and Retrieval Processor
SARPF	Strategic Air Relocatable Processing Facility
SARSAT	Search and Rescue Satellite-Aided Tracking
SART	Strategic Aircraft Recovery Team
SARV	Strategic Aerospace Reconnaissance Vehicle
SAS	(1) Strategic Area Study; (2) Strategic Aerospace Summary; (3) Special Activities Squadron; (4) Support to Analyst Subsystem; (5) Survivable Adaptive Systems
SASC	Senate Armed Services Committee
SASM	Strategic Air-to-Surface Missile
SASS	(1) Small Aerostat Surveillance System; (2) Systems Acquisition Support Services
SAT	(1) Satellite; (2) Staff Augmentation Team; (3) Satisfactory
SATCOM	Satellite Communications
SATCOMA	Satellite Communications Agency (U.S. Army)
SATKA	Surveillance, Acquisition, Tracking, and Kill Assessment
SATRAN	(1) Satellite Reconnaissance Advanced Notice; (2) Satellite Transmission
SATS	Southwest Asia Telecommunications System
SATVUL	Satellite Vulnerability

Page 3449 of 3957

SAVE	Situation Analysis and Vulnerability Estimate
SAVI	Systems Analysis of Vulnerability to Intrusion
SAWC	Special Air Warfare Center
SAWG	Simulation and Analysis Working Group
SAWIC	Strike and Amphibious Warfare Intelligence Center
SAWS	Submarine Analyst Work Station
SAWVS	Satellite Attack Warning and Verification System
SB	Sentinel Byte
S-BAND	2 to 4 GHz
SBB	Sustained Bare Base
SBI	(1) Special Background Investigation; (2) Space-Based Interceptor
SBIRS	Space-based Infrared Radar System
SBIS	Sustaining Base Information Services
SBKKV	Space-Based Kinetic Kill Vehicle
SBL	Space-Based Laser
SBM	Single-Point Mooring Buoy
SBR	(1) Special Boat Squadron; (2) Space-Based Radar
SBS	Site Backbone Segment
SBSS	Space-Based Surveillance System
SBU	(1) Special Boat Unit; (2) Sensitive but Unclassified
SBWASS	Space-Based Wide-Area Surveillance System
SC	(1) Science Committee (NATO); (2) Signal Corps; (3) Security Code; (4) Signal Company; (5) System Center; (6) Structural Category; (7) Screen Commander or Coordinator; (8) Air Force Communications-Computers Directorate; (9) Submarine Conversion
SCA	Service Cryptologic Agency
SCAD	Subsonic Cruise Armed Decoy
SCAMP	Sensor Control and Management Platoon
SCAMPI	SOF C3I Telecommunications System
SCARE	Standard Collection Asset Request Format
SCATANA	Security Control of Air Traffic and Air Navigation Aids
SCC	(1) Special Coordination Committee; (2) Standing Consultative Commission (SALT); (3) Surveillance Coordination Center; (4) System Control Center; (5) Space Control Center; (6) Service Component Commander
SC CAT	SOUTHCOM Crisis Action Team
SCC(I)	Special Coordination Committee (Intelligence)
SCCP	Single-Channel Command Post
SCCS-R	Single-Channel Collection System - Rear
SCCTV	Secure Closed-Circuit Television
SCDL	Surveillance and Control Data Link (JSTARS)
SCE	Service Cryptologic Element
SCF	Satellite Control Facility
SCF-UK	Save the Children Federation-UK
SCG	Special Consultative Group (NATO)

Page 3450 of 3957

SCI	(1) Sensitive Compartmented Information or Information Programs; (2) Source Code Indicator
SCIBS	Sensitive Compartmented Information Billet System
SCIC	State Crime Information Center
SCIF	Sensitive Compartmented Information Facility
SCIM	Subject Codes for Intelligence Management
SCIMITAR	System for Countering Interdiction Missiles and Target Radars
SCINET	Sensitive Compartmented Information Network (DoDIIS)
SCIP	Special Communications Intelligence Package
SCIPMIS	Standard Civilian Personnel Management Information System
SCIPS	Sensitive Compartmented Information Processing System
SCIS	Survivable Communication Information System
SCISS	SOUTHCOM Intelligence Support System
SCI-VTC	Sensitive Compartmented Information-Video Teleconferencing
SC J2	USSOUTHCOM J2
SCL	Standard Conventional Load
SCLNO	SOUTHCOM Liaison Officer
SCM	Security Countermeasures
SCN	Satellite Control Network
SCO	(1) Service Cryptologic Organizations; (2) Sub-Control Office
SCOLA	Satellite Communications for Learning
SCORE	Signal Communications by Orbiting Relay Equipment
SCOTT	Single-Channel Objective Tactical Terminal
SCP	Secure Conferencing Project
SCPC	Single Channel per Carrier
SCS	(1) Signal Collection System; (2) Satellite Control Squadron
SCSC	SOUTHCOM Support Center
SCSI	Small Computer Systems Interface
SCT	(1) Single-Channel Terminal; (2) Single-Channel Transponder
SCUBA	Self-Contained Underwater Breathing Apparatus
SCUD	Nickname of a Missile System
SD	(1) Space Director; (2) Standard Displacement; (3) Senior Director; (4) Security Division; (5) Strategic Command Directive
SDA	(1) Ships Destination Authority; (2) Strike Damage Assessment
S&DA	Strike and Damage Assessment
SDB	Space Data Base
SDC	(1) Strategic Dissemination Company; (2) Strategic Defense Command
SDD	Secure Data Device
SDF	Structured Data Fields
SDHS	Satellite Data Handling System
SDI	Strategic Defense Initiative
SDIE	Special Defense Intelligence Estimate

Page 3451 of 3957

SDIN	(1) Secure Digital Information Network; (2) Special Defense Intelligence Notice
SDIO	Strategic Defense Initiative Organization
SDIS	Switched Digital Integrated Service
SDLC	Synchronous Data Link Control
SDM	Standoff Destructive Munition
SDMA	Spaced Division Multiple Access
SDMS	SINET Data Management System
SDNRIU	Secure Digital Network Radio Interface Unit
SDNS	Secure Data Network System
SDO	System Development Office
SDOB	Scaled Depth of Burst
SDR	(1) Source-Directed Requirements; (2) System Design Review
SDS	(1) Satellite Data System; (2) SIGINT Direct Support; (3) Satellite Dissemination System; (4) Secondary Dissemination System; (5) Strategic Defense System; (6) Switched Data Services; (7) Spatial Data Server; (8) Small Digital Switch
SDV	(1) Swimmer Delivery Vehicle; (2) SEAL Delivery Vehicle
SDVT	SEAL Delivery Vehicle Team
SDYS	Studies
SE	Southeastern
SEA	(1) Southeast Asia; (2) Senior Enlisted Advisor
SEABEE	Navy Construction Battalion Personnel
SEALANCE	Anti-Submarine Warfare Standoff Weapons (ASW/SOW)
SEAD	Suppression of Enemy Air Defense
SEADS	Southeast Air Defense Sector
SEAGA	Selective Employment Air Ground Alert Forces
SEAL	Sea/Air/Land
SEASTAG	SEATO Standardization Agreement
SEATO	Southeast Asia Treaty Organization
SEAWATCH	NOSIC On-Line Computer System
SEC	(1) Second; (2) Section; (3) Submarine Element Coordinator
SECAF	Secretary of the Air Force
SECARMY	Secretary of the Army
SECC	Survivable Enduring Command Center
SECCLEAR	Security Clearance (Management System)
SECDEF	Secretary of Defense
SECNAV	Secretary of the Navy
SECOM	Security Committee
SECS	Survivable and Enduring Communications System
SECSTATE	Secretary of State
SECTY	Security
SED	Simulated Electronic Deception
SEDSCAF	Standard ELINT Data System Codes and Formats

Page 3452 of 3957

SEE	(1) System Engineering and Evaluation; (2) Softcopy Exploitation Environment
SEEI	Special Essential Elements of Information
SEEK	Soviet Emigre Exploitation Kit
SEI	Specific Emitter Identification
SEIP	Senior Enlisted Intelligence Program
SEIS	Survivable and Enduring Intelligence System
SELA	Latin American Economic System
SELORS	Ship Emitter Locating Reports
SELMON	Selective Monitoring
SEMA	Special Electronic Mission Aircraft
SEMEC	SOF Enhanced Moldable Explosive Change
SEN	(1) Small Extension Node; (2) Space Engagement Node
SEOS	SIGINT/Electronic Warfare Operating System
SEP	(1) Selective Employment Plan (NATO); (2) Separate
SEPA	FSU Extended Planning Annex
SEPS	NATO Selective Employment Plan
SERE	Survival, Evasion, Resistance, and Escape
SERER	Survival, Evasion, Resistance, Escape, and Recovery
SERNO	Serial Number
SES	(1) Surface Effects Ship; (2) Systems Engineering Study; (3) Senior Executive Service; (4) Sensor Employment Squadron; (5) Softcopy Exploitation System; (6) Societe European Des Satellites
SESOCC	Southeastern Sector Operations Control Center
SESS	Space Environment Sensor Suite
SET	Sensor Employment Teams
SETAF	Southern European Task Force
SEVOCCS	Secure Voice Command and Control System
SEVOX	Secure Voice
SEWC	Space and Electronic Warfare Commander
SEWCC	SIGINT/Electronic Warfare Coordination Center
SEWS	(1) Satellite Early Warning System; (2) SIGINT Electronic Warfare Subsystem
SF	(1) Special Forces; (2) Standard Form
SFA	Security Fault Analysis
SFAT	Strategic Forces Advisory Team
SFD	Saturated Flux Density
SFEM	Space Forces Engagement Model
SFG	Special Forces Group
SFG-A	Special Forces Group-A
SFG(A)	Special Forces Group (Airborne)
SFOA	Special Forces Operations Area
SFOB	(1) Special Forces Operating Base; (2) Soviet (FSU) Forces Order of Battle
SFOD	Special Forces Operational Detachment

Page 3453 of 3957

SFODA	Special Forces Operational Detachments-A
SFOD-D	First Special Forces Operational Detachment-Delta
SFOS	Special Forces Operating System
SFQC	Special Forces Qualification Course
SFR	Statement of Functional Requirement
SFRD	Safe Functional Requirements Document
SFT	Secure Fault Tolerant
SFTL	Strategic Future Targets List
SFUG	Security Features Users Guide
SGB	SOUTHCOM Ground Order of Battle
SGDPS	Second Generation Data Processing System
SGEMP	System Generated Electromagnetic Pulse
SGF	(1) Southern Group of Forces (Soviet Forces in Hungary); (2) Synthetic Aperture Radar Ground Facility
SGS	(1) Secretary to the General Staff; (2) Squadron Ground Station
SGT	(1) Satellite Ground Terminal; (2) Sergeant
SHA	Secure Hast Algorithm
SHAPE	Supreme Headquarters Allied Powers Europe (NATO)
SHARES	Shared HF Resources
SHC	Supreme High Command
SHF	Super High Frequency
SHED	Special Handling and Evaluation Detachment
SHELREP	Shell Report
SHF	Super High Frequency
SHOP	Special Handling for Operations Purposes
SHORAD	Short-Range Air Defense
SI	(1) Special Intelligence; (2) Special Instructions
S&IA	Security and Investigative Activities
SIAB	Senior Imagery Advisory Board
SIAD	Strategic Imagery Analysis Detachment
SIAP	Strategic Intelligence Architecture Program
SIB	Special Intelligence Brief
SIC	(1) Subject Indicator Code (NATO message code); (2) System Integration Configuration
SICAM	SIGINT Control and Analysis Module
SICR	Specific Intelligence Collection Requirement
SID	(1) Secondary Imagery Dissemination; (2) Subscriber Identification
SID(S)	Selective Imagery Dissemination (System)
SIDA	Single Integrated Data Base
SIDAC	Single Integrated Damage Assessment Code
SIDPAC	Strategic Imagery Detachment Pacific
SIDS	Secondary Imagery Dissemination System
SIE	Space Intelligence Element
SIF	Special Interrogation Facility

Page 3454 of 3957

SIFR	Special Intelligence Functional Requirement
Sig	Signal
SIGCEN	U.S. Army Signal Center
SIG-I	Senior Interagency Group for Intelligence
SIGINT	Signals Intelligence
SIGSEC	Signals Security
SIGSUM	SIGINT Summary
SII	Statement of Intelligence Interest
SIIR	Special Imagery Interpretation Report
SIL	Systems Integration Laboratory
SIM	(1) Sensor Interface Module; (2) Systems Integration Management
SIMIR	USSTRATCOM IDHS Monthly Integration Review
SIMM	Single Inline Memory Module
SIMNET	Single Channel Ground/Airborne Radio Sub-Systems
SIMO	SIM Office
SIMP	Space Intelligence Master Plan
SIMS SOUTHCOM	Intelligence Management System
SINCGARS	(1) Single Integrated Channel Ground and Airborne Radio Subsystems; (2) Single Channel Ground-to-Air Radio System
SINET	Strategic Intelligence Network
SINTER	SIGINT/IMINT Interaction
SIO	(1) Senior Intelligence Officer; (2) Space Intelligence Officer; (3) Ship's Intelligence Officer
SIOP	Single Integrated Operational Plan
SIORI	Self-Initiated Operational Readiness Inspection
SIPE	Strategic Intelligence Processing Element
SIPRNET	Secret Internet Protocol Router Network
SIR	(1) Shuttle Imaging Radar; (2) Specific Information Requirements; (3) Spectrum Interferance Resolution
SIRADS	Shared Imagery Repository and Dissemination System
SIRCS	Shipborne Intermediate-Range Combat System
SIREP	Sensitive Information Report
SIRVES	SIGINT Requirements Validation and Evaluation Subcommittee (of SIGINT Committee)
SIS	(1) Significant Indications Summary; (2) Space Intelligence System; (3) Special Intelligence Support; (4) Selective Inquiry System; (5) Special Information System
SISOCS	Army Logistics/Maintenance Depot Data Network
SISR	SIGINT Security Regulation
SISS	(1) Survivable Intelligence Support to SlOP; (2) Subcommittee on Information Systems Security of the NSTISSC
SISUM	Sensitive Information Summary
SIT	Specialized Investigations Team
SITAS	Strategic Industrial Target Analysis Systems
SITDEV	Situation Development
SITMAP	Situation Map

SITREP	Situation Report
SITS	Secondary Imagery Transmission System
SITSUM	Situation Summary
SITTP	(US)STRATCOM Intelligence Tactics, Techniques, and Procedures for Strategic Operations
SIW	Strategic Intelligence Wing
SJA	Staff Judge Advocate
SJCS	Secretary, Joint Chiefs of Staff
SKCATL	South Korea Conventional Air Target List
SKE	Station-Keeping Equipment
SKYLINK	Communications System Provided by the Diplomatic Telecommunications System
SKYNET	United Kingdom Military Communications Satellite
SL	Sea Level
SLA	Special U.S. Liaison Advisor
SLAM	Standoff Land Attack Missile (Navy)
SLAR	Side-Looking Airborne Radar
SLAT	Surface-Launched Air-Targeted
SLBM	Submarine-Launched Ballistic Missile
SLC	Space Launch Complex
SLCM	(1) Submarine-Launched Cruise Missile; (2) Sea-Launched Cruise Missile
SLDCOM	Satellite Launch Dispenser Communications
SLED	Safe Low-Energy Detonators
SLEP	Service Life Extension Program
SLF	Super Low Frequency
SLFCS	Survivable Low Frequency Communications System
SLGR	Small Lightweight Global Positioning System Receiver
SLIP	Serial Line Interface Protocol
SLMM	U.S. Submarine-Launched Mobile Mine
SLO	Space Liaison Officer
SLOC	Sea Lines of Communication
SLOC(S)	Sea Line(s) of Communication
SLR	Side-Looking Radar
SLS	Space Launch Squadrons
SLSSM	Submerged-Launched Surface-to-Surface Missile
SLV	Space Launch Vehicle
SM	(1) Memorandum by the Secretary, JCS; (2) Statute Mile; (3) Service Member; (4) Security Monitor; (5) Smart Modules
SMAA	Submarine Movement Advisory Authority
S/MANCO	Space/Missile Analyst NCO
SMANCO	Space/Missile Analyst NCO
SMART-T	Secure Mobile Antijam Reliable Tactical Terminal
SMCC	Survivable Mobile Command Center
SMDPS	Strategic Mission Data Preparation System
SME	Subject Matter Expert

Page 3456 of 3957

SMEB	Significant Military Exercise Brief
S/MEO	Space/Missile Event Office
SMG	Standard Mail Guard
SMIOC	Senior Military Intelligence Officers' Conference
SMLM	Soviet (FSU) Military Liaison Mission
SMM	(1) Spatial Model Matching; (2) Special Mission Mandatory Modification
SMO	(1) Support to Military Operations; (2) Senior METOC Officer; (3) Special Mission Optional Modification
SMOB	Strategic Missile Order of Battle
SMOTEC	Special Missions Operational Test and Evaluation Center
SMP	Soviet Military Power (the publication)
SMPAS	Space Mission Payload Assessment System
SMR	Sources, Methods, and Rationale
SMS	Stand-Alone Analysis Subsystems
SMTP	Single Mail Transfer Protocol
SMU	Secure Mobile Unit
SNA	(1) Soviet Naval Aviation; (2) System Network Architecture
SNAP	Soviet (FSU) Nuclear Artillery Projectile
SNCCDIPP	Selected Non-Communist Countries DIPP
SNDV	Strategic Nuclear Delivery Vehicles
S/NF	Secret/NOFORN
SNF	(1) Short-Range Nuclear Forces; (2) Secret NOFORN
SNI	Soviet (FSU) Naval Infantry
SNIE	Special National Intelligence Estimate
SNIP	Soviet (FSU) Naval Imagery Panel
SNM	Special Nuclear Materials
SNMS	Security and Network Management Segment
SNO	Special Naval Operations
SNR	Signal-to-Noise
SNS	Shared Network Server
SNUTR	SIGINT Numerical Tasking Register
SO	Special Operations
SO/LIC	Special Operations/Low Intensity Conflict
SOA	(1) Special Operations Aviation; (2) Special Operations Area; (3) Speed of Advance
SOAB	(1) Special Operations Aviation Battalion; (2) Special Operations Aviation Brigade
SOAC	(1) Special Operations Aviation Command; (2) Special Operations Aviation Company; (3) Special Operations Acquisition Center
SOAD	Special Operations Aviation Detachment
SOADS	Special Operations Automated Data System
SOAE	Deputy for Acquisition and Acquisition Executive
SOAG	Special Operations Aviation Group
SOAR	(1) Special Operations Aviation Regiment; (2) Special Operations Analytical Reports

Page 3457 of 3957

SOARS	Satellite On-Board Attack Reporting System
SOB	Space Order of Battle
SOC	(1) Special Operations Command; (2) Special Operations Capable; (3) Sector Operations Center; (4) Special Operations Craft
SOCACOM	Special Operations Command-Atlantic Command
SOCC	(1) Sector Operational Control Center; (2) Special Operations Control Center
SOCCE	(1) Special Operations Command Communications Element; (2) Special Operations Command and Control Element
SOCCENT	(1) Special Operations Command Center; (2) Special Operations Command Component, CENTCOM
SOCCMO	Special Operations Command Collection Management Office
SOCCS	Special Operations Combat Control Squadron
SOCCT	Special Operations Combat Control Team
SOCDSS	Special Operations Command Deployable Support Set
SOCET	Special Operations Command Extraction Tool
SOCEUR	Special Operations Command, Europe
SOCJIC	United States Special Operations Command Joint Intelligence Center
SOCKOR	Special Operations Command, Korea
SOC-K	Special Operations Command, Korea
SOCLANT	Special Operations Command, Atlantic
SOCLITE	Special Operations Command Laptop
SOCOM	Special Operations Command
SOCOORD	Special Operations Coordination Element
SOCOS	Special Operations Command Operating Staff
SOCPAC	Special Operations Command, Pacific
SOCRATES	Special Operations Command Research, Analysis, and Threat Evaluation System
SOCSIDS	Special Operations Command - Secondary Imagery Dissemination System
SOCSO	Special Operations Command, South
SOCSOUTH	Special Operations Command, South
SOD	Special Operations Detachment
SODARS	Special Operations Debriefing and Retrieval System
SOEAID	Special Operations Executive Aide
SOF	Special Operations Forces
SOF-IV	Special Operations Forces-Intelligence Vehicle
SOF C4I	Special Operations Forces Command, Control, Communications, Computers, and Intelligence
SOF-MOSS	SOF Modular Remote Sensing System
SOFA	Status of Forces Agreement
SOFATS	Special Operations Forces Aircrew Training System
SOFCOM	Special Operations Forces Command
SOF EW	Special Operations Forces Enhanced Weapons
SOFPAC	Special Operating Forces, Pacific
SOFI	Special Operations Forces Improvements

Page 3458 of 3957

SOF IRIS	Special Operations Forces Imagery Receiver and Intelligence System
SOFIST	Foreign Instrumentation Signals Requirement (a collection management software application)
SOFLAM	Special Operations Forces Laser Acquisition Marker
SOFPARS	Special Operations Forces Planning and Rehearsal System
SOF PLD	Special Operations Forces Protection Laser Defense
SOFPREP	Special Operations Forces Planning, Rehearsal and Execution Preparation
SOF PSA	Special Operations Forces Power Supply Assembly
SOFSA	Special Operations Forces Support Activity
SOFTACS	Special Operations Forces Tactical Assured Connectivity System
SOG	Special Operations Group
SOH	SOF Offensive Handgun
SOHFRAD	Special Operations HF Radio
SOHI	Seminar on Human Intelligence
SOI	(1) Signal Operating Instructions; (2) Signal of Interest; (3) Space Object Identification
SOIC	(1) Space Operational Intelligence Center; (2) Senior Official of the Intelligence Community; (3) Special Operations Intelligence Center
SOICS	Special Operations Improved Cryptographic System
SOIF	Special Operational Intelligence Folders
SOIN	Special Operations Intelligence Notes
SOINT	Staff Officer Intelligence
SOIPS	Special Operations Imagery Production System
SOIS	Special Operations Intelligence System
SOISUM	Space Object Identification Summary
SOIT	Seminar on International Terrorism
SOIWSD	Special Operations Information Warfare Support Demonstration
SOJ	(1) Sea of Japan; (2) Stand-Off Jamming
SOJTF	Special Operations Joint Task Force
SOLANT	South Atlantic
SOLARS	SAC On-Line Analysis and Retrieval System
SOLE	Special Operations Liasion Element
SOLIS	SIGINT On-Line Intelligence (or Information) System
SOLL	Special Operations Low Level
SOLOG	Special Operations Logistics System
SOMA	Status of Mission Agreement
SOME	Satellite Orbit Mission Evaluation
SOMOB	Strategic Offensive Missile Order of Battle
SOMPF	Special Operations Mission Planning Folder
SOMS	Special Operations Media System
SON	Statement of Need
SONAR	Sound Navigation and Ranging
SONET	Synchronous Optical Network

Page 3459 of 3957

SONI	Seminar on National Intelligence
SONMET	Special Operations Naval Mobile Environmental Teams
SOO	Space Operations Officer
SOP	(1) Standard Operating Procedure(s); (2) Senior Officer Present
SOPE	Special Operations Planning Exercise
SOPEO	Special Operations Program Executive Officer
SOPIF	Special Operations Photographic Interpretation Facility
SOPM	Special Operations Program Manager
SOPPC	Special Operations Photo Processing Cell
SOPPREP	Special Operation Forces Planning, Rehearsal, and Execution System
SOPS	(1) Space Operations Squadron; (2) Special Operations Power Sources
SOR	(1) Specific Orders and Requests; (2) Statement of Requirements
SORD	System Operational Requirements Document
SORDAC	Special Operations Research, Development and Acquisition Center
SORFMS	Special Operations Radio Frequency Management System
SORS	(1) Specific Order or Requests; (2) SIGINT Overhead Reconnaissance Subcommittee
SORTIEALOT	Sortie Allotment
SORTIC	Seminar on Reconnaissance and Technical Information Collection
SORTS	Status of Resources and Training System
SOS	(1) International Distress Signal (2) Squadron Officers' School; (3) Special Operations Squadron
SOSC	Special Operations Support Command
SOSS	Satellite Ocean Surveillance System
SOSST	Special Operations Small Secure Transceiver
SOST	Special Operations Special Technology
SOSTI	Seminar on Scientific and Technical Intelligence
SOSOS	U.S. Sound Surveillance System
SOT-A	Special or Support Operations Team-Alpha
SOTA	SIGINT Operational Tasking Authority
SOTAS	Standoff Target Acquisition System
SOT-B	Special or Support Operations Team-Bravo
SOTF	(1) Special Operations Task Force; (2) Security Operations Training Facility
SOTSE	Special Operations Theater Support Element
SOTVS	Special Operations Tactical Video System
SOTW	Special Operations Training Wing
SOUTHAM	South America
SOUTHCOM	Southern Command
SOVPACFLT	Soviet Pacific Fleet
SOW	(1) Statement of Work; (2) Special Operations Wing
SOW/TE	Special Operations Weather/Technical Element
SOWG	Special Operations Working Group

Page 3460 of 3957

SOWT	Special Operations Weather Team
SP	(1) Self-Propelled; (2) Shore Patrol; (3) Security Police
SPA	(1) Special PSYOP Analysis; (2) Special PSYOP Assessment
SPACDEFENSE	Space Defense and Operations/Anti-Satellite (ASAT) Missile System
SPACC	Space Command Center
SPACEAF	Space Air Force (14 AF)
SPACECOM	Space Command (See AFSPACECOM and USSPACECOM)
SPACING	Space Processing and Collection Internals Group
SPAD	Special Advisor
SPADATS	Space Detection and Tracking System
SPADCCS	Space Defense Command and Control System
SPADOC	Space Defense Operations Center
SPADVOS	Spaceborne Direct View Optical Scanner
SPAF	Special Airfield File
SPAIS	South Pacific Air Intelligence System
SPAN	Security Policy Automation Network
SPATS	Strategic Posture and Aerospace Threat Summary
SPB	Special Projects Branch (NATO)
SPC	SIGINT Processing Center
SPCL	Special Purpose Communications Link
SPD	Strategic Posture Display
SPEAR	(1) Signal Processing, Evaluation, Alert and Reporting; (2) SOF Personal Equipment Advanced Requirements
SPEC	Counterterrorism Database
Spec Nav	Special Navy Program
SPECAT	Special Category (Pneumatic Tube Message Precedence)
SPECBOATRON	Special Boat Squadron
SPECBOATUNIT	Special Boat Unit
Spectre	AC-130 H/U Gunship
SPECWAR	Special Warfare
SPETSNAZ	Soviet (FSU) Special Purpose Forces
SPF	(1) Special Purpose Forces; (2) Single Point of Failure
SPG	(1) Self-Propelled Gun; (2) Softcopy Products Group
SPIES	Special Insertion and Extraction System
SPIN	Space Intelligence Notes
SPINS	Special Instructions
SPINTCOM	Special Intelligence Communications (Network)
SPIREP	Spot Intelligence Report
SPIRES	Special Intelligence Reports
SPIRIT	Special Purpose Integrated Remote Intelligence Terminal
SPK	Single Point Key(ing)
SPO	Special Project Officer
SPOC	Space Operations Center
SPOD	Sea Ports of Debarkation

Page 3461 of 3957

SPOE	Sea Ports of Embarkation
SPOT	Satellite Pour l'Observation de la Terre (French)
SPOTREP	Spot Report
SPP	Shared Production Program
SPR	Strategic Petroleum Reserve
SPRAA	Strategic Plans and Research Analysis Agency
SPS	Scratch Pad Store
SPS	Special PSYOP Study
SPSS	Secured Packet Switched Service
SPT	Support
SPTCONF	Support Confirmation
SPTD	Supported
SPTG	Supporting
SPTREQ	Support Request
SQ	(1) Square; (2) Squadron
SQD	Squad
SQDN	Squadron
SQL	(1) Standard Query Language; (2) Structured Query Language
SQN	Squadron
SR	(1) Special Reconnaissance; (2) Short Range; (3) Southern Region; (4) Senior
SRBM	Short-Range Ballistic Missile
SRF	SIGINT Readiness Facility
SRHIT	Small Radar-Homing Intercept Technology (BMD Missile)
SRIG	Surveillance, Reconnaissance, and Intelligence Group
SRIS	Surface Range Imaging System
SROC	Southern Region Operations Center
SRIG	Surveillance, Reconnaissance, and Intelligence Group
SRJOIC	Southern Region Joint Operations Intelligence Center
SRAM	U.S. Short-Range Attack Missile
SRAMII	U.S. Short-Range Attack Missile (XAGM-131A; formerly AASM)
SRAM-T	Short Range Attack Missile - Tactical
SRB	Senior Review Board
SRBM	Short-Range Ballistic Missile
SRC	Strategic Reconnaissance Center
SRCU	SINCGARS Remote Control Unit
SRD	(1) System Requirements Document; (2) Special Research Detachment (U.S. Army)
SRF	(1) Strategic Rocket Forces (USSR); (2) Strategic Reserve Forces; (3) Secure Reserve Force (U.S.); (4) Selected Reserve Force; (5) SIGINT Readiness Facility; (6) SPIRIT Remote Facility (TROJAN)
SRFTL	Secure Reserve Force Target List
SRI	Surveillance, Reconnaissance and Intelligence
SRIG	Surveillance/Reconnaissance Intelligence Group

Page 3462 of 3957

SRINF	Short-Range, Intermediate-Range Nuclear Forces
SRJOIC	Southern Region Joint Operational Intelligence Center
SRMIS	Southern Region Maritime Intelligence Summary
SRO	Sensitive Reconnaissance Operations
SROE	Standing Rules of Engagement
SRP	(1) Sealift Readiness Program; (2) SIOP Reconnaissance Plan
SRR	(1) Survival, Recovery and Reconstitution; (2) Security Requirements Review
SRS	(1) Strategic Reconnaissance Squadron; (2) Software Requirements Specification
SRSG	Special Representative to the Secretary-General
SRT	(1) Strategic Relocatable Target; (2) Standard Remote Terminals
SRW	Strategic Reconnaissance Wing
SRWG	Standing Requirements Working Group
SS	Attack Submarine
SSA	(1) Security Supporting Assistance; (2) Diesel-Powered Auxiliary Submarine; (3) Special Support Activity; (4) SIGINT Support Activity; (5) Soviet (FSU) Strategic Aviation
SSAN	(1) Social Security Account Number; (2) Nuclear-Powered Auxiliary Submarine
SSB	(1) Ballistic Missile Submarine; (2) Standard Software Base; (3) Single Sideband
SSB	Ballistic Missile Submarine
SSBN	Nuclear-Powered Ballistic Missile Submarine
SSBSC	Single Sideband, Suppress Carrier
SSC	(1) Coastal Submarine; (2) Space Surveillance Center; (3) Surface Support Craft
SSCC	Special Security Communications Center
SSCI	Senate Select Committee on Intelligence
SSD	Strategic Studies Detachment
SSE	Special Security Element
SSES	Ships Signal Exploitation Space
SSF	(1) Software Support Facility; (2) Special Service Force
SSG	(1) Cruise Missile Attack Submarine; (2) Special Security Group
SSGN	Nuclear-Powered Cruise Missile Attack Submarine
SSI	(1) Specialty Skill Identifier; (2) Safety, Security and Intelligence
SSIXS	Submarine Satellite Information Exchange Subsystem
SSJ	Self-Screening Jamming
SSLP	Transport Submarine
SSLSM	Single-Source Logistics Support Manager
SSM	(1) Surface-to-Surface Missile; (2) Midget Submarine
SSM/I	Sensor System Microwave Imager
SSM/T	Sensor System Microwave/Temperature
SSMA	Spread Spectrum Multiple Access
SSME	Spread Spectrum Modulation Equipment

Page 3463 of 3957

SSMO	SIGINT Support to Military Operations
SSMOB	Surface-to-Surface Missile Order of Battle
SSMP	Security System Management Plan
SSN	(1) Nuclear-Powered Attack Submarine; (2) Social Security Number; (3) Space Surveillance Network
SSO	(1) Special Security Office; (2) Special Security Office(r)
SSO-INT	Senior Staff Officer-Intelligence (Canadian)
SSP	(1) SIGINT Support Plan; (2) Scheduled Strike Program (NATO); (3) Single-Shot Probability of Damage; (4) Single-Source Processor; (5) SIOP Support Program
SSP-S	Single Source Processor-SIGINT
SSQ	Auxiliary Submarine, Communications
SSQN	Nuclear-Powered Auxiliary Submarine, Communications
SSR	(1) Radar Picket Submarine; (2) Secondary Surveillance Radar; (3) Special Security SSRS Representative SIGINT Surveillance and Reporting System
SSS	(1) Staff Summary Sheet; (2) Systems Science and Software; (3) System Support Segment; (4) Special Support Section
SSSP	Single-Source SIGINT Processor
SST	(1) Training Submarine; (2) System Specific Threat; (3) Supersonic Transport; (4) Single Subscriber Terminal; (5) Safe Secure Transport; (6) Strategic Support Team; (7) Space Support Team
SSTO	Single-Stage-To-Orbit
SSTS	Space Surveillance and Tracking System
SSUS	Spin-Stabilized Upper Stage
ST	(1) SEAL Team; (2) Strategic Task; (3) Short Tons
S&T	Scientific and Technical
S&TI	Scientific and Technical Intelligence
ST&E	Security Test and Evaluation
STA	Surveillance and Target Acquisition
STACCS	Standard Theater Army Command and Control System
STAMIS	Standard Army Management Information System
STAMP	SOUTHCOM Topographic Augmentation Program
STAMPS	Stand-Alone Message Processing System
STANAG	Standardization Agreement (NATO)
STANAVFORLANT	Standing Naval Force, Atlantic (NATO)
STAN-EVAL	Standardization and Evaluation
STANS	(1) Soviet Tactical Nuclear Study; (2) Space Target Analysis and Networking System
STAP	Science and Technology Advisory Panel
STAR	(1) Surface-to-Air Recovery; (2) System Threat Assessment Report
STARC	State Area Command
STARS	Surveillance, Target Acquisition & Reporting System
STAR-T	SHF Tri-Band Advanced Range Extension Tactical Terminal
START	Strategic Arms Reduction Talks/Treaty

Page 3464 of 3957

STARTEX	Start Date of an Exercise
STASS	Submarine-Towed Array Surveillance System
STATDM	Statistical Time Division Multiplex
Static RI	Static Infrared Workstation
STATS	Strategic Target Analysis and Tracking System
STATSIONAR	USSR/Russian COMSAT System
STC	(1) Sensitivity Time Control; (2) Short Time Constant (ECCM); (3) SHAPE Technical Center
STCFE	Science and Technology Center Far East
STD	(1) SIGINT Technical Data; (2) Standard
STEL	Stanford Telecommunications
STEP	Standardized Technical Entry Point
STEPS	Scientific and Technical ELINT Processing System
STEPS II	Scientific and Technical ELINT Processing System II
STG	Special Tactical Group
STEL	Secure Telephone
S&TI	Scientific and Technical Intelligence
STIC	(1) Scientific and Technical Intelligence Committee; (2) Scientific and Technical Intelligence Center
STICS	Scalable Transportable Intelligence Communications System
STIFF	Strategic Intelligence Forecast File
STIISP	Scientific and Technical Intelligence Information Services Program
STINT	Science and Technology (S&T) Intelligence
STIR	Scientific and Technical Intelligence Register
STITEUR	Scientific and Technical Information Team, Europe
STK	(1) Satellite Took Kit; (2) Strike
STO	Science and Technology Objectives
STOL	Short Takeoff and Landing
STON	Short Ton
STOPS	Stand-Off Optical System
STOVL	Short Takeoff, Vertical Landing
STP	(1) Space Test Program; (2) Site Transition Plan
Str	Strength
STRAM	Static Random Access Memory
STRAT	Strategic
STRATCOM	Strategic Command
STRATJIC	USSTRATCOM Joint Intelligence Center
STRATLAT	Strategic Command Liaison Assistance Team
STRATMAS	Strategic Message Analysis Server
STRATPAT	Strategic Planning and Analysis Tool
STRED	Standard-Tactical Receive Equipment Display STRICOM Simulations, Training, and Instrumentation Command
STRIKFORSOUTH	Strike Force South
S-TRED	Standard Tactical Receive Equipment Display
STRUM	Standard Technical Reporting Using Modules

Page 3465 of 3957

STS	(1) Special Training Standard; (2) Special Tactics Squadron; (3) Subcommittee on Telecommunications Security of the NSTISSC
STT	(1) Small Tactical Terminal; (2) Special Tactics Teams; (3) Shore Targeting Terminal
STU	Secure Telephone Unit (STU II & III)
STU-III	Secure Telephone Unit III
STUR	Secure Telephone Unit/Remote
STVD	Southern Theater of Military Operations (FSU)
STW	Strike Warfare
STWC	Strike Warfare Commander
STX	Situational Training Exercise
SUAWACS	Soviet (FSU) AWACS
SUBACS	Submarine Advanced Combat System
SUBLANT	Submarine Forces, Atlantic
SUBOPAUTH	Submarine Operating Authority
SUBORD	Subordinate
SUBPAC	Submarine Forces, Pacific
SUCCESS	Secure UHF Computer Controlled Equipment Subsystems
SUG	SAFE Users Group
SUM	(1) Surface-to-Underwater Missile; (2) Structural Usage Monitor
SUMS	Structural Usage Monitor System
SUPCOM	Support Command
SUPINTREP	Supplementary Intelligence Report
SUPIR	(1) Supplemental Photographic Interpretation Report; (2) Supplemental Phase Interpretation Report
SUPNAVFOR	Supporting Naval Force
SUPPLOT	Supplemental Plot
SUPREMS	Supplemental Preliminary Mission Summary
SUPT	Superintendent
SURAN	Southeastern Universities
SURFSHIP	Surface Ship
SURFWARDEVGRU	Surface Warfare Development Group
SURTASS	Surveillance Towed Array Sonar System (U.S.)
SURV	Surveillance
SUSLAK	Special U.S. Liaison Activity Korea
SUSLO	Special U.S. Liaison Officer
SV	(1) Secure Voice; (2) Special View
SVC	Service
SVCN	Secure Voice Conferencing Network
SVD	Soviet Sniper Rifle
SVGA	Super Video Graphics Adapter
SVIP	Secure Voice Improvement Program
SVOD	Soviet Aircraft Navigation and Landing System
SVS	Secure Voice System
SVTC	Secure Voice Teleconferencing

Page 3466 of 3957

SVTS	Secure Video Teleconferencing System
SW	(1) Short Wave; (2) Surface Warfare; (3) Software; (4) Strategic Wing
S&W	Surveillance and Warning
SWA	(1) Southwest Asia; (2) Southwest Africa; (3) Standoff Weapons Assembly; (4) Senior Warning Analyst; (5) Senior Weather Analyst; (6) Secure Work Area
SWADII	Southwest Asia Defense Information Infrastructure
SWAL	Shallow-Water Attack Craft, Light
SWAM	Shallow-Water Attack Craft, Medium
SWAT	SOCRATES WS/LAN Analysis Testbed
SWB	Southwest Border
SWC	(1) Special Warfare Center (U.S. Army); (2) Special Warfare Craft; (3) Strategic Warfare Center; (4) Strategic Warning Center; (5) Space Warfare Center
S&WC	Surveillance and Warning Center/Control
SWCL	Special Warfare Craft, Light
SWCM	Special Warfare Craft, Medium
SWCS	Special Warfare Center and School
SWE	Sweden
SWHQ	Static War Headquarters
SWI	Special Weather Intelligence
SWIR	Short Wave Infrared
SWIRTERCAT	SWIR Terrain Categorization
SWIS	Survivable Wartime Intelligence System
SWO	(1) Special Weapons Officer; (2) Staff Weather Officer; (3) Senior Watch Officer
SWORD	Submarine Warfare Operations Research Department
SWP	Standing Warning Program
SWPS	Space & Weapons Systems SIGINT Working Group
SWR	Southwest Region
SWRS	Slow-Walker Reporting System
SWSC	Space Warning Systems Center
SWTMO	SW Theater of Military Operations
SYBASE	A Collection Requirements Database
SYDET	Sympathetic Detonator
SYDP	Six-Year Defense Plan
SYG	Secretary General
SYNCOM	Synchronous Communications Satellite
SYRACUSE	Systeme de Radio Communication Utilisant un Satellite
SYRUP	System Resource Utilization Package
SYS	System(s)
SYSADM	System Administrator
SYSADMIN	Systems Administration Technical Assistant
SYSCON	Systems Control
SYSOPR	System Operator

Page 3467 of 3957

T

T	(1) Tank; (2) Training; (3) Transmitter
T1	1.54 Megabits per Second Throughput
T2	Technology Transfer
T3	44.3 Megabits per Second Throughput
TA	(1) Traffic Analysis; (2) Tank Army; (3) Terrain Avoidance; (4) Theater Army; (5) Target Acquisition; (6) Target Analysis
T&A	Transcription and Analysis
TAA	(1) Tactical Air Army (FSU); (2) Total Army Analysis; (3) Tactical Assembly Area; (4) Theatre Army Area
TAACOM	Theater Army Area Command
TAB	(1) Target Acquisition Battery; (2) Theatre Air Base
TABNR	Table Number
TABS	Threat Assement Briefing System
TAC	(1) Tactical Air Command; (2) Terrain Analysis Center (U.S. Army); (3) Tactical Access Controller; (4) Tri-Service Tactical Digital Communication System; (5) Technology Assessment Center; (6) Terminal Access Control; (7) Tactical Command Post
TACAC-D	Technical Control and Analysis Center-Division
TACAIR	Tactical Air
TACAMO	(1) U.S. Air Relay Communication System; (2) Take Charge and Move Out
TACAN	Ultrahigh-Frequency Tactical Air Navigation
TACAWS	The Army Combined Arms Weapons System
TACC	(1) Tactical Air Control Center; (2) Tanker Airlift Control Center; (3) Theater Army Communications Command
TACC(A)	Tactical Air Control Center (Afloat)
TACCIMS	(1) Theater Army Command and Control Information Management System; (2) Tactical Command and Control Information Management System
TACCP	Tactical Command Post
TACCS	(1) Tactical Airborne Command and Control and Surveillance; (2) Tactical Air Control Center System
TACCSIMS	Theater Area Command and Control Information Management System
TACCS-K	Tactical Automated Command and Control Systems-Korea
TACCTA	Tactical Commander's Terrain Analysis
TAC-D	Tactical Deception
TACE	(1) Technical Analysis Cost Estimate; (2) Tactical Air Coordination Element
TACELINT	Tactical Electronic Intelligence (Report)
TACFAST	Tactical Forward Analysis Support Terminal
TACFIRE	Tactical Artillery Fire Control
TACIES	Tactical Imagery Exploitation System
TACINTEL	Tactical Intelligence
TACIT RAINBOW	Anti-Radiation Missile

Page 3468 of 3957

TACM	Tactical Amphibious Collection Management
TACO	Tactical Command Post
TACO-2	Tactical Communications-Two
TACOMM	Tactical Communications
TACOMSIM	Tactical Communications Simulator
TACON	Tactical Control
TACOPS	Tactical Air Combat Operations Staff
TACP	Tactical Air Control Party
TACRECCE	Tactical Reconnaissance
TACREP	Tactical Report
TACRON	Tactical Air Control Squadron
TACS	(1) Tactical Air Control System; (2) Technology Acquisition Coordination Subcommittee; (3) Theater Air Control System
TACS/TADS	Tactical Air Control System/Tacticai Air Defense System
TACSAM	Tactical Surface-to-Air Missile
TACSAT	Tactical Satellite
TACSATCOM	Tactical Satellite Communications
TACSIM	Tactical Simulation (Simulator)
TACTAS	Tactical Towed Array System (U.S. Surface Warship)
TACTASS	Tactical Towed-Array Surveillance System (USN)
TACTED	Tactical Trunk Encryption Device
TACTEL	Tactical Telecommunications
TACTERM	Tactical Terminal
TACW	Tactical Air Control Wing
TACWINGSLANT	Tactical Wings Atlantic
TAD	(1) Temporary Additional Duty; (2) Theater Air Defense
TADIL	Tactical Data Information Link
TADIL-J	Tactical Digital Interface Link-Joint
TADIX-B	Tactical Data Exchange System-B
TADIXS	Tactical Data Information Exchange Subsystem
TADIXS-B	Tactical Data Information Exchange System Broadcast
TADS	(1) Tactical Air Defense System; (2) Target Acquisition and Designation System
TADSS	Training Aids, Devices, Simulations and Simulators
TADMS	TRS ASARS-2 Data Manipulation System
TAE	Transportable Applications Executive
TAF	Tactical Air Forces
TAFIC	Tactical Air Forces Intelligence Center
TAFIES	Tactical Air Force Intelligence Exploitation System
TAFIIS	Tactical Air Forces Integrated Information System
TAFLC	Tactical Air Force Limited Operational Capabilities Europe
TAFSM	Tactical Fire Support Model
TAG	(1) Target Actions Group; (2) The Adjutant General; (3) Theater Army Group; (4) Target Aimpoint Graphic; (5) TEMPEST Advisory Group
TAGS	Theater Air Ground System

Page 3469 of 3957

TAH	Tactical Aviation Headquarters
TAI	Target Areas of Interest
TAISS	Telecommunication and Automated Information Systems Security
TALM	Tactical Air-Launched Missile
TALO	Tactical Airlift Liaison Officer
TALON	Theater Applicatiaon-Launch on Notice
TAOS	Thrust-Assisted Orbiter System
TALP	Total Army Linguist Program
TAMPS	(1) Threat Avoidance Mission Planning System; (2) Tactical Aircraft Mission Planning System
TANGO	Tactical Air, Naval, Ground Operations
TAO	Tactical Air Operations
TAOC	Tactical Air Operations Center
TAOR	Tactical Area of Responsibility
TAP	(1) Terrain Analysis Program; (2) Theater Analysis and Planning
TAPA	Target Analysis Pacific Area
TAPCOMP	Targeting and Analysis Program Computers
TAPS	Technical Analysis Processing System
TAR	Terrain Avoidance Radar
TARBUL	Target Bulletin
TARDEV	Target Development
TARE	Telegraph Automation Relay Equipment
TAREX	Target Exploitation
TARM	Tactical Antiradiation Missile
TARPS	Tactical Air Reconnaissance Pod System (USN)
TARRRS	Tactical Air Reconnaissance Results Reporting System
TARS	Tactical Air Reconnaissance System
TAS	(1) Tactical Airlift Squadron; (2) Traffic Analysis Survey; (3) Terminal Access System; (4) True Air Speed; (5) Timeline Analysis System; (6) Temporal Analysis System
TASE	Tactical Air Support Element
TASES	Tactical Airborne Signals Exploitation System
TASM	Tactical Air-to-Surface Missile
TASMO	Tactical Air Support of Maritime Operations
TASO	Terminal Area Security Officer
TASOC	Theater Army Special Operations Command
TASOSC	Theater Army Special Operations Support Command
TASS	(1) Towed Array Surveillance System; (2) Official News Agency of the FSU; (3) Tactical Air Support Squadron; (4) Tactical Automatic Switching System
TAT	(1) Terrorist Action Team; (2) Tactical Analysis Team; (3) Target Area Tactics
TATERS	TROJAN Air Transportable Electronic Reconnaissance System
TAV	(1) Total Asset Visibility; (2) Trans-Atmospheric Vehicle
TAVR	Territorial and Army Volunteer Reserve
TAW	Tactical Airlift Wing

Page 3470 of 3957

TAWC	Tactical Air Warfare Center
TAWDS	Transportable Automated Weather Distribution System
TAXIS-A	Tactical Data Information Exchange Subsystem A
TB	(1) Tank Battalion; (2) Tuberculosis
TBA	To Be Announced
TBD	To Be Determined
TBM	(1) Tactical Ballistic Missile; (2) Theater Battle Management; (3) Theater Ballistic Missile
TBP	To be published
TC	(1) Tank Company; (2) Transportation Corps; (3) Transport Cradles
TC3	Theater Command, Control, and Communications
TCA	(1) Theater Collection Assets; (2) Theater Communications Architecture; (3) Tactical Communication Augmentation
TCAC	Technical Control and Analysis Center
TCAC-C	Technical Control and Analysis Center - Corps
TCAC PIP	Technical Control and Analysis Center-Product
TCAE	(1) Technical Control and Analysis Element; (2) Tactical Control and Analysis Element
TCAE C/D/B	Technical Control and Analysis Element Corps/Division/Brigade
TC-AIMS II	Transportation Coordinator Automated Information For Movements Systems II
TCB	Trusted Computing Base
TCC	(1) Telecommunications Center; (2) Tactical Command Center
TCCC	Theater Communications Control Center
TCCE/CA	Theater Contingency Communications Equipment, Central Area
TCCS	Theater Command and Control System
TCD	Time Compliance Data
TCICA	Theater Counterintelligence Coordinating Authority
TCIM	Tactical Communications Interface Module
TCJ2	TRANSCOM J2
TCM	Tactical Cruise Missile
TCMS	Tactical Communications Management System
TCO	(1) Test Control Officer; (2) Telecommunications Control Officer; (3) Telecommunications Contracting Office
TCOS	Tactical Combat Operations System
TCP	(1) Technological Coordinating Paper; (2) Tactical Cryptologic Program; (3) Transmission Control Protocol; (4) Traditional CINC Programs
TCP/IP	Transmission Control Protocol/Internet Protocol
TCR	Time Critical Requirements
TCS	(1) Tactical Computer System; (2) Test/Crisis Service
TCSEC	DOD Trusted Computer System Evaluation Criteria
TCT	(1) Tactical Commanders Terminal; (2) Tactical Computer Terminal(s)
TCU	Tactical Computer Unit

Page 3471 of 3957

TD	(1) Tank Destroyer; (2) Tank Division; (3) Time Dominant (imagery); (4) Tactical Deception; (5) Training Detachment; (6) Target Designator; (7) Transfer Device
TDA	(1) Table of Distribution and Allowances; (2) Target Damage Assessment; (3) Tactical Decision Aids
TDAD	Training Development and Analysis Directorate
TDAR	Tactical Defense Alert Radar
TDC	(1) Tactical Digital Computer; (2) Theater Deployable Communications
TDD	Target DBZ Designator
TDDP	Tactical Defense Dissemination Program
TDDS	(1) Tactical Defense/Data Dissemination System; (2) TRAP Data Dissemination System
TDES	Theater Document Exploitation System
TDF	(1) Tactical Data Facsimile; (2) Tactical Digital Facsimile
TDFD	Time Delay Firing Device
TDI	(1) Target Data Inventory; (2) Target Data Inventory; (3) ETIBS Datalink Interface
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TDOA	Time Difference of Arrival
TDP	(1) Threat Display & Projection; (2) Tactical Display Programmer; (3) Tactical Data Processor
TDRSS	Tracking and Data Relay Satellite System
TDS	(1) Target Data Sheet; (2) Training Device System; (3) Target Development System
TDSS	Theater Display Support System
TDT	Tactical Data Terminal
TDY	Temporary Duty
TE	(1) Tactical Exploitation; (2) Table of Equipment
T&E	Test & Evaluation
TEA	Tactical Exploitation Assessment
TEAMS	Trend and Error Analysis Methodology System
TEARR	Time, Elevation, Azimuth, Range, Range Rate
TEB	Tactical Exploitation Battalion
TEC	Topographic Engineering Center
TECCE	Tactical Exploitation Collection and Coordination Element
TECH	Technical
TECHELINT	Technical ELINT
TECHINT	Technical Intelligence
TECHLIB	Technical Library
TECHSUM	Technical Summary
TECRAS	Technical Reconnaissance and Surveillance
TED	Trunk Encryption Device
TEDB	Technical ELINT Data Base
TEDS	Tactical Expendable Drone System
TEG	Tactical Exploitation Group (JSIPS)

Page 3472 of 3957

TEK	Traffic Encryption Key
TEL	Transporter-Erector-Launcher
TELAR	Transporter-Erector-Launcher and Radar
TELCON	Telephone Conversation
TELECOM	Telecommunications
TELEFAC	Telecommunications Facilities Vulnerability Study
TELINT	Telemetry Intelligence
TELNET	Telecommunications Network
TEMP	Test and Evaluation Master Plan
TEMPEST	(1) Unclassified Name for Compromising Emanations; (2) Compromising Electronic Emission Control Program; (3) Transient Electromagnetic Pulse Emanations
TENCAP	Tactical Exploitation of National Capabilities
TEOC	Technical Objective Camera
TEP	(1) Tactical ELINT Processor; (2) TEMPEST Endorsement Program
TEPP	Tomahawk Employment Planning Package
TERCAT	Terrain Categorization
TERCOM	Terrain Contour Matching
TEREC	(1) Tactical Electronic Reconnaissance; (2) Tactical ELINT Receiver
TERPES	Tactical Electronic Reconnaissance Processing and Evaluation System
TERS	(1) Tactical Electronic Reconnaissance System; (2) Tactical ELINT Reporting System; (3) Tactical Event Reporting System
TES	(1) Tactical Electronic Squadron; (2) Tactical Event System
TESAR	Tactical Endurance Synthetic Aperture Radar
TESS	Tactical Engagement Simulation System
TET	Transportable Electronic Tower
TEWS	Tactical Electronic Warfare System
TEXAS	Tactical Exchange Automation System
TF	(1) Task Force; (2) Transaction Format
TFAS	Task Force Able Sentry
TFC	Tactical Fusion Center
TFCICA	Task Force CI Coordinating Authority
TFCC	Tactical Flag Command Center
TFJ2	Task Force Director of Intelligence
TFM	Trusted Facility Manual
TFR	Terrain Following Radar
TFS	(1) Tactical Fighter Squadron; (2) Terrain and Feature Server; (3) Traffic Flow Security
TFT	(1) Tri-Band Field Terminal; (2) Tactical Facsimile Terminal
TF/TA	Terrian Following/Terrain Avoidance
TFU	Tactical Forecast Unit
TFW	Tactical Fighter Wing
TFWC	Tactical Fighter Weapons Center

Page 3473 of 3957

TG	(1) Task Group; (2) Training Group
T&G	Tracking and Guidance
TGA	Target Analysis
TGCF	Tactical Ground Control Facility
TGIF	Transportable/Tactical Ground Intercept Facility
TGPF	Transportable Ground Processing Facility
TGS	(1) Transportable Ground Station; (2) Turkish General Staff
TGT	Target
TGTINT	Targeting Intelligence
TGTINFOREP	Target Information Report
TGW	Terminal-Guidance Warhead
THAAD	Theater High-Altitude Area Defense
THAAD/GBR	Theater High-Altitude Area Defense/Ground Based Radar
THEC	Theater HUMINT Exploitation Center
THMT	Tactical High Mobility Terminal
THREATCON	JCS Terrorist Threat Condition
THz	Terahertz
TI	(1) Technical Intelligence (TECHINT); (2) Target Intelligence; (3) Transition Increment
TI/TTR	Target Illumination/Target Tracking Radar
TIA	Target Implications Annex
TIAP	Theater Intelligence Architecture Program
TIAPCO	TIAP Communications Overlay
TIARA	Tactical Intelligence and Related Activities
TIARRA	Target Identification And Recognition Radar
TIAS	Target Identification & Acquisition System
TIB	Target Intelligence Branch
TIBS	Tactical Information Broadcast System
TIC	(1) Theater Intelligence Center; (2) Technical Information Center
TICANA	Tactical Imagery Communications and Network Alternatives
TICC	Tactical Information Communications Center
TICON	Tight Control
TID	Theater Intelligence Digest
TIDL	Tactical Imagery Data Link
TIDY	Teletype Integrated Display System
TIEC	Theater Imagery Exploitation Capability
TIES	Tactical Information Exchange System
TIF(S)	Theater Interrogation Facility(ies)
TIFA	Theater Intelligence Fusion Architecture
TIFF	Tagged Image File Format
TIG	Tactical Intelligence Group
TIHB	Target Intelligence Handbook
TIIF	Tactical Imagery Interpretation Facility
TIIMS	Text and Image Information Management System
TILO	Transportation Intelligence Liaison Officer

Page 3474 of 3957

TIM	Target Intelligence Material
TIM-DIS	Time & Distance
TIMS	(1) Tactical Information Management System; (2) TFCC Information Management System
TIO	Target Intelligence Officer
TIP	(1) Target Intelligence Package; (2) Theater Intelligence Plan; (3) Tracking and Impact Prediction; (4) Tactical Imagery Program
TIPE	Tactical Intelligence Product Enhancement
TIPI	Tactical Information Processing and Interpretation System
TIPP	Target Intelligence Production Plan
TIPS	(1) Terrorist Incident Profile System; (2) Tactical Intelligence Processing System; (3) Target Intelligence Packages
TIR	Terminal Imaging Radar
TIROS	Television Infrared Observation Satellite
TIROS-N	Television Infrared Observation Satellite-National
TIRS	Thermal Infrared Scanner
TIRSAG	Tactical Intelligence, Reconnaissance, Surveillance Action Group
TIRSS	Theater Intelligence, Reconnaissance & Surveillance Study
TIS	(1) Tactical Intelligence Squadron; (2) Thermal Imaging Sight; (3) Tactical Input Segment
TISD	Tactical (Air Forces) Integrated Situation Display
TISEO	Target Identification System, Electro-Optical
TISL	Target Identification System, Laser
TISO	Theater Intelligence Support Officer
TISP	Transition Implementation Support Plan
TISS	Tactical Intelligence Support Staff
TITF	Theater Intelligence Training Facility
TIU	ETIBS Interface Unit
TJS	Tactical Jamming System
TK	Talent-Keyhole
Tk	Tank
TKR	Tanker
TLAM	Tomahawk Land Attack Missile
TLAR	Transporter-Launcher and Radar
TLC	(1) Telecommunication Link Controller; (2) Teleconferencing
TLCF	(1) TACINTEL Link Control Facility; (2) Teleconferencing
TLE	Target Location Error
TLS	Top-Level Specification
TLST	TACAMO Logistics Support Team
TM	(1) Tactical Missile; (2) Threat Manager; (3) Target Material; (4) Landsat Thematic Mapper; (5) Technical Manual; (6) Team Materials; (7) Team
TMA	Theater of Military Action
TMB	Technical Management Board
TMCN	Tactical Target Materials Change Notice

Page 3475 of 3957

TMD	(1) Theater Missile Defense; (2) Tactical Map Depot
TMDE	Test Measurement and Diagnostic Equipment
TMD/GBR	Theater Missile Defense/Ground-Based Radar
TMET	Transportable Medium Earth Terminal
TMFU	Theater METOC Forecasting Unit
TMMRS	Trojan Mobile Remote Receiver System
TMO	(1) Technical Management Office; (2) Theater of Military Operations
TMP	Training Management Plan
TMPC	Theater Mission Planning Center
TMPG	Target Materials Producers Group
TMPO	Target Materials Program Office
TMPS	Theater Mission Planning System
TMRG	Terrain-Masked Radar Graphics
TMSR	Tactical Meteorological Satellite Receiver
TMS	Target Materials Squadron
TMT	Target Marking Technologies
TMUG	Target Materials Users Group
TMWG	Target Materials Working Group
TMWS	Target Materials Workstation
TNAPS+	Tactical Network Analysis and Planning System Plus
TNET	Teletraining Network
TNF	Theater Nuclear Forces
Tng	Training
TNI	Trusted Network Interpretation
TNIEG	Trusted Network Interpretation Environment Guideline
TNK	Tanker
TNL	Target Nomination List
TNT	Tunnel Neutralization Team
TNO	Theater Nuclear Option
T/O	Take Off
TO&E	Tables of Organization and Equipment
TOA	(1) Total Obligational Authority; (2) Time of Arrival; (3) Transportation Operation Agency; (4) Time of Attack; (5) Transfer of Authority; (6) Table of Organic Allowance
TOC	(1) Tactical Operations Center; (2) Theater of Operations Command
TOE	(1) Table of Organization and Equipment; (2) Time of Entry
TOF	Time of Flight
TOPCAT	Tactical Operations Planner for Collection, Analysis, and Tasking
TOPINS	Theater Operational Intelligence System
TOPO	Topographic
TOPS	Tactical Operations Support
TOR	(1) Terms of Reference; (2) Tactical Operations Room; (3) Tentative Operational Requirement; (4) Time of Receipt
TORP	Torpedo

TORPCM	Torpedo Countermeasures & Deception
TOS	(1) Tactical Ocean Surveillance; (2) Theater Operating System
TOSP	Tailored Ocean Surveillance Product
TOSS	(1) Tactical Operations Support System; (2) Technical Oriented Support System
TOT	(1) Time over Target; (2) Time of Transmission
TOVS	TIROS Operational Vertical Sounder
TOW	Tube-Launched Optically-Tracked Wire-Guided Missile
T/P	Terminal/Printer
TPA	Theater Production Assets
TPAS	Target Planning and Scheduling
TPC	(1) Tactical Pilotage Chart; (2) Tempest Personal Computer; (3) Two-Person Control
TPCS	Team Portable COMINT System
TPEP	(1) TEREC Portable Exploitation Processor; (2) Trusted Products Evaluation Program
TPF	Topographic Production Facility
TPFD	Time-Phased Force Deployment
TPFDD	Time-Phased Force Deployment Data
TPFD(L)	Time-Phased Force Deployment (List)
TPI	Two-Person Integrity
TPL	Time-Phased Line
TPN	Tactical Packet Network
TPP	Thermal Powerplant
TPS	(1) Thermal Protection System; (2) Telecommunications Prioritization System
TPSD	(1) Theater Planning Support Division (J-5); (2) Theater Planning Support Document
TPU	Troop Programs Units
TPV	Terrain Perspective Viewing
TQL	Total Quality Leadership
TQM	Total Quality Management
T/R	Transmit-Receive
TR	(1) Tank Regiment; (2) Transportation Request
TRA	Temporary Restricted Areas
TRAC	(1) Tactical Radar Correlator; (2) TRADOC Analysis Center
TRADOC	U.S. Army Training and Doctrine Command
TRAINS	Interactive Video Teletraining System
TRAM	Target Recognition and Attack-Multisensor
TRANSCOM	Transportation Command
TRANSEC	Transmission Security
TRANSIT	Navy Navigation Satellite System
TRANSNAT	Transnational
TRAP	(1) Threat Research and Analysis Program; (2) TRE and Related Applications; (3) Terrorist Research and Analysis Project; (4) Tactical Related Applications
TRAP-I	TRAP-Improved

Page 3477 of 3957

TRAPS	TRE & Related Applications
TRB	Technical Review Board
TRDL	Tactical Reconnaissance Data Link
TRE	Tactical Receive Equipment
TRED	Tactical Receive Equipment Display
TREDS	(1) Tactical Reconnaissance Exploitation Demonstration System; (2) Tactical Receive Equipment (TRE) Display System
TREE	Transient Radiation Effects on Electronics
TRF	Topographic Readiness Facility
TRICOMS	Triad Computer System
TRI-MEF	Tri-Marine Expeditionary Force
TRI-MEFO	Tri-Marine Expeditionary Force Order
TRITAC	Tri-Service Tactical Communications System
TRI-TAC	(1) U.S. Joint Tactical Communications Program; (2) Tri-Service Tactical Communications
TRIES	Tactical Radar Imagery Exploitation System
TRIGS	TR-1 Ground Station
TRIMSS	TRANSCOM Imagery Management Support System
TRITAF	Tactical Air Forces of TAC, USAFE and PACAF
TRIX(S)	Tactical Reconnaissance Intelligence Exchange System
TRL	Target Recommendation List
TRML	USAFE Target Reference Material List
TRN	(1) Target Reference Number; (2) Target Reference Point
TROFA	Temporary Remote Operating Facility, Airborne (NSA)
TROJAN	Name of Technical Training System
TROJAN SPIRIT	TROJAN Special Purpose Integrated Remote Intelligence Terminal
TROKA	Third ROK Army
TROPO	Tropospheric Scatter Radio
TROSCOM	United States Army Troop Support Command
TRP	(1) Target Reporting Parameters; (2) Theater Response Package
Trp	Troops
TRRIP	(1) Theater Rapid Response Intelligence Package; (2) Tactical Rapid Reaction Intelligence
TRS	(1) Tactical Reconnaissance Squadron; (2) Tactical Reconnaissance System; (3) Trunked Radio System; (4) Telecommunications Service Request
TRSS	Tactical Remote Sensor System
TRT	TEREC Remote Terminal
TRUS	Tilting Wing/Rotor UAV System
TRV	Tank Recovery Vehicle
TRW	Tactical Reconnaissance Wing
TS	(1) Top Secret; (2) Transaction Services; (3) Target Spotting; (3) TROJAN SPIRIT
TSAR	Transmission Security Analysis Report
TSART	Test Support and Analysis Report Terminal
TSB	PSYOP Tactical Support Battalion

Page 3478 of 3957

TSC	(1) Tactical Support Center; (2) Top Secret Control; (3) Technical Support Center; (4) Tactical Support Company; (5) TROJAN Switching Center; (6) Training Support Center
TSC2	Tactical/Strategic Command & Control
TSCA	Time-Sensitive Collection Actions
TSCE	Time-Sensitive Collection Emphasis
TSCIF	Tactical/Temporary Sensitive Compartmented Information Facility
TSCIXS	Tactical Support Center Information Exchange System
TSCM	Technical Surveillance Countermeasures
TSCO	Top Secret Control Officer
TSCR	Time-Sensitive Collection Requirement
TSCS	Transportable Satellite Communications System
TS/SCI	Top Secret/Sensitive Compartmented Information
TSCSI	Temporary Surface Cryptologic Support Installation
TSCW	Top Secret Codeword
TSDS	Tactical SIGINT Data Support
TSE	Target Support Element
TSEC	Telecommuncations Security
TSF	Technical Support Facility
TSG	Threat Steering Group
TSIT	Technical Service Intelligence Team
TSK	Transmission Security Key
TSM	Threat Spectrum Model
TSMA	Theater of Strategic/Military Action
TSOC	Theater Support Operations Cell
TSOR	Technical Standards of Readiness
TSP	(1) Transshipment Point; (2) Training Support Base; (3) Tactical Sensor Planner
TSR	(1) Time-Sensitive Requirement; (2) Telecommunications Support Request; (3) Trans-Siberian Railroad
TSRS	Tactical Support Reconnaissance System
TSS	(1) Telecommunications Security System; (2) Time-Sharing System; (3) Target Summary Sheets; (4) Target Selection Standards
TSSAM	Tri-Service Standoff Attack Missile
TSSR	Tropo Satellite Support Radio
TSSS (TS3)	(1) Tactical Simulator Study Support; (2) Time-Sensitive Support System
TSSTM	Tactical SIGINT Systems Training Module
TST	(1) Tactical Surveillance Technology; (2) Theater Support Team; (3) Tactical Support Team
T-STAR	TRANSCOM Situation Transportation Analysis Review
TS/TM	Target Support/Target Materials
TSWA	Temporary Secure Working Area
TSWG	Technical Support Working Group Of IG/T
TT	(1) Technology Transfer; (2) Target Track

Page 3479 of 3957

TT&C	Telemetry Tracking and Command
TTAC	Technology Transfer Analysis Center
TTADB	Tactical Terrain Analysis Data Base
TTAP	Telemetry Technical Analysis Position
TTBT	Threshold Test Ban Treaty
TTC	(1) Transportation Terminal Command; (2) Tactical Telephone Central
TTD	Tactical Terrain Data
TTG	Technical Training Group
TTI	Tactical Target Illustration
TTIC	Technology Transfer Intelligence Committee
TTM	Tactical Target Materials
TTMC	Tactical Target Materials Catalogue
TTMP	Tactical Target Materials Program
TTMPD	Tactical Target Material Production Document
TTP	Tactics, Techniques, and Procedures
TTPI	Trust Territory of the Pacific Islands
TTR	Target Tracking Radar
TTSB	Theater Tactical Selection Board
TTU	(1) Transportation Terminal Unit; (2) Tape Transport Unit
TTY	(1) Teletypewriter; (2) Teletype
TU	Task Unit
TUDE	Teletype User Display Equipment
TUHTKP	Time Urgent Hard Target Kill Potential
TUSA	Third U.S. Army
TUT	Tactical User's Terminal
TUV	Task Unit Van
TV	(1) Television; (2) Theater of War (FSU); (3) Target Vulnerability
TVA	Target Value Analysis
TVD	Theater of Military Operations (FSU)
TVITS	Tactical Video Imagery Transmission System
TVSSC	TACCIMS VTC Support System
TW	Targeting and Weaponeering
TW/AA	Tactical Warning/Attack Assessment
TWAC	Tactical Weather Analysis Center
TWCS	(1) Tomahawk Weapon Control System; (2) Tactical Warfare Control System
TWG	(1) Threat Working Group; (2) Technology Working Group
TWI	Training With Industry
TWRL	Two-Way Radio Link
TWS/IPS	Topographic Workstation/Imagery Processing System
TWT	Traveling Wave Tube
TWTA	Traveling Wave Tube Amplifier
TYC	Tactical Message Central
TX	(1) Technology Exploitation; (2) Transmission

Page 3480 of 3957

U

U	Unclassified
U-2	(1) Designator for a Military Reconnaissance Aircraft; (2) AF Reconnaissance Aircraft
UA	User Agent
UAAF	Unified Action Armed Forces
UAE	United Arab Emirates
UAM	Underwater-to-Air-Missile
UAMP	USIS Architecture Migration Plan
UARR	Universal Aerial Refueling Receptical
UATP	UNIX Advanced Tracking Prototype
UAV	Unmanned Aerial Vehicle
UAV-CR	Unmanned Aerial Vehicle-Close Range
UAV-E	Unmanned Aerial Vehicle-Endurance
UAV-H	Unmanned Aerial Vehicle-HUNTER
UAVJPO	Unmanned Aerial Vehicle Joint Program Office
UAV-M	Unmanned Aerial Vehicle-Maneuver
UAV-SR	Unmanned Aerial Vehicle-Short Range
UBA	Underwater Breathing Apparatus
UBR	Unassigned Bit Rate
UC	Under Construction
UCAB	USIS Customer Advisory Board
UCC	ULTRA-Compact Camera
UCG	Universal Communications Gateway
UCIB	USAFE Command Intelligence Brief
UCIRF	USAREUR Combat Intelligence Readiness Facility
UCMJ	Uniform Code of Military Justice
UCP	Unified Command Plan
UD	Deputy USCINCSPACE
UDEAC	Economic and Customs Union of Central Africa
UDF	United Democratic Front
UDIR	USAREUR Daily Intelligence Report
UDT	Underwater Demolition Team
UE	Unit Equipment
UEAC	Union of Central African States
UEC	USAREUR Exploitation Center
UFO	(1) Unidentified Flying Object; (2) UHF Follow-On Satellites
UFR	Unfunded Requirements
UGM	Underwater Guided Missile
UGS	Unattended Ground Sensors
UHF	Ultra High Frequency
UI	(1) Unidentified; (2) Unit of Issue

Page 3481 of 3957

UIC	(1) USAREUR Interrogation Center; (2) Unit Identification Code
UIES	USAREUR Imagery Exploitation System
UIR	User Interface Requirements
UIRK	Unique Interswitch Rekeying Key
UIS	User Interface System
UJTL	Universal Joint Task List
UK	United Kingdom
UKADGE	United Kingdom Air Defense Ground Environment
UKAGE	United Kingdom Air Defense Ground Environment
UKAIR	United Kingdom Air Forces
UKLF	United Kingdom Land Forces
Ukn	Unknown
ULAN	Unit Local Area Network
ULANA	Universal Location Area Network Architecture
ULCC	Ultra Large Crude Carrier
ULCS	Unit-Level Circuit Switch
ULF	Ultra Low Frequency
ULO	USAREUR Liaison Office
ULV	Unmanned Launch Vehicle
UMD	Unit Manning Document
UMF	Unconventional Military Forces (NATO)
UMIES	USAREUR Modernized Imagery Exploitation System
UMO	Unconventional Military Operations
UMOP	Unintentional Modulation on Pulse
UN	United Nations
UNAAF	Unified Action Armed Forces
UNAMIR	United Nations Assistance Mission for Rwanda
UNAVEM	United Nations Angola Verification Mission
UNC	United Nations Command
UNCIVPOL	United Nations Civilian Police
UNCLAS	Unclassified
UNDERSEC	Under Secretary
UNDHA	United Nations Department of Humanitarian Affairs
UN-DMT	United Nations Disaster Management Team
UNDOF	United Nations Disengagement Observer Force
UNDP	United Nations Development Program
UNEF	United Nations Emergency Forces
UNESCO	United Nations Educational, Scientific & Cultural Organization
UNFICYP	United Nations Peacekeeping Force in Cyprus
UNGA	United Nations General Assembly
UNHCR	United Nations High Commissioner for Refugees
UNHQ	United Nations Headquarters
UNICEF	United Nations Childrens' Fund
UNIFIL	United Nations Interim Force in Lebanon

Page 3482 of 3957

UNIKOM	United Nations Iraq-Kuwait Observer Mission
UNITA	National Union for the Total Independence of Angola
UNITAF	Unified Task Force
UNITAS	United International Antisubmarine Warfare Exercise (Joint U.S.-Latin American Naval Exercise)
UNITREP	Unit Report
UNITSITREP	Unit Situation Report
UNIX	Orginally UNICS, for Uniplex Information and Computing System
UNMIH	United Nations Mission in Haiti
UNMO	United Nations Military Observers
UNMOGIP	United Nations Military Observer Group in India and Pakistan
UNOMIG	United Nations Mission in Georgia
UNOMIL	United Nations Observer Mission in Liberia
UNOMUR	United Nations Mission for Uganda-Rwanda
UNOSOM	United Nations Operations in Somalia
UNMSC	United Nations Military Staff Committee
UNODIR	Unless Otherwise Directed
UNPROFOR	United Nations Protection Force
UNPP	UN Peace Plan
UNSAT	Unsatisfactory
UNSC	United Nations Security Council
UNTSO	United Nations Truce Supervision Organization
UQL	Universal Query Language
UNREF	United Nations Refugee Fund
UNRWA	United Nations Relief & Works Agency
UO	Using Organization
UPI	United Press International
UPP	User Partnership Program
UPS	(1) Uninterruptible Power Supply; (2) Universal Polar Stereographic
U2R	Reconnaissance Aircraft (U.S. Air Force)
URBBO	Urban Area Boundary File
URBPOP	Urban Population File
URD	User Requirements Document
URG	Underway Replenishment Group
URS	User Readout Simulator
US	United States
U&S	Unified and Specified (Archaic, now Unified) Commands
US MLO	U.S. Military Liaison Office
US/AIA	USEUCOM/ACE Interface Architecture
USA	(1) U.S. Army; (2) United States of America
USAABMDA	United States Army Advanced Ballistic Missile Defense Agency
USAADASCH	U.S. Army Air Defense Artillery School
USACAPOC	U.S. Army Civil Affairs and Psychological Operations Command

Page 3483 of 3957

USACC	U.S. Army Communications Command
USACE	U.S. Army Corps of Engineers
USACID	U.S. Army Criminal Investigative Division Command
USACSLA	United States Army Communications Security Logistics Agency
USACOM	U.S. Atlantic Command
USAEIS	United States Army Electronic Intelligence & Security
USAF	U.S. Air Force
USAFE	U.S. Air Forces, Europe
USAFE/CC	Commander, U.S. Air Forces Europe
USAFINTEL	United States Air Force Intelligence
USAFISA	U.S. Army Force Integration Support Agency
USAFJ	U.S. Air Forces, Japan
USAFK	U.S. Air Forces, Korea
USAFLANT	U.S. Air Force, Atlantic
USAFR	U.S. Air Force Reserve
USAFRED	U.S. Air Force Readiness Command
USAFSO	U.S. Air Force Southern Command
USAFSOC	U.S. Air Force Special Operations Command
USAFSOS	U.S. Air Force Special Operations School
USAFSS	United States Air Force Security Service
USAFTAC	(1) U.S. Air Force Technical Applications Center; (2) U.S. Air Force Tactical Air Command
USAFWTC	U.S. Air Force Weapons and Tactics Center
USAIA	U.S. Army Intelligence Agency
USAICE	U.S. Army Intelligence Center, Europe
USAIC	U.S. Army Intelligence Center
USAICS	U.S. Army Intelligence Center and School
USAID	U.S. Agency for International Development
USAIIA	United States Army Imagery Interpretation Agency
USAINSCOM	U.S. Army Intelligence and Security Command
USAISC	U.S. Army Information Systems Command
USAISD	U.S. Intelligence School, Fort Devens
USAITAC	U.S. Army Intelligence Threat Analysis Center
USAITFG	United States Army Intelligence Threats & Forecasts Group
USAJFKWCS	U.S. Army John F. Kennedy Special Warfare Center and School
USAKA	U.S. Army Kwajalein Atoll
USAOG	U.S. Army Operational Group
USAR	U.S. Army Reserve
USARAK	U.S. Army Alaska
USARC	U.S. Army Reserve Command
USARCENT	U.S. Army Forces, Central Command
USARCO	U.S. Army Commercial Communications Office
USAREUR	U.S. Army, Europe
USARJ	U.S. Army, Japan
USARLANT	U.S. Army, Atlantic

Page 3484 of 3957

USARPAC	U.S. Army, Pacific
USARSO	(1) U.S. Army, South; (2) U.S. Army Forces, South
USARSOC	U.S. Army Reserve, Special Operations Command
USARSPACE	U.S. Army Space Command
USARSPACECOM	U.S. Army Space Command
USASAALA	US Army Security Assistance Agency Latin America
USASACDA	United States Army Security Agency Combat Development Activity
USASACDSA	United States Army Security Agency Command Data Systems Activity
USASAE	United States Army Security Agency, Europe
USASAPAC	United States Army Security Agency, Pacific
USASASA	United States Army Security Agency Systems Activity
USASASSA	United States Army Security Agency Signal Security Activity
USASATCOMA	United States Army Satellite Communications Agency
USASATEC	United States Army Security Agency Test & Evaluation Center
USASEXC	United States Army Services Exploitation Center
USASFC	U.S. Army Special Forces Command
USASOA	U.S. Army School of the Americas
USASOC	U.S. Army, Special Operations Command
USASOF	U.S. Army, Special Operations Forces
USASOSC	U.S. Army Special Operations Support Command
USASSDC	U.S. Army Space and Strategic Defense Command
USASSG	U.S. Army Special Security Group
USATAC	U.S. Army Terrain Analysis Center
USATACOM	U.S. Army Tank Command
USATC	United States Air Target Chart
USATEC	U.S. Army Topographic Engineering Center
USATSC	U.S. Army Training Support Center
USB	Upper Sideband
USC	(1) Under Secretaries Committee; (2) United States Code
USCENTAF	U.S. Air Forces Central Command
USCENTCOM	U.S. Central Command
USCG	U.S. Coast Guard
USCG INT	U.S. Coast Guard Intelligence
USCGNET	U.S. Communications Grid Network
USCINCACOM	Commander in Chief, U.S. Atlantic Command
USCINCARRED	Commander in Chief, United States Army Forces, Readiness Command
USCINCCENT	Commander in Chief, U.S. Central Command
USCINCEUR	Commander in Chief, U.S. European Command
USCINCFOR	United States Commander in Chief, US Forces Command
USCINCLANT	Commander in Chief, U.S. Atlantic Command
USCINCMEAFSA	United States Commander in Chief Middle East, Southern Asia, & Africa South of the Sahara
USCINCPAC	Commander in Chief, U.S. Pacific Command

Page 3485 of 3957

USCINCPACFLT	Commander in Chief, U.S. Pacific Fleet
USCINCRED	United States Commander in Chief, US Readiness Command
USCINCSO	Commander in Chief, U.S. Southern Command
USCINCSOC	Commander in Chief, U.S. Special Operations Command
USCINCSOINT	Commander in Chief, U.S. Special Operations Intelligence
USCINCSPACE	Commander in Chief, U.S. Space Command
USCINSTRAT	Commander in Chief, Strategic Command
USCINCTRANS	Commander in Chief, U.S. Transportation Command
USCMA	United States Court of Military Appeals
USCOB	United States Command Berlin
USCOMEASTLANT	U.S. Commander, Eastern Atlantic
USCS	(1) U.S. Customs Service; (2) Unified Soils Classification System; (3) U.S. Cryptologic System
USD	Under Secretary of Defense
USD(A&T)	Under Secretary of Defense (Acquisition & Technology)
USD(P)	Under Secretary of Defense for Policy
USDA	U.S. Department of Agriculture
USDAO	U.S. Defense Attache Office
USDE	Undesired Signal Data Emanations
USDR	United States Defense Representative
USELEMNORAD	U.S. Element NORAD
USEMB	United States Embassy
USEUCOM	U.S. European Command
USFJ	U.S. Forces, Japan
USFK	U.S. Forces, Korea
USFORAZ	U.S. Forces, Azores
USFORCARIB	U.S. Forces, Caribbean
USFORDOMREP	U.S. Forces, Dominican Republic
USFORSCOM	U.S. Forces Command
USFORSOM	U.S. Forces, Somalia
USG	United States Government
USGS	U.S. Geological Survey
USI	U.S. Intelligence
USIA	U.S. Information Agency
USIS	(1) U.S. Information Service (USIA abroad); (2) U.S. Imagery System
USIC	U.S. Intelligence Community
USILO	U.S. Imagery Liaison Officer
USIS	(1) U.S. Information Service; (2) U.S. Imagery System
USJTF	United States Joint Task Force
USLANTCOM	U.S. Atlantic Command
USLO	United States Liaison Officer
USM	Underwater-to-Surface Missile
USMAAG	U.S. Military Assistance Advisory Group
USMARCENT	U.S. Marine Forces Central Command

Page 3486 of 3957

USMARDEZLANT	U.S. Maritime Defense Zone, Atlantic
USMARFORK	U.S. Marine Forces, Korea
USMARFORLANT	U.S. Marine Forces, Atlantic
USMC	U.S. Marine Corps
USMILGP	U.S. Military Group
USMLM	U.S. Military Liaison Mission
USMOG-W	U.S. Military Observer Group-Washington
USMS	U.S. Marshal Service
USMTF	(1) U.S. Message Text Formats; (2) U.S. Message Text Formatter
USMTM	U.S. Military Training Mission
USN	U.S. Navy
USNAVAK	U.S. Navy Alaska
USNAVCENT	U.S. Naval Forces, Central Command
USNAVEUR	U.S. Naval Forces, Europe
USNAVFORJAPAN	U.S. Naval Forces, Japan (also USNAVFORJ)
USNAVFORKOREA	U.S. Naval Forces, Korea (also USNAVFORK)
USNAVSO	U.S. Naval Forces, Southern Command
USNI	U.S. Naval Institute
USNR	U.S. Naval Reserve
USNS	U.S. Naval Ship
USO	(1) United Service Organization; (2) Unit Security Officer
USODC	U.S. Office of Defense Cooperation
USOMC	U.S. Office of Military Cooperation
USOUTHAF	United States Southern Command Air Forces
USOS	USAF Special Operations School
USP&FO	U.S. Property and Fiscal Officer
USPACOM	U.S. Pacific Command
USR	Unit Status Report
USREDCOM	U.S. Readiness Command
USREPMILCOMUN	United States Representative, UN Military Staff Committee
USRNMC	United States Representative To NATO Military Committee
USS	(1) User Support System; (2) U.S. Ship
USSID	U.S. Signals Intelligence Directive
USSIS	U.S. Signals Intelligence System
USSOCOM	U.S. Special Operations Command
USSOCPAC	U.S. Special Operations Command Pacific
USSOUTHAF	U.S. Southern Command Air Forces
USSOUTHCOM	U.S. Southern Command
USSPACECOM	U.S. Space Command
USSR	(1) Union of Soviet Socialist Republics (now FSU); (2) Union of Soviet Sovereign Republics
USSS	(1) U.S. SIGINT System; (2) U.S. Secret Service
USSTRATCOM	U.S. Strategic Command
USTRANSCOM	U.S. Transportation Command
USTS	UHF Satellite Terminal System

Page 3487 of 3957

USW	Undersea Warfare
USYG	Under-Secretary General
UT	Users' Terminal
UTAIN	USAFE Tactical Air Intelligence Network
UTAIS	USAFE Tactical Air Intelligence System
UTC	(1) Unit Type Code; (2) Universal Coordinated Time
UTCB	USCENTCOM Transportable Communications Backbone
UTH	USAREUR Transportable Host
UTIC	USAREUR Tactical Intelligence Center
UTM	Universal Transverse Mercator (Grid)
UTTAS	Utility Tactical Transport Aircraft System
UV	Ultra Violet
UW	(1) Unconventional Warfare; (2) Underwater
UWB	Ultra Wide Band
UWOA	Unconventional Warfare Operational Area

Page 3488 of 3957

V

V-22 OSPREY	Joint Advanced Vertical-Lift Aircraft (Formerly JVX)
VA	Veterans Administration
VAAP	Vulnerability Analysis and Assistance Program
VAB	French Front Armored Vehicle
VAC	Volts, Alternating Current
VAN	Value-Added Networks
VAR	Variable
VAX	Virtual Address Extension
VBR	Variable Bit Rate
VCA	Virginia Contracting Activity
VCINCNORAD	Vice Commander in Chief, NORAD
VCJCS	Vice Chairman, Joint Chiefs of Staff
VCR	Video Cassette Recorder
VCS	(1) Video Conference Server; (2) VLAN Common Server; (3) Voice Communications Services
VCSA	Vice Chief of Staff, Army
VDL	Video Down Link
VDP	Video Disk Player
VDS	Variable Depth Sonar
VDT	Video Display Terminal
VDU	(1) Video Display Unit (TV Monitor); (2) Video Docking Unit
VDV	Soviet (FSU) Airborne Forces
veh	Vehicle
VERT	Vertical
VF	Voice Frequency
VFR	Visual Flight Rules
VGA	Virtual Graphics Array
VGK	Supreme High Command (FSU)
VGW	Variable-Geometry Wing
VHF	Very High Frequency
VHS	Video Home System
VHSIC	Very High Speed Integrated Circuit
vic	Vicinity
VICE	Voice Interceptor Comprehensive Evaluation
VID	Visual Identification (Canadian)
VIDINT	Video Intelligence
VIDS	Visually Integrated Display System
VIN	Vehicle Identification Number
VIP	(1) Very Important Person; (2) Variable Incentive Payment; (3) Visual Input Processor
VISINT	Visual Intelligence
VISTA	Very Intelligent Surveillance & Target Acquisition

Page 3489 of 3957

VIXS	Video Information Exchange System
VLAN	Very Local Area Network
VLAR	Vertical Launch and Recovery
VLCC	Very Large Crude Carrier
VLDS	Very Large Data Storage
VLF	Very Low Frequency
VLS	Vertical Launch System
VLSI	Very Large-Scale Integration
VM	Virtual Memory
VMAP	Vector Product Format
VMAQ	Marine Tactical Electronic Warfare Squadron
VMFP	Marine Tactical Reconnaissance Squadron
VMO	(1) Marine Observation Squadron; (2) Tactical Operations Squadron
V Model	Advanced Development Model
VMS	Virtual Memory System
VN	Vulnerability Number
VO	Validation Office
V/O	Vertical/Oblique
VOA	Voice of America
VOCOM	Voice Communications
VOD	Vertical On-Board Delivery
VOL	Volume
VOR	Very High Frequency Omnidirectional Range
VORTAC	Collocated VOR and TACAN
VP	(1) Patrol Aircraft (Navy); (2) U.S. Naval Patrol Squadron; (3) Maritime Patrol Squadron
VPCN	Virtual Personal Communications Networking
VPF	Vector Product Format
VPH	Video Phase History
VPK	Military Industrial Commission (FSU)
VPN	Voice Product Net
VQ	U.S. Naval Fleet Air Reconnaissance Squadron
VR	Virtual Reality
VRD	Virtual Retinal Display
VRBM	Variable-Range Ballistic Missile
VRHS	VIDMAR Robotic Hoist System
VRIT	Volume Reduced Imagery Transmission
VSAT	(1) Very Small Aperture Satellite Terminal; (2) Very Small Aperture Terminals
VSO	Vault Security Officer
VSS	VIDMAR STAK System
V/STOL	Vertical/Short Takeoff & Landing
VSWING	Anti-Submarine Wing
VT	(1) Variable Time (Fuse); (2) Video Terminal

Page 3490 of 3957

VTA	Military Transport Aviation (FSU)
VTB	Video Telebroadcasting
VTC	(1) Video Teleconferencing; (2) Video Telegraph
VTOL	Vertical Takeoff and Landing
VTR	Tracked Recovery Vehicle
VTS	Vandenberg Tracking Station
VTT	Video Teletraining
VULREP	Vulnerability Report
VVS	FSU Air Forces

Page 3491 of 3957

W

W	(1) A W prefix to any ship type designates it as subordinated to a quasi-military force; (2) Watt
WABNRES	WWMCCS Airborne Resources
WAC	(1) World Aeronautical Chart; (2) World Area Code
WADS	West Air Defense Sector
WAG	World Area Grid
W-CIOC	Wartime Combined Intelligence Operations Center
WAM	WWMCCS ADP Modernization
WAN	Wide-Area Network
WARC	World Administrative Radio Conference
WARLOG	Wartime Logistics
WARM	Wartime Reserve Mode
WAS	Wide-Area Search
WASAS	Weekly All-Source Algerian Situation Report
WASHFAX	Washington Area Secure Facsimile System
WASP	War Air Service Program
WARSIM	War Simulation
WASS	Wide-Area Surveillance System
WASSO	WWMCCS ADP System Security Officer
WATCHCON	Watch Condition
WATS	Wide Area Telecommunications System
WAWS	Washington Area Wideband System
WB	Wideband
WBIS	Wideband Intercept System
WBMS	Wideband Measurement System
WBST	Wideband Subscriber Terminals
WC	(1) Weather Center; (2) Weapon Control
WCCS	Wing Command and Control System
WCG	Workstation Computer Graphics
WDCS	Weapons Data Correlation System
WE	Weather Element
WEBE	Western European Basic Encyclopedia
WECON	Weather Control
WEFAX	Weather Facsimile
WES	WWMCCS Entry System
WESS	Weather Environmental Support System
WESTLANT	Western Atlantic Area (NATO)
WESTPAC/WPAC	Western Pacific
WESTLCF	WES Teleconferencing System
WETM	Cadre Weather Team
WEU	West European Union
WFC	World Food Council

Page 3492 of 3957

WFOV	Wide Field of View
WFP	World Food Program
WG	(1) Wing; (2) Working Group
WGS	World Geodetic System
WH	White House
WHCA	White House Communications Agency
WHD	Western Hemisphere Defense
WHO	World Health Organization
WHQ	War Headquarters
WHSR	White House Situation Room
WIA	Wounded in Action
WIC	Worldwide Intelligence Conference
WICP	Wing Initial Communications Package
WICS	Worldwide Intelligence Communications System
WIDARSURV	Wide-Area Surveillance
WIFC	Wallops Island Flight Center
WIG	Wing-in-Ground Effect
WIMS	Warning and Indications Monitoring System
WIN	(1) WWMCCS Intercomputer Network; (2) WWMCCS Interconnected Network
WINCO	Warning Intelligence Non-Commissioned Officer
WINCS	WWMCCS Information Network Communications System
WINE	Warning and Indications in Europe
WINK	Warning in Korea
WINTEX	Winter Exercise
WIP	Weekly Intelligence Production Listing
WIR	Weekly Intelligence Review
WIS	(1) Weekly Intelligence Summary; (2) WWMCCS Information System; (3) Weaponeering Information Sheet
WISE	Warning Indicators System Europe
WISP	(1) Warning Improvement Study Plan; (2) Wartime Information Security Program; (3) Worldwide Intelligence Support Program
WISS	WESTCOM Intelligence Support System
WMD	(1) Western Military District; (2) Weapons of Mass Destruction
WMTR	Western Missile Test Range
WN	Warning-Intelligence Sources and Methods Involved
WNA	Would Not Answer
WN/WNINTEL	Warning Notice-Intelligence Sources and Methods Involved
WNY	Washington Navy Yard
WO	(1) Washington Office; (2) Warrant Officer
W/OAP	With Offset Aim Point
WOC	Wing Operations Center
WORM	Write Once/Read Many
WP	(1) Warsaw Pact; (2) Word Processing
WPAC	West PAC

Page 3493 of 3957

WPC	(1) Warsaw Pact Countries; (2) Word Processing Center; (3) World Peace Council
WPM	Words Per Minute
Wpn	Weapon
WPNS	Weapons
WPNVG	Waterproof Night Vision Goggles
WPRS	War Powers Reporting System
WR	(1) Weapon Radius; (2) Western Range
WRA	Weapon Release Authority
WRM	War Reserve Materiel
WRMS	War Reserve Materiel Stocks
WRNC	Washington National Records Center
WRS	(1) Weapons Recommendation Sheet; (2) War Reserve Stocks
WRSA	War Reserve Stocks for Allies
WRSK	War Readiness Spares Kits
WS	(1) Workstation; (2) Weather Squadron; (3) Weapons School
WSAP	Weapons System Acquisition Program
WSEP	Weapon System Evaluation Program
WSI	Weapons School of Intelligence
WSI/L	War Supporting Industries and Logistics
WSMC	Western Space and Missile Center
WSMR	White Sands Missile Range
WSS	Workfile Support System
WSSIC	Weapon and Space Systems Intelligence Committee
WTM	World Target Mosaic
WTO	Warsaw Treaty Organization
WVRD	World Vision Relief and Development, Inc.
WWABNCP	Worldwide Airborne Command Post
WWCT	Worldwide Color TV
WWDMS	WWMCCS Data Base Management System
WWHFIBSN	Worldwide High Frequency Interlocking Base Station Network
WWIMS	Worldwide Warning Indicator Monitoring System
WWMCCS	Worldwide Military Command and Control System(s)
WWSVCS	Worldwide Secure Voice Conferencing System
WWW	Worldwide Web
WX	Weather
WXFCST	Weather Forecast

Page 3494 of 3957

X

XDM/X Model	Experimental Development Model/Exploratory Development Model
Xfer	Transfer
XIDB	Extended Integrated Database
XMIT	Transmit
XMTR	Transmitter
XO	Executive Officer
XOI	USAFE Director of Intelligence
XOIN	USAFE Combat Operations Division
XOIX	USAFE Plans & Systems Division
XP	Director(ate) of Plans
XRL	X-Ray Laser
XTR	Transmitter
XVIII ABC	XVIII Airborne Corps

Page 3495 of 3957

Y

YAG	Yttrium Aluminum Garnet
YAGE	Experimental Service Craft
YAM	Missile Support Craft
YAMM	Missile Support Barge
YC	Open Barge
YCF	Car Barge
YCK	Lighter Open Cargo
YCV	Lighter Aircraft Transport
YD	Floating Crane
YDG	Deperming/Degaussing Barge
YDT	Diving Tender
YE	Ammunition Lighter
YEN	Ammunition Barge
YF	Covered Lighter
YFB	Ferry
YFDB	Large Floating Drydock
YFDL	Small Floating Drydock
YFDM	Medium Floating Drydock
YFL	Launch
YFN	Covered Barge
YFNB	Large Covered Barge
YFND	Drydock Companion Barge
YFP	Floating Power Barge
YFR	Refrigerated Lighter
YFRN	Refrigerated Barge
YFU	Harbor Utility Transport
YG	Garbage Lighter
YGN	Garbage Barge
YGS	Survey Craft
YGT	Target Service Craft
YGTN	Target Barge
YH	Ambulance Craft
YM	Dredge
YMN	Non-Self-Propelled Dredge
YNC	Net Cargo Craft
YNG	Gate Craft
YO	Fuel Lighter
YON	Fuel Barge
YOS	Oil Storage Barge
YOSR	Nuclear Waste Disposal Barge
YOSS	Submersible Oil Storage Barge
YPD	Floating Pile Driver
YPL	Barracks Barge

Page 3496 of 3957

YPT	Torpedo Retriever
YR	Floating Workshop Barge
yr	Year
YRC	Cable Tender
YRD	Auxiliary Repair Dock
YRG	Tank Cleaning Craft
YRRN	Radiological Repair Barge
YRS	Salvage Craft
YSR	Sludge Removal Craft
YSS	Service Submersible
YTB	Large Harbor Tug
YTL	Small Harbor Tug
YTM	Medium Harbor Tug
YTR	Fireboat
YTS	Sail Training Craft
YVS	Seaplane Service Craft
YW	Water Lighter
YWN	Water Barge
YXR	Hulk or Relic
YXT	Training Craft

Page 3497 of 3957

Z

Z	Zulu Time (Greenwich Mean Time)
ZBB	Zero-Based Budget
ZF	Zone of Fire
ZG	Zero Gravity
ZI	Zone of the Interior
ZICON	(1) Zone of the Interior Consumers' Network; (2) Zone of Interior Communication Network
ZOS	Zone of Separation
ZPU	Soviet (FSU) Antiaircraft Machinegun
ZSU	Soviet (FSU) Self-Propelled Antiaircraft Gun
ZU	Soviet (FSU) Towed Antiaircraft Gun
ZULU	Greenwich Mean Time

Page 3498 of 3957

CODES FOR GEOPOLITICAL AREAS

Abkhazia	AB
Adriatic Sea	8D
Aegean Sea	8G
Afghanistan	AF
Albania	AL
Algeria	AG
American Samoa	AQ
Andaman Islands	ZQ
Andorra	AN
Angola	AO
Anguilla	AV
Annobon (Pagulu)	YR
Antarctica	AY
Antigua and Barbuda	AC
Arabian Peninsula	A4
Arabian Sea	6R
Arctic Ocean	5A
Argentina	AR
Armenia	AM
Aruba	AA
Ashmore and Cartier Islands	AT
Asia	A
Atlantic Ocean	Z8
Atlantic Ocean, North	1A
Atlantic Ocean, South	2A
Australia	AS
Austria	AU
Azerbaijan	AJ
Azores Islands	AZ
Bahamas	BF
Bahrain	BA
Baker Island	FQ
Balearic Islands	BI
Baltic Sea	7B
Bangladesh	BG
Barbados	BB
Barents Sea	5B

Page 3499 of 3957

Bassas Da India	BS
Belarus	BO
Belgium	BE
Belize	BH
Benin	BN
Bering Sea	5D
Bering Strait	5R
Bermuda	BD
Bhutan	BT
Black Sea	8B
Bolivia	BL
Bosnia and Herzegovina	BK
Botswana	BC
Bouvet Island	BV
Brazil	BR
British Indian Ocean Territory	I0
British Virgin Islands	VI
Brunei	BX
Bulgaria	BU
Burkina Faso (formerly Upper Volta)	UV
Burma	BM
Burundi	BY
Belarus	BO
Cabinda	VK
Cambodia (now Kampuchea)	CB
Cameroon	CM
Canada	CA
Canary Islands	ZZ
Cape Verde	CV
Caribbean Islands	N5
Caribbean Sea	1X
Caroline Islands	ZL
Caspian Sea	8C
Cayman Islands	CJ
Central African Republic	CT
Central America	N4
Chad	CD
Chile	CI
China (Peoples Republic of)	CH
Christmas Island	KT
Chukchi Sea	5C

Page 3500 of 3957

Clipperton Island	IP
Cocos (Keeling Islands)	CK
Colombia	CO
Comoros	CN
Congo	CF
Cook Islands	CW
Coral Sea Islands	CR
Corsica	VP
Costa Rica	CS
Crete	VJ
Croatia	HR
Cuba	CU
Cyprus	CY
Czechoslovakia (former)	CZ
Czech Republic	EZ
Denmark	DA
Diego Garcia	YL
Djibouti	DJ
Dominica	DO
Dominican Republic	DR
Easter Island	XZ
Eastern Europe	E5
Ecuador	EC
Egypt	EG
El Salvador	ES
Elobey, Islas de	YU
Equatorial Guinea	EK
Eritrea	ER
Estonia	EN
Ethiopia	ET
Europa Island	EU
Falkland Islands	FK
Faroe Islands	FO
Fiji	FJ
Finland	Fl
France	FR
French Guiana	FG
French Polynesia	FP
French Southern and Antarctic Lands	FS
Gabon	GB
Gambia	GA

Page 3501 of 3957

Gaza Strip	GZ
Georgia	GG
Germany	GM
Germany, Democratic Republic of (former)	GC
Germany, Federal Republic of	GE
Ghana	GH
Gibraltar	GI
Glorioso Islands	GO
Greece	GR
Greenland	GL
Grenada	GJ
Guadeloupe	GP
Guam	GQ
Guatemala	GT
Guernsey	GK
Guinea	GV
Guinea-Bissau	PU
Gulf of Mexico	1M
Guyana	GY
Haiti	HA
Heard Island and McDonald Islands	HM
Holy See	VT
Honduras	HO
Hong Kong	HK
Howland Island	HQ
Hungary	HU
Iceland	IC
India	IN
Indian Ocean	6A
Indian Ocean Islands	V2
Indonesia	ID
Iran	IR
Iraq	IZ
Iraq/Saudi Arabia Neutral Zone	IY
Ireland	El
Israel	IS
Italy	IT
Ivory Coast	IV
Jamaica	JM
Jan Mayen	JN
Japan	JA

Page 3502 of 3957

Japan, Sea of	3J
Jarvis Island	DQ
Jersey	JE
Johnston Atoll	JQ
Jordan	JO
Juan De Nova Island	JU
Juan Fernandez Archipelago	YV
Kampuchea (formerly Cambodia)	CB
Kazakhstan	KZ
Kenya	KE
Kingman Reef	KQ
Kiribati	KR
Korea, Democratic Peoples Republic of (North Korea)	KN
Korea, Republic of (South Korea)	KS
Kuwait	KU
Kyrgyzstan	KG
Lakshadweep Islands (Laccadive Islands)	LD
Laos	LA
Latin America	L7
Latvia	LG
Lebanon	LE
Lesotho	LT
Liberia	LI
Libya	LY
Liechtenstein	LS
Lithuania	LH
Luxembourg	LU
Macau	MC
Macedonia	MK
Madagascar	MA
Madeira Islands	VD
Malawi	MI
Malaysia	MY
Maldives	MV
Mali	ML
Malta	MT
Man, Isle of	IM
Marshall Islands	VH
Marshall Islands, Republic of	RM
Martinique	MB
Mauritania	MR

Page 3503 of 3957

Mauritius	MP
Mayotte	MF
Mediterranean, Eastern	8E
Mediterranean, Western	8W
Mediterranean Sea	Z9
Mexico	MX
Micronesia, Federated States of	FM
Middle East	F8
Midway Islands	MQ
Moldova	MD
Monaco	MN
Mongolia	MG
Montenegro	MW
Montserrat	MH
Morocco	MO
Mozambique	MZ
Namibia	WA
NATO Countries	N2
Nauru	NR
Navassa Island	BQ
Nepal	NP
Netherlands	NL
Netherlands Antilles	NT
New Caledonia	NC
New Hebrides (now Vanuatu)	NH
New Zealand	NZ
Nicaragua	NU
Nicobar Island	YZ
Niger	NG
Nigeria	NI
Niue	NE
Norfolk Island	NF
North Africa	F1
North Africa and Middle East	F9
Northern Island	WN
Northern Mariana Islands	CQ
Norway	NO
Norwegian Sea	5N
Okhotsk, Sea of	3Q
Okinawa	XG
Oman	MU

Page 3504 of 3957

Pacific Islands (Palau), Trust Territory of the	PS
Pacific Ocean	Z7
Pacific Ocean Islands	V1
Pacific Ocean, North	3A
Pacific Ocean, South	4A
Pakistan	PK
Palmyra Atoll	LQ
Panama	PM
Papua New Guinea	PP
Paracel Islands	PF
Paraguay	PA
Pemba Island	PB
Persian Gulf	6P
Peru	PE
Philippines	RP
Pitcairn Islands	PC
Poland	PL
Portugal	PO
Puerto Rico	RQ
Qatar	QA
Red Sea	6E
Reunion	RE
Romania	RO
Russia	RS
Rwanda	RW
Sala y Gomez Island	WC
San Ambrosio, Isla	YX
San Felix, Isla	YK
San Marino	SM
Sao Tome and Principe	TP
Sardinia (Sardegna)	SD
Saudi Arabia	SA
Senegal	SG
Serbia	SR
Seychelles	SE
Sierra Leone	SL
Singapore	SN
Slovak Republic	LO
Slovenia	SI
Socotra	SJ
Solomon Islands	BP

Somalia	SO
South Africa	SF
South America	S
South Asia	A5
South China Sea	3U
Southeast Asia	A6
South Orkney Islands	WG
South Shetland Islands	WH
Southwest Asia	A7
Spain	SP
Spratly Islands	PG
Sri Lanka	CE
St. Christopher (Kitts) and Nevis	SC
St. Helena	SH
St. Lucia	ST
St. Pierre and Miquelon	SB
St. Vincent and the Grenadines	VC
Sub-Saharan Africa	F7
Sudan	SU
Suriname	NS
Svalbard	SV
Swaziland	WZ
Sweden	SW
Switzerland	SZ
Syria	SY
Taiwan	TW
Tajikistan	TI
Tanzania	TZ
Thailand	TH
Togo	TO
Tokelau	TL
Tonga	TN
Trinidad and Tobago	TD
Tromelin Island	TE
Tunisia	TS
Turkey	TU
Turkmenistan	TX
Turks and Caicos Islands	TK
Tuvalu	TV
Uganda	UG
Ukraine	UP

Page 3506 of 3957

Union of Soviet Socialist Republics	UR
United Arab Emirates	TC
United Kingdom	UK
United Nations	UN
United States	US
United States (Miscellaneous Pacific Islands)	IQ
Upper Volta (now Burkina Faso)	UV
Uruguay	UY
Uzbekistan	UZ
Vanuatu (formerly New Hebrides)	NH
Vatican City (Holy See)	VT
Venezuela	VE
Vietnam	VM
Virgin Islands	VQ
Wake Island	WQ
Wallis and Futuna	WF
Walvis Baai	YA
West Bank	WE
Western Europe	E6
Western Sahara	WI
Western Samoa	WS
Worldwide	W
Yellow Sea	3Y
Yemen	YM
Yemen Arab Republic (North Yemen, arch.)	YE
Yemen, Peoples Democratic Republic of (South Yemen, arch)	YS
Yugoslavia (former)	YO
Zaire	CG
Zambia	ZA
Zanzibar	ZY
Zimbabwe	ZI

Page 3507 of 3957

GEOPOLITICAL AREAS BY CODE

A4	Arabian Peninsula
A5	South Asia
A6	Southeast Asia
A7	Southwest Asia
1A	Atlantic Ocean, North
1M	Gulf of Mexico
1X	Caribbean Sea
2A	Atlantic Ocean, South
3A	Pacific Ocean, North
3J	Sea of Japan
3Q	Sea of Okhotsk
3U	South China Sea
3Y	Yellow Sea
4A	Pacific Ocean, South
5A	Arctic Ocean
5B	Barents Sea
5C	Chukchi Sea
5D	Bering Sea
5N	Norwegian Sea
5R	Bering Strait
6A	Indian Ocean
6E	Red Sea
6P	Persian Gulf
6R	Arabian Sea
7B	Baltic Sea
8C	Caspian Sea
8D	Adriatic Sea
8E	Mediterranean, Eastern
8W	Mediterranean, Western
8G	Aegean Sea
A	Asia
AA	Aruba
AB	Abkhazia
AC	Antigua and Barbuda
AF	Afghanistan
AG	Algeria
AL	Albania
AM	Armenia
AN	Andorra
AO	Angola

Page 3508 of 3957

AQ	American Samoa
AR	Argentina
AS	Australia
AT	Ashmore and Cartier Islands
AU	Austria
AV	Anguilla
AY	Antarctica
AZ	Azores Islands
BA	Bahrain
BB	Barbados
BC	Botswana
BD	Bermuda
BE	Belgium
BF	Bahamas
BG	Bangladesh
BH	Belize
BI	Balearic Islands
BK	Bosnia and Herzegovina
BM	Burma
BN	Benin
BO	Belarus
BP	Solomon Islands
BQ	Navassa Island
BR	Brazil
BS	Bassas Da India
BT	Bhutan
BU	Bulgaria
BV	Bouvet Island
BX	Brunei
BY	Burundi
CA	Canada
CB	Kampuchea (formerly Cambodia)
CD	Chad
CE	Sri Lanka
CF	Congo
CG	Zaire
CH	China (Peoples Republic ofl
CI	Chile
CJ	Cayman Islands
CK	Cocos (Keeling Islands)
CM	Cameroon

Page 3509 of 3957

CN	Comoros
CO	Colombia
CQ	Northern Mariana Islands
CR	Coral Sea Islands
CS	Costa Rica
CT	Central African Republic
CU	Cuba
CV	Cape Verde
CW	Cook Islands
CY	Cyprus
CZ	Czechoslovakia
DA	Denmark
DJ	Djibouti
DO	Dominica
DQ	Jarvis Island
DR	Dominican Republic
E5	Eastern Europe
E6	Western Europe
EC	Ecuador
EG	Egypt
El	Ireland
EK	Equatorial Guinea
EN	Estonia
ER	Eritrea
ES	El Salvador
ET	Ethiopia
EU	Europa Island
EZ	Czech Republic
F1	North Africa
F7	Sub-Saharan Africa
F8	Middle East
F9	North Africa and Middle East
FK	Falkland Islands
FG	French Guiana
FI	Finland
FJ	Fiji
FM	Micronesia, Federated States of
FO	Faroe Islands
FP	French Polynesia
FQ	Baker Island
FR	France

Page 3510 of 3957

FS	French Southern and Antarctic Lands
GA	Gambia
GB	Gabon
GC	Germany, Democratic Republic of (arch.)
GE	Germany, Federal Republic of
GG	Georgia
GH	Ghana
Gl	Gibraltar
GJ	Grenada
GK	Guernsey
GL	Greenland
GM	Germany
GO	Glorioso Islands
GP	Guadeloupe
GQ	Guam
GR	Greece
GT	Guatemala
GV	Guinea
GY	Guyana
GZ	Gaza Strip
HA	Haiti
HK	Hong Kong
HM	Heard Island and McDonald Islands
HO	Honduras
HQ	Howland Island
HR	Croatia
HU	Hungary
IC	Iceland
ID	Indonesia
IM	Man, Isle of
IN	India
IO	British Indian Ocean Territory
IP	Clipperton Island
IQ	United States (Miscellaneous Pacific Islands)
IR	Iran
IS	Israel
IT	Italy
IV	Ivory Coast
IY	Iraq/Saudi Arabia Neutral Zone
IZ	Iraq
JA	Japan
JE	Jersey

Page 3511 of 3957

JM	Jamaica
JN	Jan Mayen
JO	Jordan
JQ	Johnston Atoll
JU	Juan De Nova Island
KE	Kenya
KG	Kyrgyzstan
KN	Korea, Democratic Peoples Republic of (North Korea)
KQ	Kingman Reef
KR	Kiribati
KS	Korea, Republic of (South Korea)
KT	Christmas Island
KU	Kuwait
KZ	Kazakhstan
L7	Latin America
LA	Laos
LD	Lakshadweep Islands (Laccadive Islands)
LE	Lebanon
LG	Latvia
LH	Lithuania
LI	Liberia
LO	Slovak Republic
LQ	Palmyra Atoll
LS	Liechtenstein
LT	Lesotho
LU	Luxembourg
LY	Libya
MA	Madagascar
MB	Martinique
MC	Macau
MD	Moldova
MF	Mayotte
MG	Mongolia
MH	Montserrat
MI	Malawi
MK	Macedonia
ML	Mali
MN	Monaco
MO	Morocco
MP	Mauritius
MQ	Midway Islands

Page 3512 of 3957

MR	Mauritania
MT	Malta
MU	Oman
MV	Maldives
MW	Montenegro
MX	Mexico
MY	Malaysia
MZ	Mozambique
N2	NATO countries
N4	Central America
N5	Caribbean Islands
NC	New Caledonia
NE	Niue
NF	Norfolk Island
NG	Niger
NH	Vanuatu (formerly New Hebrides)
NI	Nigeria
NL	Netherlands
NO	Norway
NP	Nepal
NR	Nauru
NS	Suriname
NT	Netherlands Antilles
NU	Nicaragua
NZ	New Zealand
PA	Paraguay
PB	Pemba Island
PC	Pitcairn Islands
PE	Peru
PF	Paracel Islands
PG	Spratly Islands
PK	Pakistan
PL	Poland
PM	Panama
PO	Portugal
PP	Papua New Guinea
PS	Trust Territory of the Pacific Islands (Palau)
PU	Guinea-Bissau
QA	Qatar
RE	Reunion
RM	Marshall Islands, Republic of

Page 3513 of 3957

RO	Romania
RP	Philippines
RQ	Puerto Rico
RS	Russia
RW	Rwanda
S	South America
SA	Saudi Arabia
SB	St. Pierre and Miquelon
SC	St. Christopher (Kitts) and Nevis
SD	Sardinia (Sardegna)
SE	Seychelles
SF	South Africa
SG	Senegal
SH	St. Helena
SI	Slovenia
SJ	Socotra
SL	Sierra Leone
SM	San Marino
SN	Singapore
SO	Somalia
SP	Spain
SR	Serbia
ST	St. Lucia
SU	Sudan
SV	Svalbard
SW	Sweden
SY	Syria
SZ	Switzerland
TC	United Arab Emirates
TD	Trinidad & Tobago
TE	Tromelin Island
TH	Thailand
TI	Tajikistan
TK	Turks and Caicos Islands
TL	Tokelau
TN	Tonga
TO	Togo
TP	Sao Tome and Principe
TS	Tunisia
TU	Turkey
TV	Tuvalu

Page 3514 of 3957

TW	Taiwan
TX	Turkmenistan
TZ	Tanzania
UG	Uganda
UK	United Kingdom
UN	United Nations
UP	Ukraine
UR	Union of Soviet Socialist Republics
US	United States
UV	Burkina Faso (formerly Upper Volta)
UY	Uruguay
UZ	Uzbekistan
V1	Pacific Ocean Islands
V2	Indian Ocean Islands
VC	St. Vincent and the Grenadines
VD	Madeira Islands
VE	Venezuela
VH	Marshall Islands
VI	British Virgin Islands
VJ	Crete
VK	Cabinda
VM	Vietnam
VP	Corsica
VQ	Virgin Islands
VT	Vatican City (Holy See)
W	Worldwide
WA	Namibia
WC	Sala y Gomez Island
WE	West Bank
WF	Wallis and Futuna
WG	South Orkney Islands
WH	South Shetland Islands
WI	Western Sahara
WN	Northern Island
WQ	Wake Island
WS	Western Samoa
WZ	Swaziland
XG	Okinawa
XZ	Easter Island
YA	Walvis Baai
YE	Yemen Arab Republic (North Yemen, arch.)

Page 3515 of 3957

YK	San Felix, Isla
YL	Diego Garcia
YM	Yemen
YO	Yugoslavia
YR	Annobon (Pagulu)
YS	Yemen, Peoples Democratic Republic of (South Yemen, arch.)
YU	Eloby, Islas de
YV	Juan Fernandez Archipelago
YX	San Ambrosio, Isla
YZ	Nicobar Island
Z7	Pacific Ocean
Z8	Atlantic Ocean
Z9	Mediterranean Sea
ZA	Zambia
ZI	Zimbabwe
ZL	Caroline Islands
ZQ	Andaman Islands
ZY	Zanzibar
ZZ	Canary Islands

Page 3516 of 3957

Page 3517 of 3957

GLOSSARY (UNCLASSIFIED)

9 June 2014

TERMS & DEFINITIONS OF INTEREST FOR COUNTERINTELLIGENCE PROFESSIONALS

Wisdom begins with the definition of terms
-- Socrates

2X. The manager of the counterintelligence and human intelligence missions at various levels of DoD structure, including joint, command, service, and task force. The 2X structure includes the Counterintelligence Coordinating Authority (CICA) and the Human Intelligence Operations Center (HOC). (AR 381-20, Army CI Program, 25 May 2010) Also see *J2X*.

-- Also, the counterintelligence and human intelligence advisor to the C/J/G/S-2. Denotes the 2X positions at all echelons. The 2X staff conducts technical control and oversight for all counterintelligence and human intelligence entities with[in] their operational purview. It coordinates, de-conflicts, and synchronizes all counterintelligence and human intelligence activities at each level of command. (Army FM 2-22.2, Counterintelligence, Oct 2009)

Term also refers to the staff section that the 2X leads.

Interesting historical note: During World War II the counterintelligence element of the Office of Strategic Services (OSS) was known as "X-2" (Counter Espionage Branch). The OSS--predecessor to today's Central Intelligence Agency--was established on 13 June 1942 by order of President Roosevelt. Also "XX" was the Double-Cross System, a World War II counterespionage and deception operation controlled British military intelligence; see *The Double-Cross System*, Yale University Press (1972) by Sir John Cecil Masterman,

603 Referral. See *Section 603 Referral*.

811 Referral. See *Section 811 Referral*.

This Glossary is designed to be a reference for counterintelligence (CI) professionals within the Department of Defense (DoD); however other CI professionals may find it of use. It provides a comprehensive compilation of unclassified terms that may be encountered when dealing with the dynamic discipline of counterintelligence and related activities. Where some words may several meanings within the counterintelligence or intelligence context, a variety of definitions are included.

Definitions within this Glossary cite an original source document. The quotes selected, as well as the views and comments expressed in the shadow boxes are those of the editor and do not necessarily reflect the official policy or position of the Department of Defense, the Office of the National Counterintelligence Executive, the Intelligence Community, the Office of National Intelligence, or the United States Government.

This Glossary is periodically updated. Users are encouraged to submit proposed changes, corrections, and/or additions. Please provide a source citation for any recommended definitions.

Editor: COL Mark L. Reagan (USA Ret), mmreagan@msn.com

A ==========

A-Space (abbreviation for *Analytical Space*). A-Space transitioned to i-Space -- see "i-Space." A-Space was a virtual work environment that provided "analysts" from across the Intelligence Community a common platform for research, analysis and collaboration.

Abort. To terminate a mission for any reason other than enemy action. It may occur at any point after the beginning of the mission and prior to its completion. (previously in Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, hereafter referred to as JP 1-02)*

Abduction. [One of the four basic types of reasoning applied to intelligence analysis,] it is the process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar explanation. (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *deduction; induction; scientific method.*

> For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003) and *Critical Thinking and Intelligence Analysis* by David T. Moore, JMIC Press (2006).

Access. In counterintelligence and intelligence use: 1) A way or means of approach to identify a target; 2) Exploitable proximity to or ability to approach an individual, facility, or information that enables target to carry out the intended mission. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the ability and opportunity to obtain knowledge of classified sensitive information or to be in a place where one could expect to gain such knowledge. (Counterintelligence Community Lexicon, June 2000, hereinafter referred to as CI Community Lexicon)

-- Also, the ability or opportunity to obtain knowledge of classified or sensitive information. (IC Standard 700-1, 4 Apr 2008 and DoD Manual 5200.01-Vol 1, Information Security Program, 24 Feb 2012)

-- Also, the ability and opportunity to obtain knowledge of classified information. (DoD Manual S-5240.09-M, OFCO Procedures & Security Classification Guide, 13 Jan 2011 and DSS Glossary)

> Access generally refers to the ability of a human source/asset (either CI or HUMINT) to perform a specific operational task within the limits of acceptable risk. Types of access include direct, indirect, first-hand, second-hand, etc.

Access Agent. An individual used to acquire information on an otherwise inaccessible target. (Human Derived Information Lexicon Terms and Definitions for HUMINT, Counterintelligence, and Related Activities, April 2008, hereinafter referred to as HDI Lexicon) Also see *agent*.

-- Also, an agent whose relationship or potential relationship with a foreign intelligence personality allows him or her to serve as a channel for the introduction of another controlled agent for the purpose of recruitment of the target. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

---

* Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms* (JP 1-02), as amended; available online at: <http://www.dtic.mil/doctrine/dod_dictionary/> Note: also available online at: <https: //jdeis.js.mil>

-- Also, a person who facilitates contact with a target individual or entry into a facility. (*Spycraft: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda*, 2008; hereinafter referred to as Spycraft)

Access Agents

Another method of identifying and keeping track of suspected intelligence personnel is to recruit people close to suspects, known in the jargon as "access agents." Counterintelligence operators can seek out secretaries, janitors, chauffeurs, interpreters, neighbors, or friends and request that they pass on information about the target's predilections and behavior.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert and Counterintelligence* (1995), pp. 218-219

Access to Classified Information. The ability and opportunity to obtain knowledge of classified information. Persons have access to classified information if they are permitted to gain knowledge of the information or if they are in a place where they would be expected to gain such knowledge. Persons do not have access to classified information by being in a place where classified information is kept if security measures prevent them from gaining knowledge of the information. (JP 1-02)

Accommodation Address. An address for a person or organization that does not occupy the premises. (HDI Lexicon, April 2008)

-- Also, an address where regular posted mail, or sometimes another type of communication, is received and then held for pickup or forwarded, transmitted, or relayed to a member of a intelligence service who does not occupy the premises. Sometimes called a mail drop, live letterbox, or cutout. (AFOSI Manual 71-142, OFCO, 9 Jun 2000 and Spy Book)

-- Also, a "safe" address, not overtly associated with intelligence activity, used by an agent to communicate with the intelligence service for whom he working. (FBI -- Affidavit: USA vs. Robert Philip Hanssen, 16 Feb 2001)

-- Also, an address with no obvious connection to an intelligence agency, used for receiving mail containing sensitive material or information (Spycraft)

-- Also, a prearranged temporary address or location where an intelligence operative may receive mail clandestinely from a third party. (*Encyclopedia of the CIA*, 2003)

ACIC. See *Army Counterintelligence Center*.

Acknowledged SAP. A SAP [Special Access Program] whose existence is acknowledged but its specific details (technologies, materials, techniques, etc.) are classified as specified in the applicable security classification guide. (DoDD 5205.07, SAP Policy, 1 July 2010) Also see *unacknowledged SAP*.

-- Also, a Special Access Program that is acknowledged to exist and whose purpose is identified (e.g., the B-2 or the F-117 aircraft program) while the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is generally unclassified. Note: Members of the four Congressional Defense Committees are authorized access to the program. (DSS Glossary)

Acoustic Intelligence (ACINT). Intelligence derived from the collection and processing of acoustic phenomena. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Acoustical Security. Those security measures designed and used to deny aural access to classified information. (DSS Glossary and AR 381-14, Technical Counterintelligence, 30 Sep 2002)

Acoustical Surveillance. Employment of electronic devices, including sound-recording, -receiving, or -transmitting equipment, for the collection of information. (JP 1-02)

Acquisition Special Access Program. A special access program established primarily to protect sensitive research, development, testing, and evaluation or procurement activities in support of sensitive military and intelligence requirements. (DSS Glossary)

Acquisition Security Database (ASDB). A classified DoD database designed to support Program Managers, Research Technology Protection (RTP), Anti-Tamper, Counterintelligence, OPSEC, and Security personnel supporting DoD Acquisition Programs with automated tools and functionality to enable efficient and cost-effective identification and protection of Critical Technologies (CT) and Critical Program Information (CPI).

-- Also, [proposed definition] the DoD horizontal protection database providing online storage, retrieval, and tracking of CPI and supporting Program Protection documents in order to facilitate comparative analysis of defense systems' technology and align CPI protection activities across the DoD. (*Draft* DoDI 5200.39, CPI Identification and Protection within RDA Programs)

> All DoD CI personnel providing CI support to RDA should obtain an ASDB account.
>
> ASDB is a key database for CI support to Research Development & Acquisition (RDA) which provides on-line storage and retrieval of Program Protection Plans (PPPs), Anti-Tamper Plans, Technology Assessment/Control Plans, Multi-Disciplined Counterintelligence Threat Assessments, Program Protection Implementation Plans, OPSEC Plans and Security Classification Guides (SCGs).
>
> On SIPRNet see <https://asdb.strikenet.navy.smil.mil>

Acquisition Systems Protection (ASP). The safeguarding of defense systems anywhere in the acquisition process as defined in DoD Directive 5000.1, the defense technologies being developed that could lead to weapon or defense systems, and defense research data. ASP integrates all security disciplines, counter-intelligence, and other defensive methods to deny foreign collection efforts and prevent unauthorized disclosure to deliver to our force uncompromised combat effectiveness over the life expectancy of the system. (DoD 5200.1-M, Acquisition Systems Protection Program, Mar 1994)

Actionable Intelligence. Intelligence information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process. (ICS Glossary and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Active Cyber Defense. The Department of Defense's real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities to defend networks and systems. (DoD Strategy for Operating in Cyberspace, May 2011)

Active Measures. In Russian, *aktivnyye mery* or *aktivnyye meropriyatiya*. …Soviet KGB tradecraft jargon for operation involving disinformation, manipulation of communist-front organizations, agent-of-influence operations, forgeries and counterfeiting. (The CIA Insider's Dictionary by Leo D. Carl, 1996)

-- Also, influence operations organized by the Soviet government. These include white, gray, and black propaganda, as well as disinformation. (Encyclopedia of Espionage, Intelligence, and Security by The Gale Group, Inc)

-- Also, the Soviet term for strategies that in the West would be described as black propaganda. The purpose was to denigrate ‘‘the main adversary’’ by using whatever disinformation channels were available to spread false stories, plant bogus reports into the media, spread untrue rumors, and support Soviet foreign policy objectives by undermining confidence in its opponents. (Historical Dictionary of Cold War Counterintelligence by Nigel West)

-- Also, a form of political warfare conducted by Soviet intelligence and security services to influence the course of world events. Active measures ranged “from media manipulations to special actions involving various degrees of violence" and included disinformation, propaganda, counterfeiting official documents, assassinations, and political repression, such as penetration in churches, and persecution of political dissidents. (Extract from Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West*, 2000)

The scale of the Soviet’s active measures campaign, and the KGB’s involvement in the development and execution of specific items of disinformation was disclosed by a KGB officer, Anatoli Golitsyn, following his defection in Helsinki in December 1961.

Active measures proved highly relevant to the Western counterintelligence community because it was in the KGB’s interests to subvert the CIA, by suggesting it was driven by corruption and influenced by dishonest politicians. The key to successful campaigns proved to be the deliberate distortion of known facts, mixed with an element of fabrication. […] In addition, there is some evidence to suggest that the KGB attempted to protect some of its most vital sources by interfering in Western mole hunts through the introduction of false or misleading clues to throw the investigations onto unproductive lines of inquiry.

-- Nigel West, *Historical Dictionary of Cold War Counterintelligence*

For more information see: *Soviet Active Measures in the "Post-Cold War" Era 1988-1991*, A Report Prepared at the Request of the United States House of Representatives Committee on Appropriations by the United States Information Agency, June 1992. Copy available on line at: <http://intellit.muskingum.edu/russia_folder/pcw_era/index.htm>

Also see *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference* by Fletcher Schoen and Christopher J. Lamb, Institute for National Strategic Studies, National Defense University, June 2012; copy available on line at: <http://www.ndu.edu/inss/news.cfm?action=view&id=160>

Activity Based Intelligence (ABI). A discipline of intelligence where the analysis and subsequent collection is focused on the activity and transactions associated with an entity, a population or an area of interest. (NGA)

ABI is a multi-intelligence approach based on persistent collection of intelligence over a broad area from multiple sources. Geospatial Intelligence (GEOINT), coupled with human domain analytics, is the foundation of ABI.

The National Geospatial-Intelligence Agency (NGA) is at the forefront of the ABI push within the Intelligence Community. The ubiquitous nature of geo-spatial intelligence (GEOINT), coupled with Human Domain Analytics (HDA), forms the true foundation of ABI.

See **“**A Brief Overview of Activity Based Intelligence and Human Domain Analytics,” (Sep 2012) by Mark Phillips available on line at: <http://trajectorymagazine.com/images/winter2012/A_Brief_Overview_of_ABI.pdf>

ABI is an inherently multi-INT approach to activity and transactional data analysis to resolve unknowns, develop object and network knowledge, and drive collection.

-- Cited by Letitia A. Long, Director NGA, in her article “Activity Based Intelligence: Understanding the Unknown,” in *The Intelligencer: Journal of U.S. Intelligence Studies*, Vol 20 No. 2, Fall/Winter 2013, p. 7

ABI is really a new tradecraft that builds on top of something that's been around for awhile called 'patterns of life.'

-- Jordan Becker, Vice President & General Manger for GEOINT-ISR, BAE Systems, Quoted in "GEOINT Tradecraft: Human Geography" by Greg Slabodkin, *DefenseSystems*, Vol 7, No. 6, Oct/Nov 2013, p. 7

Activity Security Manager. The individual specifically designated in writing and responsible for the activity's information security program, which ensures that classified information (except SCI which is the responsibility of the SSO appointed by the senior intelligence official) and CUI are properly handled during their entire life cycle. This includes ensuring information is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure that appropriate corrective action is taken. The security manager may be assigned responsibilities in other security disciplines such as personnel and physical security, etc. (DoD Manual 5200.01-Vol 1, Information Security Program, 24 Feb 2012)

Ad-Hoc Requirement (AHR). A HUMINT collection requirement with a limited emphasis, based on time or other requirements. (Defense HUMINT Enterprise Manual 3301.02, Vol II Collection Operations, 23 Nov 2010)

-- Also, an intelligence need that was not addressed in [a] standing tasking. (National HUMINT Glossary)

Adaptive Planning. The joint capability to create and revise plans rapidly and systematically, as circumstances require. Also see *Adaptive Planning and Execution (APEX); intelligence planning*.

Adaptive Planning and Execution (APEX). A Department of Defense system of joint policies, processes, procedures, and reporting structures, supported by communications and information technology, that is used by the joint planning and execution community to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities associated with joint operations. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Adequate Security. Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. (NIST, Glossary of Key Information Security Terms, May 2013)

Adherents. [In counterterrorism usage] individual who have formed collaborative relationships with, act on behalf of, or are otherwise inspired to take action in furtherance of the goals of al-Qa'ida—the organization and ideology—including b engaging in violence regardless of whether such violence is targeted at the United States, its citizens, or its interests. (National Strategy for Counterterrorism, June 2011)

Ad-hoc HUMINT Requirement (AHR). A HUMINT collection requirement with a limited emphasis, based upon time or other requirements. (DHE-M 3301.001, DIA HUMINT Manual, Vol I, 30 Jan 2009 w/ chg 2)

Adjudication. Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted or retain eligibility for access to classified information, and continue to hold positions requiring a trustworthiness decision. (DSS Glossary)

Administrative Control (ADCON). Direction or exercise of authority over subordinate or other organizations in respect to administration and support. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Admission. A polygraph examinee's acknowledgement of a fact or a capable statement associated with a relevant issue. (AR 381-20, Army CI Program, 25 May 2010)

Advanced Persistent Threat (APT). An extremely proficient, patient, determined, and capable adversary, including two or more of such adversaries working together. (DoDI 5205.13, Defense Industrial Base Cyber Security/Information Assurance Activities, 29 Jan 2010)

-- Also, an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. (NIST, Glossary of Key Information Security Terms, May 2013)

-- Also, a cyberattack campaign with specific, targeted objectives, conducted by a coordinated team of specialized experts, combining organization, intelligence complexity, and patience. (Cybersecurity and Cyberwar)

-- Also, cyber attacks mounted by organizational teams that have deep resources, advanced penetration skills, specific target profiles and are remarkably persistent in their efforts. They tend to use sophisticated custom malware that can circumvent most defenses, stealthy tactics and demonstrate good situational awareness by evaluating defenders responses and escalating their attack techniques accordingly. (<www.hackingtheuniverse.com/infosec/isnews/advanced-persistent-threat>; accessed 5 Jan 2010)

> The technological (cyber) APT has been used by actors in many nations as a means to gather intelligence on individuals, and groups of individuals of interest. See additional information at:
> -- <http://www.businessweek.com/magazine/content/08_16/b4080032220668.htm>
> -- <http://www.prometheus-group.com/blogs/36-web-security/152-anatomy-of-apt.html>
> -- <http://en.wikipedia.org/wiki/GhostNet>
>
> ---
>
> Also see Mandiant Report, *APT1: Exposing One of China's Cyber Espionage Units*, undated (circa Feb 2013); copy available at: <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>

Adverse Information. Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security. (DoD Manual 5220.22-M, National Industrial Security Program Operating Manual, 28 Feb 2006)

Adversarial Supply Chain Operation (ASCO). ASCOs are the actions taken across the entire supply chain life-cycle to attck and exploit the supply chain. ASCOs can include threatening or exploiting the supply chains. These operations are carried out through compromise, subversion, and exposure of material and components to or through the supply chain. The implications of ASCOs are possible adverse effects to mission assurance affecting material, system operations and key capabilities. (DIA) Also see *supply chain, supply chain risk, supply chain risk management*.

Adversary. An individual, group, organization, or government that must be denied essential information. (DoD Manual 5200.1-M, Acquisition Systems Protection Program, Mar 1994)

-- Also, a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

-- Also, any individual, group, organization, or government that conducts or has the intent and capability to conduct activities detrimental to the US Government or its assets. Adversaries may include intelligence services, political or terrorist groups, criminals, and private interests. (CI Community Lexicon)

-- Also, any foreign individual, group, organizations, or government that conducts or has the intent and capability to conduct activities detrimental to the national security or defense of the United States or its assets, including foreign intelligence services, political or international terrorist groups, and insurgents. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (NIST, Glossary of Key Information Security Terms, May 2013)

Adversary Collection Methodology. Any resource and method available to and used by an adversary for the collection and exploitation of sensitive/critical information or indicators thereof. (DSS Glossary)

Adversary Intelligence Systems. Resources and methods available to and used by an adversary for the collection and exploitation of critical information or indicators thereof. (DoDD 5205.02E, DoD OPSEC Program, 20 Jun 2013)

Advisory Tasking. A term used in collection management to refer to collection notices that are discretionary rather than directive in nature, with the receiving agency determining whether the requirement is relevant to the mission of the agency and whether the agency has the resources to collect against it. (AR 381-20, Army CI Program, 25 May 2010)

AFOSI. Acronym, see *Air Force Office of Special Investigations*.

Agency. In intelligence usage, an organization or individual engaged in collecting and/or processing information. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Agent. In intelligence usage, one who is authorized and trained to obtain or to assist in obtaining information for intelligence or counterintelligence purposes. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *agent of influence; agent of a foreign entity; asset; foreign intelligence agent.*

-- Also, a person who engages in clandestine intelligence activities under the direction of an intelligence organization, but is not an officer, employee, or co-opted worker of that organization. (National HUMINT Glossary)

-- Also, an individual other than an officer, employee, or co-opted worker of an intelligence service to whim specific intelligence assignments are given by an intelligence service. An agent in a target country can be operated by a legal or illegal residency or directly by the center. An agent can be of any nationality. (FBI FCI Terms)

-- Also, 1) A person who engages in clandestine intelligence activity under the direction of an intelligence organization but who is not an officer, employee, or co-opted worker of that organization; 2) An individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence or counterintelligence proposes; [and] 3) One who is authorized or instructed to obtain or assist in obtaining information for intelligence or counterintelligence purposes. (ICS Glossary)

> *Typically, the aim of an espionage operation is to recruit an **agent** [emphasis added], usually a foreign person, to carry out the actual spying. The person who targets, recruits, trains, and runs the agent is, in American parlance, the 'case officer.'*
>
> -- Arthur S. Hulnick, "Espionage: Does It Have a Future in the 21st Century?" *The Brown Journal of World Affairs;* v XI: n 1 (2004).

…[T]ypes of agents—singletons, sleepers, illegal spies actively running one or more sources, illegal residents running a group of other illegals, and so forth.

-- Peter Wright, *Spycatcher* (1987), p. 139

Espionage is one of the toughest games played. An agent in the right place is hard to find, but when he is found he should be regarded as a pearl beyond price.

-- David Nelligan, *The Spy in the Castle* (1968)

Agent-in-Place. A person who remains in a position while acting under the direction of a hostile intelligence service, so as to obtain current intelligence information. It is also called a recruitment-in-place. (FBI -- Affidavit: USA *vs*. Robert Philip Hanssen, 16 Feb 2001) Also see *recruitment-in-place (RIP).*

Agent of Influence. An agent of some stature who uses his or her position to influence public opinion or decision making to produce results beneficial to the country whose intelligence service operates the agent. (AFOSI Manual 71-142, OFCO, 9 Jun 2000) [Originally a Soviet term]

-- Also, a person who is directed by an intelligence organization to use his position to influence public opinion or decision-making in a manner that will advance the objective of the country for which that organization operates. (ICS Glossary)

-- Also, an individual who acts in the interest of an adversary without open declaration of allegiance and attempts to exercise influence covertly, but is not necessarily gathering intelligence or compromising classified material, is known as an agent of influence. (Historical Dictionary of Cold War Counterintelligence, 2007)

-- Also, an agent operating under intelligence instructions who uses his official or public position, and other means, to exert influence on policy, public opinion, the course of particular events, the activity of political organizations and state agencies in target countries. (KGB Lexicon: The Soviet Intelligence Officer's Handbook, edited by KGB archivist Vasiliy Mitrokhin, 2002).

An agent of influence is a person who uses his or her position, influence, power, and credibility to promote the objectives of an alien power…, in ways unattributable to that power, Such agents may operate openly or surreptitiously, and their effectiveness depends on their position and the extent to which they are prepared to misuse it, but any degree of deliberate support for an adversary power, especially if applied in an underhanded way, savours of treachery.

-- Chapman Pincher, *Traitors: The Anatomy of Treason*, First U.S. Edition (1999), p. 34

Agent of a Foreign Entity. A person who engages in intelligence activities under the covert direction of a foreign intelligence or security entity, but is not an officer, employee, or co-opted worker of that entity. (ONCIX Analytic Chiefs Working Group, Jan 2011) Also see *agent; agent of a foreign power; asset.*

Agent of a Foreign Power. Means: (1) any person other than a United States person, who – (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (C) engages in international terrorism or activities in preparation therefore; or (2) any person who - (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power; (D) knowingly enters the United States under a false or fraudulent identity for or on behalf

of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C). (Source: 50 USC § 1801b) Also see *foreign power*.

Agent Handler. An [intelligence] officer or principal agent who directly manages an agent or agent network. (National HUMINT Glossary) Also see *case officer*.

Agent Net. An intelligence gathering unit of agents supervised by a principal agent who is operating under the direction of an intelligence officer. An agent net can operate in either the legal or illegal field. (ICS Glossary and FBI FCI Terms)

Agent Recruitment Cycle (ARC). See *recruitment cycle*.

Air Force Office of Special Investigations (AFOSI). U.S. Air Force's major investigative service; a federal law enforcement and investigative agency operating throughout the full spectrum of conflict, seamlessly within any domain; conducting criminal investigations and providing counterintelligence services. (<www.osi.andrews.af.mil>; accessed 27 June 2012)

AFOSI Mission: Identify, exploit and neutralize criminal, terrorist and intelligence threats to the Air Force, Department of Defense and U.S. Government.

AFOSI Capabilities:
-- Protect critical technologies and information
-- Detect and mitigate threats
-- Provide global specialized services
-- Conduct major criminal investigation
-- Engage foreign adversaries and threats offensively

Source: AFOSI web site (accessed 27 June 2012)

Fact sheet at: <http://www.osi.andrews.af.mil/library/factsheets/factsheet_print.asp?fsID=4848&page=1>

All-Source Analysis. An intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include human intelligence, signals intelligence, geospatial intelligence, measurement & signature intelligence, and open source intelligence. (DoDD 5240.01, DoD Intelligence Activities, 27 Aug 2007) Also see a*nalysis; analysis and production*; *counterintelligence analysis.*

-- Also, an intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include HUMINT, SIGINT, MASINT, GEOINT, OSINT, and CI. (DoDI 5105.21, DIA, 18 Mar 2008) {note this definition includes *counterintelligence*}.

All-source analysis can transform raw intelligence, data, and information into knowledge and understanding.

Integrated all-source analysis should also inform and shape strategies to collect more intelligence…. The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots."

-- Final Report of the National Commission on Terrorist Attacks Upon the United States (2004)

All-Source Intelligence. 1) Intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence. 2) In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, intelligence information derived from several or all the intelligence disciplines, including SIGINT, HUMINT, MASINT, OSINT, and GEOINT. (ODNI, U.S. Intelligence – An Overview 2011)

-- Also, the integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations. (ADRP 2-0, Intelligence, Aug 2012)*

> * Note: supersedes the definition in Army FM 2-0, *Intelligence*, 23 Mar 2010.
>
> ADRP = Army Doctrinal Reference Publication.
> ADRPs are available online at <hhtps://armypubs.us.army.mil/doctrine/index.html>

Alliance. The relationship that results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Alias. A false identity used while carrying out authorized activities and lawful operations. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

-- Also, an alternative name, used for cover purposes. (Defense HUMINT Enterprise Manual 3301.002, Vol II, Collection Operations, 23 Nov 2010)

-- Also, a false name. (National HUMINT Glossary)

-- Also, a false name assumed by an individual for a specific and often temporary purpose, i.e., to conceal a true identity from persons or organizations with whom he or she is in contact. Also called a pseudonym or cover name. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, an assumed name, usually consisting of a first and last name, used by an individual for a specific and often temporary purpose. (FBI FCI Terms)

Alternate Meet. A prearranged meeting that takes place in the event a regularly scheduled meet is missed for any reason. (FBI FCI Terms)

Alternative Analysis. [Analysis that] involves a fairly intensive, though time limited, effort to challenge assumptions or to identify alternative outcomes, depending on the technique employed, with the results captured, implicitly or explicitly, in a written product delivered to relevant policy-makers.(CIA - Sherman Kent Center for Intelligence Analysis)

> Alternative analysis includes techniques to challenge analytic assumptions (e.g., “devil’s advocacy”), and those to expand the range.
>
> See article “Rethinking “Alternative Analysis” to Address Transnational Threats” at:
> <https://www.cia.gov/library/kent-center-occasional-papers/vol3no2.htm>

Alternative Compensatory Control Measures (ACCM). Measures designed to safeguard sensitive intelligence and operations when normal security measures are either not sufficient to achieve strict controls over access to information, but where strict SAP [Special Access Program] access controls are either not required or are too stringent. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, used to safeguard sensitive intelligence or operations and support information (acquisition programs do not qualify) when normal measures are insufficient to achieve strict need-to-know controls, and where Special Access Program controls are not required. (DSS Glossary)

> ACCMs are not Special Access Programs (SAPs). Guidance for ACCMs is contained in DoD Manual 5200.01, Vol 3, *DoD Information Security Program: Protection of Classified Information*, 24 Feb 2012,

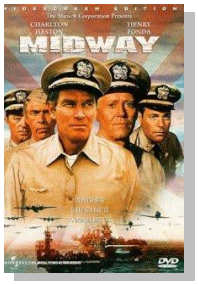
Ambassador. Diplomatic official of the highest rank who is accredited to a foreign sovereign or government, or to an international organization, as the resident representative of the sending government or appointed for a specific diplomatic assignment. (Department of State) Also see *Chief of Mission*.

A U.S. ambassador serving abroad symbolizes the sovereignty of the United States and serves as the personal representative of the President of the United States. Ambassadorial duties include negotiating agreements, reporting on political, economic and social conditions, advising on policy options, protecting American interests, and coordinating the activities of all U.S. Government agencies and personnel in the country.

Analysis. [In intelligence usage] the process by which information is transformed into intelligence; a systemic examination of information to identify significant facts, make judgments, and draw conclusions. (ODNI, U.S. Intelligence – An Overview 2011) Also see a*nalysis and production; all-source analysis; counterintelligence analysis; intelligence analysis*.

-- Also, the process by which collected information is evaluated and integrated with existing information to produce intelligence that describes the current—and attempts to predict the future—impact of the threat, terrain and weather, and civil considerations on operations. (Army FM 2-0, Intelligence, 23 Mar 2010)

-- Also, a stage in the intelligence processing cycle whereby collected information is reviewed to identify significant facts; the information is compared with and collated with other data, and conclusions, which also incorporate the memory and judgment of the intelligence analyst, are derived from it. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)



INTELLIGENCE ANALYSIS…

"Joe, you're guessing!"
Navy Capitan Matthew Garth
(Charlton Heston)

"Sir, we like to call it analysis."
Naval Intelligence Officer Joseph Rochefort
(Harold Rowe "Hal" Holbrook, Jr.)
-- The movie *Midway* (1976)

Analysis is the process by which people transform information into intelligence. It includes integrating, evaluating, and analyzing all available data -- which is often fragmented and even contradictory -- and preparing intelligence products.

Former DCI Richard Helms noted that despite all the attention focused on the operational (collection) side of intelligence, *analysis* is the core of the process to inform decision makers.

_____

It is of the highest importance in the art of detection to be able to recognize, out of a number of facts, which are incidental and which are vital.

-- Sherlock Holmes
From A. Conan Doyle's "The Reigate Squire" June 1893
(M. Hardwick, *The Complete Guide to Sherlock Holmes,* 1986, pp. 86-87)

_____

Analysis is the thinking part of the intelligence process
-- James B. Bruce and Roger Z. George

_____

It is not enough, of course, simply to collect information. Thoughtful analysis is vital to sound decisionmaking.
-- President Ronald Reagan (4 Dec 1981)

_____

…[A]nalysis must always be timely, responsive and relevant to… customer's needs.

-- LTG Michael T. Flynn, USA, Director Defense Intelligence Agency (Jul 2012)

Intelligence analysts select and filter information; they interpret the resultant evidence, put it into context, and tailor it to meet… customers' needs. In short, analysts and analysts only, create intelligence.

-- David T. Moore, "Species of Competencies for Intelligence," *American Intelligence Journal* (2005)

Analysis must do more than just describe what is happening and why; it must identify a range of opportunities… Analysis is the key to making sense of the data and finding opportunities to take action.

-- DNI 2006 Annual Report of the US Intelligence Community (Feb 2007)

The primary purpose of analytic effort is "sensemaking" and understanding, not producing reports; the objective of analysis is to provide information in a meaningful context, not individual factoids.

-- Jeffrey R, Cooper, *Curing Analytical Pathologies*, Center for the Study of Intelligence (Dec 2005), p. 42

Today, U.S. intelligence analysts spend roughly 80 percent of their time gathering intelligence but only 20 percent analyzing it.

-- LTG Bob Noonan (USA Ret) and Greg Wenzel, "Fixing the 'I' in ISR," *DefenseNews*, 24 Sep 2012, p. 45

Analysts are the voice of the Intelligence Community

-- WMD Report (31 Mar 2005), p. 388

Analysts must absorb information with the thoroughness of historians,
organize it with the skill of librarians, and disseminate it with the zeal of journalists.

--TRADOC Pam 525-2-1, *US Army Functional Concept for Intelligence 2016-2028*, 13 Oct 2010; p. 66

Intelligence analysis is inherently an intellectual activity
that requires knowledge, judgment, and a degree of intuition.

Selected references for **intelligence analysis**:

Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency), 1999.
Copy available online at: <http://www.archive.org/details/PsychologyOfIntelligenceAnalysis>
Also at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/index.html>

Richards J. Heuer, Jr. and Randolph H. Pherson, *Structured Analytical Techniques for Intelligence Analysis* (Washington, DC; CQ Press), 2010.

Richards J. Heuer, Jr, *Improving Intelligence Analysis with ACH*, 2005.
This learning aid extracts, revises, and partially updates those portions of the author's book, *Psychology of Intelligence Analysis* [cited above], that deal with Analysis of Competing Hypotheses (ACH) and with how and why the ACH software helps intelligence analysts reduce the risk of surprise. ACH software is available at: <http://www2.parc.com/istl/projects/ach/ach.html>

Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: Origins, Obstacles, and Innovation* (Washington, DC: Georgetown University Press), 2008.

Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*, rev. ed. (Washington, DC: CQ Press), 2007; also paperback 2012

David A. Schum, *Evidence and Inference for the Intelligence Analyst* (Lanham, MD: University Press of America) 1987.

Morgan Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*, rev. ed. (New York: Three Rivers Press), 1998.

Robert S. Sinclair, *Thinking and Writing: Cognitive Science and Intelligence Analysis,* revised edition (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency), 2010.
Copy available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/thinking-and-writing.html>

David T. Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington, DC: National Defense Intelligence College, 2011).
Copy available at <http://ni-u.edu/ni_press/pdf/Sensemaking.pdf>

A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis (Washington, DC: U.S. Government), 2009.
Copy available at: <https://www.cia.gov/library/ publications/publications-rss-updates/tradecraft-primer-may-4-2009.html>

A Compendium of Analytic Tradecraft Notes, Volume I, Notes 1-10, reprinted (Washington, DC: Central Intelligence Agency), 1997.
Copy available at: <http://www.au.af.mil/au/awc/awcgate/cia/tradecraft_notes/contents.htm>

The Sherman Kent Center for Intelligence Analysis Occasional Papers, (CIA).
Available online at: <https://www.cia.gov/library/kent-center-occasional-papers/index.html>

Frank Watanabe, "Fifteen Axioms for Intelligence Analysts." *Studies in Intelligence*, CIA, Semiannual Edition, No. 1, 1997, pp. 45-47.
Copy available on line at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol40no5/pdf/v40i5a06p.pdf>

Also see Mark Lowenthal, PhD, *Intelligence: From Secrets to Policy,* 5th Edition (CQ Press), 2011.

Analysis and Production. In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012) Also see *analysis; all-source analysis; counterintelligence analysis.*

-- Also, the ability to integrate, evaluate, and interpret information from available sources and develop intelligence products that enable situational awareness. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Analysis of Competing Hypothesis (ACH). Identification of alternate explanations (hypothesis) and evaluation of all evidence that will disconfirm rather that confirm hypotheses. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

ACH a highly effective technique when there is a large amount of data to absorb and evaluate. It is particular appropriate for controversial issues when analysts want to develop a clear record that shows what theories they have considered and how they arrived at their judgments.

See Richards J. Heuer, Jr, *Improving Intelligence Analysis with ACH*, Nov 2005 (Learning Aid, ACH Version 2.0). This learning aid extracts, revises, and partially updates those portions of the author's book, *Psychology of Intelligence Analysis* [cited above], that deal with Analysis of Competing Hypotheses (ACH) and with how and why the ACH software helps intelligence analysts reduce the risk of surprise.

ACH software available for download at: <http://www2.parc.com/istl/projects/ach/ach.html>

Analysis Report. A type of DoD CI analytical product prepared IAW DoDI 5240.18; it may require in-depth study and research, but generally is not as involved as an assessment. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013). Also see *Counterintelligence Analytical Product*.

Analytic Outreach. The open, overt, and deliberate act of an IC [Intelligence Community] analyst engaging with an individual outside the IC to explore ideas and alternate perspectives, gain new insights, generate new knowledge, or obtain new information. (ICD 205, Analytic Outreach, 16 Jul 2008)

Analytic Tradecraft. The practiced skill of applying learned techniques and methodologies appropriate to an issue to mitigate, gain insight, and provide persuasive understanding of the issue to members of the U.S. Government and its allies. (DIA, *A Tradecraft Primer: Basic Structured Analytic Techniques,* March 2008).

Note: The source document (First Edition) cited above is no longer available online. The current version: *Tradecraft Primer: Structured Analytic Techniques*, 3rd Edition (3 March 2010) is now Defense Intelligence Reference Document, *Analytic Methodologies*, DIA-01-1003-001A, and is controlled as UNCLASSIFIED//FOR OFFICIAL USE ONLY.

Anomalies. Foreign power activity or knowledge, inconsistent with the expected norms that suggest prior foreign knowledge of US national security information, processes or capabilities. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 30 Dec 2010) See *anomalous activity; anomaly*.

-- Also, irregular or unusual activities that may cue the analyst on the existence of FISS and ITO [international terrorist organizations] activity. (Army FM 2-22.2, Counterintelligence, Oct 2009)

CI anomalies differ from CI indicators (see *potential espionage indicators*). CI anomalies surface as a result of FIE activities, whereas CI indictors are manifested in an insider's actions, activities, and/or behaviors.

Recognizing the importance of CI anomalies in the early detection and neutralization of espionage, a White House Memorandum of August 23, 1996 called for a more systematic approach to the handling of CI anomalies. The memorandum emphasized the need for, and value of, timely participation of CI elements in detecting and reporting CI anomalies indicating threats to U.S. national security.

-- DIA tri-fold, *Counterintelligence Anomalies: What are They and Why Should We Look for Them?*, Jan 2012

Look for the anomalies…
Look for the odd bits that seem to be out of focus, or out of sequence.
Look for the inexplicable.

-- Sean Flannery, *Crossed Swords*, 1989

Anomalous Activity. Irregular or unusual deviations from what is usual, normal, or expected; activity inconsistent with the expected norm. See *anomalies; anomaly*.

-- Also, [in DoD cyber usage] network activities that are inconsistent with the expected norms that may suggest FIE [Foreign Intelligence Entity] exploitation of cyber vulnerabilities or prior knowledge of U.S. national security information, processes, or capabilities. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010 with change 1 dated 16 Oct 2013)

Anomalous Behavior Analysis

[The CI] analyst seeks out strange or puzzling behavior pointing to a counterintelligence problem even before it is known to exist. There are various kinds of anomalous behaviors that might tip off an analyst about a foreign intelligence service's successful operations. One is strategic behavior. When a foreign government starts using the same secret technology as another government, the analyst who finds this out may hypothesize that it because such secrets have been stolen.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 196

Anomaly. Activity or knowledge, outside the norm, that suggests a foreign entity has foreknowledge of U.S. information, processes, or capabilities. (DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 3013) See *anomalies, anomalous activity, anomaly-based detection.*

Anomaly-based Detection. The process of comparing CI, security, IA [Information Assurance], LE [law enforcement], and AT/FP [antiterrorism and force protection] behaviors and activities that are deemed normal against other observed events to identify significant deviations and or anomalous behavior. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 with change 1 dated 15 Oct 2013)

-- Also, the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. (NIST, Glossary of Key Information Security Terms, May 2013)

Anomaly Detection

The systems and processes used to assess deviant or unscheduled activities or presences which may indicate anomalous activities or unauthorized access. This interpretation assumes a baseline norm from which deviations are assumed to indicate some type of intrusion.

-- Julie K. Petersen, *Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications* (2001)

Anti-Tamper. Systems engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system in order to impede countermeasure development, unintended technology transfer, or alteration of a system. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008)

Note: DoDI 5200.39 under revision, proposed revised definition for AT: *Systems engineering activities intended to prevent, or delay exploitation of CPI in U.S. defense systems to impede countermeasure development, unintended technology transfer, or alteration of a system due.* (Draft circa Feb 2014)

DoD Anti-Tamper Executive Agent: chartered by the Under Secretary of Defense (Acquisition, Technology, and Logistics), and assigned to the Directorate for Special Programs, Office of the Assistant Secretary of the Air Force for Acquisition.

Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. (JP 1-02; and JP 3-07.2, Antiterrorism, 24 Nov 2010)

Also see DoDI 2000.12, *DoD Antiterrorism Program*, 1 Mar 2012 (w/ chg 1) and DoD O-2000.12-H, *DoD Antiterrorism Handbook*, 1 February 2004

Apportionment. In the general sense, distribution for planning of limited resources among competing requirements. (JP 1-02)

Apprehension. The taking of a person into custody or the military equivalent of “arrest.” Under Rule 304, Manual for Courts Martial (MCM), the restraint of a person by oral or written order directing him to remain within specified limits. (AR 381-20, Army CI Program, 25 May 2010)

Area of Responsibility (AOR). The geographical area associated with a combatant command within which a geographic combatant commander has authority to plan and conduct operations. (JP 1-02)

Army Counterintelligence Center (ACIC). The Army’s counterintelligence analysis and production center.

ACIC’s mission is to provide timely, accurate, effective multidiscipline counterintelligence analysis in support of the US Army combating terrorism program, ground systems technologies, and counterintelligence investigations, operation, and activities. The ACIC is a subordinate unit of the 902d Military Intelligence Group, US Army Intelligence and Security Command, located at Fort Meade, Maryland.

Army G-2X. The element which manages and provides technical control of the CI and HUMINT missions in the Army. (AR 380-20, Army CI Program, 25 May 2010)

Arrest. The act of detaining in legal custody. An "arrest" is the deprivation of a person's liberty by legal authority in response to a criminal charge. (www.ojp.usdoj.gov; accessed 29 Apr 2013)

ASDB. Acronym, see *Acquisition Security Database*.

Assassination. The murder or attempted murder of DoD personnel for political or retaliatory reasons by international terrorists or agents of a foreign power. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, to murder (usually a prominent person) by a sudden and/or secret attack, often for political reasons. (Wikipedia; accessed 15 Feb 2010)

"[The KGB] did everything from plotting ways to poison the capital's water systems to drawing up assassination plans for US leaders."

-- Oleg Kalugin, Former Major General in the KGB
as cited in Andrew & Mitrokhin, *The Mitrokhin Archive* (1999)

Assassination constitutes an act of murder that is prohibited by international law and Executive Order 12333. In general, assassination involves murder of a targeted individual for political purposes. Example, the 1978 "poisoned-tip umbrella" killing of Bulgarian defector Georgi Markov by Bulgarian State Security agents on the streets of London falls into the category of an act of murder carried out for political purposes, and constitutes an assassination.

"Wet Work" – a term originated within the Soviet intelligence – describes the art of assassination. In 1965, Peter Deriabin, a KGB defector, testified to a Senate committee –

> *"The [KGB] thirteenth department is responsible for assignation and terror. This Department is called the department of wet affairs, or in Russian 'Mokrie Dela'…. 'Mokrei' means 'wet' and in this case 'mokrie' means 'blood wet'."*

Unquestionably the most neglected aspect of U.S. counterintelligence. EO 12333 specifically provides that "*Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against… **assassinations** [emphasis added] conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities."

The word *assassin* is derived from the word Hashshashin (Arabic: حشّاشين, ħashshāshīyīn, also Hashishin, Hashashiyyin, or Assassins). It referred to the Nizari branch of the Ismāʿīlī Shia founded by the Persian Hassan as-Sabbah during the Middle Ages. They were active in Iran from the 8th to the 14th centuries, and also controlled the castle of Masyaf in Syria. The group killed members of the Muslim Abbasid, Seljuq, and Christian Crusader élite for political and religious reasons.

The important thing to know about any assassination or an attempted assassination is not who fired the shot, but who paid for the bullet.

-- Eric Ambler, *A Coffin for Dimitrios* (1939)

Assessment. 1) a continuous process that measures the overall effectiveness of employing joint force capabilities during military operations; 2) determination of the progress toward accomplishing a task, creating a condition, or achieving an objective; 3) analysis of the security, effectiveness, and potential of an existing or planned intelligence activity; and 4) **[in human source operations] judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents."** [emphasis added] (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

-- Also, [In CI analysis usage] a type of DoD CI analytical product prepared IAW DoDI 5240.18; it requires in-depth study and research. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013). Also see *Counterintelligence Analytical Product*.

-- Also, [in intelligence usage], appraisal of the worth of an intelligence activity, source, information, or product in terms of its contribution to a specific goal, or the credibility, reliability, pertinence, accuracy, or usefulness of information in terms of an intelligence need. (National HUMINT Glossary)

Assessment--within the human source environment…

"A process of getting to know and understand people and describing them."
-- Robert R. Holt, *Assessing Personality* (1971)

Effective assessment of human beings is an art

From an Agent Handler perspective…
"…[F]inding a likely candidate, getting to know him personally, ascertaining his interests, uncovering his vices and possible Achilles' heel."
-- Victor Cherkashin, KGB Counterintelligence Officer and author of *Spy Handler* (2005)

Asset. Any human or technical resource available to an intelligence or security service for operational purposes. (FBI FCI Terms) Also see *agent; foreign intelligence agent; Intelligence asset; source.*

-- Also, [in human source operations] a recruited source. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, any resource—human, technical, or otherwise—available to an intelligence or security service for operational use. In U.S. usage, usually a person. (Spy Book)

-- Also, [in defense critical infrastructure usage] a distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned or operated by domestic, foreign, public, or private sector organizations. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *defense critical infrastructure program*.

-- Also, [in critical infrastructure protection] person, structure, facility, information, material, or process that has value. (DHS Lexicon, 2010) Also see *crucial infrastructure*.

Asset Owner. [In DCIP usage,] the DoD Components with responsibility for a DoD asset, or organizations that own or operate a non-DoD asset. (DoDI 3020.45, DCIP Management, 21 Apr 2008) Also see *task asset, task critical asset*.

Asset Validation. In intelligence use, the process used to determine the asset authenticity, reliability, utility, suitability, and degree of control the case officer or others have. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Source Validation*.

The cardinal rule in tradecraft is: Never, ever fall in love with your agent.
-- Robert D. Chapman, Retired CIA Operations Officer
"Patriot or Traitor?" Book review of *A Secret Life* in *International Journal of Intelligence and Counterintelligence*, Vol 18 No 2 (Summer 2005), p. 367

Some human intelligence agencies do a poor job of validating human sources.

The story of 'Curveball'—the human source who lied to the Intelligence Community about Iraq's biological weapons programs—is an all-too familiar one. Every agency that collects human intelligence has been burned in the past by false reporting; indeed, the Intelligence Community has been completely fooled several times by large-scale double-agent operations run by, among others, the Cubans, East Germans, and Soviets. It is therefore critical that our human intelligence agencies have excellent practices of validating and vetting their sources.
-- WMD Report, Chapter 7 - Collection, p. 367*
* Available online at: <https://www.fas.org/irp/offdocs/wmd_chapter7.pdf>

-- Also, the process used to determine the asset authenticity, reliability, utility, suitability, and degree of control the case officer or others have. This process continues through the life of the relationship. It may be more or less formal depending on the sensitivity of the relationship and the nature of the source. For clandestine sources, particularly foreign nationals, the process is usually formal and revalidation is required on a periodic basis. Whether or not it is conducted formally, it must be a well-planned and thought out activity. (DoD CI Collection IWG Handbook, TTP for CI Collection, Collection Management, and Collection Operations, 8 Aug 2006)

In the spy trade asset validation is simply
a system of measures to establish the reliability and veracity of sources.
-- Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present*, 2013, p. 255

For any organization that collects human intelligence, having an independent system for asset validation is critical to producing reliable, well-vetted intelligence.
-- WMD Report (31 Mar 2005), p. 455

Every intelligence service has the problem of distinguishing…
between a bona fide volunteer and a penetration agent who has been sent by the other side. This is no easy matter.
-- Allen W. Dulles, *The Craft of Intelligence* (2006), p. 121

See DoDI S-3325.07, *Guidance for the Conduct of DoD Human Source Validation* (U) and National HUMINT Manager Directive 001.008, *HUMINT Source Validation*.

Assign. 1) To place units or personnel in an organization when such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function, or greater portion of the functions, of the unit or personnel; or 2) To detail individuals to specific duties or functions where such duties or functions are primary and/or relatively permanent. (JP 1-02 and JP 5-0, Joint Operations Planning, 11 Aug 2011) Also see *attach.*

Assumption. A supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action. (JP 1-02 and JP 5-0, Joint Operations Planning, 11 Aug 2011)

Asylum. Protection granted by the U.S. Government within the United States to a foreign national who, due to persecution or a well-founded fear of persecution on account of his or her race, religion, nationality, membership in a particular social group, or political opinion, is unable or unwilling to avail himself or herself of the protection of his or her country of nationality (or, if stateless, of last habitual residence). (DoDI 2000.11, Procedures for Handling Requests for Asylum and Temporary Refuge, 13 May 2010)

Asymmetric Threat. An adversary strength that can be used against a friendly vulnerability. An adversary may pursue an asymmetric advantage on the tactical or strategic level by identifying key vulnerabilities and devising asymmetric concepts and capabilities to strike or exploit them. To complicate matters, our adversaries may pursue a combination of asymmetries. (USD/I Taking Stock of Defense Intelligence Report, 22 Jan 2004)

-- Also, a broad and unpredictable spectrum of military, paramilitary, and information operations, conducted by nations, organizations, or individuals or by indigenous or surrogate forces under their control, specifically targeting weaknesses and vulnerabilities within an enemy government or armed force. (Source: Michael L. Kolodzie, US Army, circa 2001)

-- Also, a broad and unpredictable spectrum of risks, actions, and operations conducted by state and non-state actors that can potentially undermine national and global security. (Cyber Threats to National Security, Symposium Five, 2011)

Asymmetric Warfare. Combat between two or more state or non-state actors whose relative military power, strategies, tactics, resources, and goals differ significantly. (Cyber Threats to National Security, Symposium Five, 2011)

Atmospherics. Information regarding the surrounding or pervading mood, environment, or influence on a given population. (DoDD 3600.01, Information Operations, 14 Aug 2006 with Chg 1, 23 May 2011)

Attach. 1) The placement of units or personnel in an organization where such placement is relatively temporary; or 2) The detailing of individuals to specific duties or functions where such functions are secondary or relatively temporary. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *assign.*

Attaché. A diplomatic official or military officer attached to an embassy or legation, especially in a technical capacity. Also see *Senior Defense Official / Defense Attaché (SDO/DATT).*

Authenticate. A challenge given by voice or electrical means to attest to the authenticity of a message or transmission. (JP 1-02)

Authentication. 1) A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator; 2) A means of identifying individuals and verifying their eligibility to receive specific categories of information; 3) Evidence by proper signature or seal that a document is genuine and official; and 4) In personnel recovery missions, the process whereby the identity of an isolated person is confirmed. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Authenticator. A symbol or group of symbols, or a series of bits, selected or derived in a prearranged manner and usually inserted at a predetermined point within a message or transmission for the purpose of attesting to the validity of the message or transmission. (JP 1-02)

B ==========

Background Investigation (BI). An official inquiry into the activities of a person designed to develop information from a review of records, interviews of the subject, and interviews of people having knowledge of the subject. (IC Standard 700-1, 4 Apr 2008) See *personnel security investigation*.

> The Office of Personnel Management, Federal Investigative Services (OPM-FIS) provides investigative products and services for over 100 Federal agencies to use as the basis for suitability and security clearance determinations as required by Executive Orders, et al. OPM provides over 90% of the Government's background investigations, conducting over two million investigations a year.
>
> See OPM web site at: <http://www.opm.gov/investigations/background-investigations/>

Backdoor. Typically unauthorized hidden software or hardware mechanism used to circumvent security controls. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Backstop. Arrangements made to support a cover so that inquiries about the cover will elicit responses that make the cover appear to be true. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

-- Also, the arrangement made by documentary or oral means to support a cover story so that inquiries about it will elicit responses indicating the story is true. (ICS Glossary & AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, to make arrangements made through documentary, oral, technical, fiscal, legal, or other means to support covers (both individual and organizational). A backstopped cover provides sufficient documentation to protect an identity in the immediate area or circumstance and in primary U.S. Government and commercial information systems. A backstopped cover is constructed to withstand routine scrutiny. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, an arrangement made to support a cover story. (FBI FCI Terms)

Backstopping. Arrangements made to support covers and activities. (HDI Lexicon, April 2008)

-- Also, arrangements made through documentary, oral, technical, fiscal, physical, or other means to support covers (both individual and organizational). A backstopped cover provides sufficient documentation to project an identity in the immediate area or circumstance and in primary USG and commercial information systems. Backstopping cover may be constructed to withstand scrutiny ranging from casual or unwitting general population to a targeted hostile adversary. (DTM 08-050, Defense Cover Program Guidance (U), 31 Mar 2009 w/ chg 2 dated 14 Apr 2011)

-- Also, verification and support of cover arrangements for an agent [case officer or intelligence operative] in anticipation of inquiries or other actions that might test credibility of his or her cover. (Spy Book)

-- Also, a CIA term for providing appropriate verification and support of cover arrangements for an agent or asset in anticipation of inquiries or other actions which might test the credibility of his or its cover. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Badge. A distinctive official device usually made of cast metal, which is provided by the DoD Component and worn or carried by the bearer as a sign of authority. (DoDI 5240.25, Counterintelligence Badges and Credentials, 30 Sep 2011 with change 1 dated 15 Oct 2013) Also see *credentials*.

Basic Intelligence. Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (JP 1-02)

Beacon. A device typically fastened to an object or individual that transmits a radio signal in order to track its location. The technological discipline is called beaconry. (Spycraft)

Behavioral Science Consultant. A professional with extensive training in behavioral science, mental health, psychiatry, or psychology. (Previously in JP 2-01.2, CI & HUMINT Support to Joint Operations, 13 Jun 2006)

> Behavioral Science Consultants are psychologists and forensic psychiatrists, not assigned to clinical practice functions, but to provide consultative services to support authorized law enforcement, counterintelligence or intelligence activities, including detention and related counterintelligence, intelligence, interrogation, and detainee debriefing operations.

Bilateral Collection. A collection activity run jointly with a foreign intelligence service. (Previously in DoDI S-5240.17, CI Collection, 12 Jan 2009) Also see *multilateral.*

> Bilateral: Activities conducted with only a single foreign nation.

Bilateral/BILAT Operation. An operation run jointly with a foreign intelligence service or between two US intelligence/CI services. (CI Community Lexicon) Also see *unilateral operation.*

Bigot Case. An investigation that due to the sensitivity of the subject or the nature of the investigation, requires that it be handled on a strict need to know basis. Access to these investigations is controlled by maintaining a list of personnel who have been approved for access, called a "bigot list." (AR 381-20, Army CI Program, 25 May 2010) Also see *bigot list*, *compartmentation.*

Bigot List. Tradecraft jargon for any list of names of cleared personnel having restricted access (need-to-know) to a sensitive operation, investigation or to special access/compartmented intelligence. Also see *bigot case, compartmentation*.

-- Also, a restrictive list of persons who have access to a particular, and highly sensitive class of information. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

> *In some instances, a case, due to its sensitivity or the sensitivity of the information involved, will require that it be handled on a strict need-to-know basis. These cases are often referred to as BIGOT cases because access to them is controlled by a BIGOT list.*
>
> -- Army FM 2-22.2, *Counterintelligence*, October 2009
>
> ---
>
> According to a variety of sources, the term dates back to World War II when Allied orders for officers were stamped "TO GIB" for those being sent to Gibraltar for preparations for the invasion of North Africa; later their orders were stamped "BIG OT" (TO GIB backwards) when they were sent back to begin planning Operation OVERLORD, the invasion of Normandy. In WWII, it was convenient, in trying to find out if someone had access to highly restricted NEPTUNE and OVERLORD planning information, to ask "are you bigoted?" An indignant answer of "no" ended that part of classified discussion.

Biographical Intelligence. That component of intelligence that deals with individual foreign personalities of actual or potential importance. (JP 1-02)

Biometrics. The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *biometrics enabled-intelligence.*

-- Also, a general term used alternatively to describe a characteristic or a process. *As a characteristic:* A measurable biological (anatomical & physiological) and behavioral characteristic that can be used for automated recognition. *As a process:* Automated methods of recognizing an individual based on measurable biological (anatomical & physiological) and behavioral characteristics. (DoDD 8521.01E, DoD Biometrics, 21 Feb 2008)

-- Also, the measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition; examples include fingerprint, face, and iris recognition. (NSPD 59 / HSPD 24, Biometrics for Identification and Screening to Enhance National Security, 5 Jun 2008)

-- Also, measurable biological (anatomical and physiological) and behavioral characteristic that may be used for automated recognition of the identity of a person or to verify his claimed identity. Includes fingerprints, iris/retina, voice, facial, DNA, fingernail, and thermal signature. (AR 381-20, Army CI Program, 25 May 2010)

"Biometrics has become a non-lethal weapons systems in complex, irregular warfare environments. When you enroll a person in biometric systems now in use on the battlefield, you take away from our enemies the ability to remain anonymous. It's a high impact tool in the ongoing War on Terror and gives tactical commanders a decisive edge in today and tomorrow's battlespace."

-- LTG John F. Kimmons, U.S. Army G-2

The Secretary of the Army is the DoD Executive Agent for DoD Biometrics.

The term "biometrics" also describes both a *process* and a *characteristic*. As a process, biometrics consists of the automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Two basic types of biometrics: 1) *physical characteristics*, e.g., face, hand & finger geometry, iris, and vein structure; and 2) *behavioral characteristics*, e.g., voice, handwriting, typing, rhythm, and gait. For general information see <http://www.howstuffworks.com/biometrics.htm>

See Army TC 2-22.82, *Biometrics-Enabled Intelligence*, March 2011

Also see John Woodward, "Biometrics in the War on Terror," RAND Corporation (Dec 2005); available at -- <http://www.rand.org/commentary/2005/12/18/UPI.html>

Biometrics-Enabled Intelligence (BEI). Intelligence information associated with and or derived from biometrics data that matches a specific person or unknown identity to a place, activity, device, component, or weapon that supports terrorist / insurgent network and related pattern analysis, facilitates high value individual targeting, reveals movement patterns, and confirms claimed identity. (DoDD 8521.01E, DoD Biometrics, 21 Feb 2008) Also see *biometric-enabled watch list (BEWL).*

-- Also, the intelligence derived from the processing of biologic identity data and other all-source for information concerning persons of interest. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, the information associated with and/or derived from biometric signatures and the associated contextual information that positively identifies a specific person and/or matches an unknown identity to a place, activity, device, component, or weapon. (ADRP 2-0, Intelligence, Aug 2012)

BEI is a specialized analytical discipline that relies on all-source collections and a distinct processing, exploitation, reporting, and dissemination enterprise to integrate the information from U.S. and non-U.S. biometric collection and processing capabilities into all-source intelligence analysis for the purpose of monitoring or neutralizing the influence and operational capacity of individuals, cells, and networks of interest.

-- TC 2-22.82, *Biometrics-Enabled Intelligence*, March 2011, p. 1-9

Biometrics-Enabled Watch List (BEWL). Any list of interest with individuals identified by biometric sample instead of by name, and the desired/recommended disposition instructions for each individual. (TC2-22.82, Biometrics-Enabled Intelligence, March 2011)

> Within DoD, BEWL is a decision aid to help commanders determine what action to take when encountering a person of interest.

Black. 1) tradecraft jargon for inconspicuousness in the sense of being free of hostile surveillance [*going black*: become free of surveillance before conducting an operational act]; and 2) CIA tradecraft jargon for clandestine or covert. (Leo D. Carl, *The CIA's Insider Dictionary*, 1996)

-- Also, being free of hostile surveillance while on a clandestine mission; also refers to being in place undetected or unknown, such as flying in black. (A Spy's Journey)

-- Also, BLACK: designation applied to encrypted information and the information systems, the associated areas, circuits, components, and equipment processing that information. Also see *RED*. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Black Bag Job. [Tradecraft jargon] a surreptitious entry operation usually conducted by the FBI against a domestically located foreign intelligence target. (Spy Dust) Also see *surreptitious entry.*

> **Aka Covert Entry…**
>
> *Tactical Operations, a supersecret unit of FBI break-in artists who conduct court-authorized burglaries [covert entries] in homes, offices, and embassies to plant hidden microphones and video cameras and snoop into computers. …In any given year, TacOps conducts as many as four hundred of what the FBI calls covert entries. Eighty percent are conducted in national security cases relating to terrorism or counterintelligence.*
>
> *Over the years, the FBI has conducted successful covert entries at the Russian and Chinese embassies or their official diplomatic establishments, as well as at the homes of their diplomats and intelligence officers.*
>
> *Going up against foreign intelligence agencies is the biggest challenge because they set traps to detect entries.*
>
> -- Ronald Kessler, *The Secrets of the FBI* (2011), pp 2, 7, 11, & 173
>
> ---
>
> "Black Bag" -- *The term applied to clandestine entries of premises containing information that is likely to be of exceptional importance. The material may range from cryptographic data to the membership rolls of target organizations.*
>
> -- Nigel West, *Historical Dictionary of International Intelligence*.

Black List. [A list that] contains the identities and locations of individuals whose capture and detention are of prime importance, or individuals who have been determined to be intelligence fabricators. (CI Community Lexicon) Also see *Gray List; White List*.

-- Also, an official counterintelligence listing of actual or potential hostile collaborators, sympathizers, intelligence suspects, or other persons viewed as threatening to the security of friendly military forces. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

> Previous DoD definition in JP 1-02: an official counterintelligence listing of actual or potential enemy collaborators, sympathizers, intelligence suspects, and other persons whose presence menaces the security of friendly forces. *Note: this definition rescinded by JP 2-01.02, 11 Mar 2011.*
>
> ---

Examples of individuals who may be included on a Black List:
1) Known or suspected enemy or hostile espionage, sabotage, terrorist, political, and subversive individuals.
2) Known or suspected leaders and members of hostile paramilitary, partisan, or guerrilla groups.
3) Political leaders known or suspected to be hostile to the military and political objectives of the United States and/or an allied nation.
4) Known or suspected officials of enemy governments whose presence in the theater of operations poses a security threat to the U.S. Forces.
5) Known or suspected enemy collaborators and sympathizers whose presence in the theater of operations poses a security threat to the U.S. Forces.
6) Known enemy military or civilian personnel who have engaged in intelligence, CI, security, police, or political indoctrination activities among troops or civilians.
7) Other enemy personalities such as local political personalities, police chiefs, and heads of significant municipal and/or national departments or agencies.

-- USMC, MCWP 2-6 (previously 2-14), *Counterintelligence*, 5 Sep 2000

Black Swan Event. An event that is rare, predictable only in retrospect, with extreme impacts.

Blow [Tradecraft jargon] to expose—often unintentionally—personnel, installations or other elements of a clandestine activity or organization. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976) Also see *blown*.

Blown [Tradecraft jargon] to have one's cover exposed; to have an operation become public. (A Spy's Journey)

Bona Fides. The lack of fraud or deceit: a determination that a person is who he/she says he/she is. (National HUMINT Glossary)

Tradecraft jargon for credentials which establishes the credibility of a human source.

The determination of a defector or agent's bona fides, the verification of their truthfulness, is critical to the assessment of the information they provide.

-- Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present*, 2013, p. 77

-- Also, good faith. In personnel recovery, the use of verbal or visual communication by individuals who are unknown to one another, to establish their authenticity, sincerity, honesty, and truthfulness. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

-- Also. the lack of fraud or deceit: a determination that a person is who he/she says he/she is. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, physical and/or oral exchanges employed by an unknown individual to prove identity and foster trust. (HDI Lexicon, April 2008)

-- Also, documents, information, action, codes, etc., offered by an unknown or otherwise suspected individual to establish his or her good faith, identification, dependability, truthfulness, or motivation. (ICS Glossary & AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Border Crosser. An individual, living close to a frontier, who normally has to cross the frontier frequently for legitimate purposes. (JP 1-02)

Botnet. A collection of zombie PCs [personal computers]. Botnet is short for robot network. A botnet can consist of tens or even hundreds of thousands of zombie computers. A single PC in a botnet can automatically send thousands of spam messages per day. The most common spam messages come from zombie computers. (McAfee Labs - Threat Glossary) Also see *zombie*.

-- Also, Botnets, or Bot Networks, are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. (CRS Report PL32114, 29 Jan 2008)

-- Also, A network of "zombie" computers controlled by a single actor. Botnets are a common tool for malicious activity on the Internet, such as denial-of-service attacks and spam, since they provide free 9stolen) computation and network resources while hiding the identity of the controller. (Cybersecurity and Cyberwar)

> Botnets have been described as the
> ***"Swiss Army knives of the underground economy"***
> because they are so versatile.

Brevity Code. [In intelligence usage] Communications security (COMSEC) term for a code used only for shortening the length of a message, but not to conceal its content. (Cited as FBI Glossary in *CIA's Insider's Dictionary* by Leo D. Carl) [Note: although the brevity code does not conceal content (the actual words used), it can be used to conceal true meaning]

-- Also, [non intelligence usage] a code which provides no security but which has as its sole purpose the shortening of messages rather than the concealment of their content. (JP 1-02; JP 3-04; and FM 1-02.1, Multi-Service Brevity Codes, Jun 2005)

Brief Encounter. A short and discreet operational contact. (HDI Lexicon, April 2008) Also see *brush contact; brush pass*.

-- Also, any brief physical contact between a case officer and an agent under threat of surveillance. (CI Centre Glossary)

Brush Contact. A discreet momentary contact, usually prearranged between intelligence personnel, during which material or oral information is passed. (ICS Glossary & AFOSI Manual 71-142, OFCO, 9 Jun 2000) Also see *brush pass; brief encounter*.

> *Such a contact is extremely brief as well as surreptitious,*
> *and usually it is quite secure if well executed.*
> -- Victor Marchetti & John D. Marks,
> *The CIA and the Cult of Intelligence,* 2nd edition (1980), p 230

-- Also, a discreet, usually prearranged momentary contact between intelligence personnel when information or documents are passed. Also known as a brief encounter. (FBI FCI Terms)

-- Also, a technique used by case officers to receive [or] exchange information from an agent clandestinely without betraying any signs of recognition between participants. The objective is to complete the transaction without detection by any hostile surveillance. (*Historical Dictionary of Cold War Counterintelligence,* 2007)

> ***Brush Contact*** – credited largely to Haviland Smith, who served as the CIA station chief in Prague from 1958 to 1960. See Benjamin Weiser, *A Secret Life: The Polish Officer, His Covert Mission, and the Price He Paid to Save His Country* (2004)
>
> *"He found that if he walked along a street and turned right, he created a gap in which the agents [surveillance] trailing him would lose sight of him for a few seconds…. Do not elude surveillance, accept it as a way of life."*

Brush Pass. A brief operational encounter (seconds or less) in which the case officer passes something (verbally or physically) to or receives something from the agent, or a two-way exchange takes place. (National HUMINT Glossary) Also see *brief encounter; brush contact*.

-- Also, a discreet, monetary contact during which something is exchanged. (HDI Lexicon, April 2008)

-- Also, a brief encounter where something is passed between a case officer and an agent. (CI Centre Glossary)

-- Also, the clandestine, hand-to-hand delivery of items or payments – made as one person walks past another in a public place [The Russian Foreign Intelligence Service (SVR) refers to a brush pass as a "flash meeting"]. (FBI – Court Affidavit re: Russian Illegals, 25 June 2010)

Bug. [Tradecraft jargon] 1) Concealed listening device or other equipment used in audio surveillance; 2) To install such a device; the term "bugged" refers to a room or object that contains a concealed listening device. (Spy Book)

-- Also, a concealed listening device or microphone, or other audiosurveillance device; also to install the means for audiosurveillance of a subject or target. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Bugging… Electronic Surveillance

Bugging is a term in common use that refers to the various forms of clandestine electronic surveillance, or eavesdropping. See *Spycraft*, pp. 405-416, for details.

Bug -- *a covert or clandestine listening or viewing device that is noted for its small, inconspicuous (bug-like) size. Bugs used to primarily mean primarily listening devices, small microphones that could be hidden in plants or phone handsets, but the term now is also used to describe tiny pinhole cameras that are as small as audio bugs used to be twenty years ago. A bug may be wired or wireless and may or may not be sending information a recording device.*

-- Julie K. Petersen, *Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications* (2001)

[The FBI's] Engineering Research Facility at Quantico… makes custom-designed bugging devices, tracking devices, sensors, and surveillance cameras to watch and record bad guys. It also develops ways to penetrate computers and defeat locks, surveillance Cameras, and alarm and access control systems.

…state-of-the-art FBI bug… a circuit board that is the size of a postage stamp and the thickness of two stacked quarters "It's a transmitter and stereo recorder… it records for about twenty-one hours, and will transmit to a local receiver in encrypted form…. This is actually big in comparison to some of our bugs."

-- Ronald Kessler, *The Secrets of the FBI* (2011), pp 8-9 and 227-228

Bugged. Room or object that contains a concealed listening device. (JP 1-02)

Burned. [Tradecraft jargon] When a case officer or agent is compromised, or a surveillant has been made by a target, usually because they make eye contact. (CI Centre Glossary)

Burn Notice. *Within DoD: None – term removed from JP 1-02 per JP 2-0 Joint Intelligence (22 Oct 2013).*

Previously defined in JP 1-02 as: an official statement by one intelligence agency to other agencies, domestic or foreign, that an individual or group is unreliable for any of a variety of reasons.

C ==========

Campaign. A series of related military operations aimed at achieving strategic or operational objectives within a given time and space. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *DoD Strategic CI Campaign*.

Campaign Plan. A joint operation plan for a series of related military operations aimed at achieving strategic or operational objectives within a given time and space. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *Campaign; Campaign Planning; DoD Strategic CI Campaign*.

Campaign Planning. The process whereby combatant commanders and subordinate joint force commanders translate national or theater strategy into operational concepts through the development of an operation plan for a campaign. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *campaign; campaign plan*.

Capability. The ability to execute a specified course of action. (A capability may or may not be accompanied by an intention.) (JP 1-02)

Capability Gap. The inability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. The gap may be the result of no existing capability or lack of proficiency or sufficiency in existing capability.

Captured or Detained Personnel. Any person captured, detained, held, or otherwise under the control of DoD personnel (military or civilian). This does not include DoD personnel or DoD contractor personnel being held for law enforcement purposes. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

Car Pick-Up. A personal meeting wherein the handler picks up the source. (HDI Lexicon, April 2008)

Car Toss. A form of dead drop using a concealment device thrown to a preselected site from a vehicle traveling along a designated route. (HDI Lexicon, April 2008) Also see *brief encounter; brush contact, brush pass.*

-- Also, the method of conveying information clandestinely by throwing a package into, or out of, a vehicle is known as the "car toss." (*Historical Dictionary of Cold War Counterintelligence*, 2007)

> *[P]ull just far enough ahead of [surveillance] so that when he turned a curve…. or disappeared over a small hill, he was able to create ten- to twenty-second gaps during which he could throw a soda can or bottle out the window and in to a ditch by the road. In such "car tosses", beepers might be placed inside the object along with a message, so that the agent with a small radio could find it easily.*
>
> -- Benjamin Weiser, *A Secret Life* (2004) pb, p.79

Carbons. Paper that produces secret writing [SW] through the use of chemicals. (FBI FCI Terms and Spy Book) Also see *secret writing*.

-- Also, paper invisibly impregnated with chemicals which, when used in accordance with directions, will produce secret writing. Illegals and agents often posses carbons which appear as ordinary sheets in writing pads that are manufactured in the target country. (AFOSI Manual 71-142, OFCO, 9 June 2000)

Carve-Out. A provision approved by the Secretary or Deputy Secretary of Defense that relieves DSS [Defense Security Service} of its National Industrial Security Program obligation to perform industrial security oversight functions for a DoD SAP [Special Access Program]. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

-- Also, a classified contract for which the Defense Security Service (DSS) has been relieved of inspection responsibility in whole or in part. (DSS Glossary)

CARVER. A special operations forces acronym used throughout the targeting and mission planning cycle to assess mission validity and requirements. The acronym stands for criticality, accessibility, recuperability, vulnerability, effect, and recognizability. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Case. The framework which not only acts as the repository for all logically/physically related facts, issues, allegations and products (outputs) associated with the investigative process, but also serves to document, in a case file, the approvals, authorities, waivers, plans, notes and other artifacts relevant to that particular instance of the process. (ONCIX Insider Threat Detection – Glossary)

-- Also, an intelligence operation in its entirety; the term also refers to a record of the development of an intelligence operation, how it will operate, and the objectives of the operation. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

> Can also be used as a verb, to case, meaning to surreptitiously observe a physical location to determine its suitability for possible future operational use.
>
> Previously defined in DoD (JP 1-02) as: 1) An intelligence operation in its entirety; or 2) Record of the development of an intelligence operation, including personnel, modus operandi, and objectives. Approved for removal per JP 2-0 *Joint Intelligence* (22 Oct 2013).

Case Officer (C/O). A professional employee of an intelligence or counterintelligence organization who is responsible for providing directions for an agent operation and/or handling intelligence assets. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; CI Community Lexicon; and ICS Glossary) Also see *Agent Handler*.

-- Also, [an intelligence employee] who is responsible for managing and directing agents (assets) in the field. Case officers are sometimes referred to as "operations officers." (*Encyclopedia of the CIA*, 2003)

> *"…the case officer's job is to handle operational cases and assets; this is to say the case officer recruits and directs foreign indigenous spies who are known as "agents."*
>
> -- Fred Rustmann, Jr., "Debunking the CIA Case Officer Myth," *AFIO Newsletter*; 25: 1&2 (2002)

Casing. Reconnaissance of an operating area, whether for surveillance or for personal or impersonal communications. (CI Community Lexicon)

-- Also, a study of a site to determine operational suitability. (HDI Lexicon, April 2008)

-- Also, covert or clandestine inspection or surveillance of an area, place, or building to determine its suitability for operational use or its vulnerability to an intelligence operation. (AFOSI Instruction 71-101, 6 Jun 2000 and AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Catastrophic Event. Any natural or man-made incident, including terrorism, which results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013) Also see *complex catastrophe*.

Caveat. A designator used with or without a security classification to further limit the dissemination of restricted information, e.g., FOUO and NOFORN. (IC Standard 700-1, 4 Apr 2008)

-- Also, a designator used with a classification to further limit the dissemination of restricted information. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

Cell. [In intelligence usage,] a small group of individuals who work together for clandestine or subversive purposes.

CELLEX. See *cellular telephone exploitation*.

Cellular Telephone Exploitation (CELLEX). Exploitation of cellular phones at the logical or physical level to extract cogent contextual information, includes holistic examinations of mobile devices and associated digital media (e.g., SIM cards, media cards).

Center [British spelling: *Centre*]. The headquarters site in the home country where control of intelligence and espionage operations in foreign countries is maintained. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, intelligence service headquarters. (FBI FCI Terms)

Center of Gravity (COG). The source of power that provides moral or physical strength, freedom of action, or will to act. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Central Intelligence Agency (CIA). An independent US Government agency responsible for providing national security intelligence to senior US policymakers. Primary mission: collect, analyze, evaluate, and disseminate foreign intelligence to assist the President and senior US government policymakers in making decisions relating to national security. Major components: National Clandestine Service (NCS), Directorate of Intelligence, Directorate of Science & Technology and Directorate of Support. (cia.gov) Also see *National Clandestine Service*.

We do espionage. That is the nature of what we do. We steal secrets.
-- DCI George Tenet, 23 June 1998
Interview in *Studies in Intelligence*, 42:1 (1998)

Director CIA is designated the Functional Manager for human intelligence IAW EO 12333; and is also the National HUMINT Manager IAW ICD 304, Human Intelligence.

Director CIA coordinates the clandestine collection of foreign intelligence through human sources or through human-enabled means and counterintelligence activities outside the United States (EO 12333).

The CIA may engage in covert action at the President's direction and in accordance with applicable law; see *covert action*.

The Director CIA serves as the head of the Central Intelligence Agency and reports to the Director of National Intelligence. The CIA director's responsibilities include:

-- Collecting intelligence through human sources and by other appropriate means, except that he shall have no police, subpoena, or law enforcement powers or internal security functions;
-- Correlating and evaluating intelligence related to the national security and providing appropriate dissemination of such intelligence;
-- Providing overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the Intelligence Community authorized to undertake such collection and, in coordination with other departments, agencies, or elements of the United States Government which are authorized to undertake such collection, ensuring that the most effective use is made of resources and that appropriate account is taken of the risks to the United States and those involved in such collection; and
-- Performing such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct.

The function of the Central Intelligence Agency is to assist the Director of the Central Intelligence Agency in carrying out the responsibilities outlined above.

Source: https://www.cia.gov/about-cia/index.html (accessed 20 Aug 2012)

CFIUS. See *Committee of Foreign Investment in the United States*.

Chain of Custody. A chronological written record reflecting the release and receipt of evidence from initial acquisition until final disposition. (AR 195-5, Evidence Procedures, 25 Jun 2007) Also see *evidence; chain of evidence*.

-- Also, a process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a process used to maintain and document the chronological history of the evidence. (Documents should include name or initials of the individual collecting the evidence, each person or entity subsequently having custody of it, dates the items were collected or transferred, agency and case number, victim's or suspect's name, and a brief description of the item.) (Crime Scene Investigation: A Guide for Law Enforcement, Sep 2013)

> Chain of Custody is a process used to document the chronological history of evidence to maintain the security, integrity and accountability of its handling.

Chain of Evidence. A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *evidence; chain of custody*

Chairman's Guidance (CG). Provides a common set of assumptions, priorities, intent, and critical planning factors required to develop future strategies and plans. It is an integral part of the strategy development process. CG may be established pursuant to conducting a Joint Strategy Review, to preparing a Joint Vision, or to Drafting a new National Military Strategy; or it may be provided separately if deemed appropriate. (CJCSI 3100.01A, Joint Strategic Planning System, 1 Sep 1999)

Chancery. The building upon a diplomatic or consular compound which houses the offices of the chief of mission or principal officer. (JP 1-02)

Characterization. [In critical infrastructure protection usage] the analytic decomposition of functions, systems, assets, and dependencies related to supporting DoD operational capabilities and assets. DoDD 3020.40, (DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010, w/ chg 2 dated 21 Sep 2012)

Chief of Mission (CoM). The principal officer in charge of U.S. Diplomatic Missions and U.S. offices abroad, which the Secretary of State has designated as diplomatic in nature. The CoM reports to the President through the Secretary of State. Also see *Ambassador*.

-- Also, the principal officer (the ambassador) in charge of a diplomatic facility of the United States, including any individual assigned to be temporarily in charge of such a facility. The CoM is the personal representative of the President to the country of accreditation and is responsible for the direction, coordination, and supervision of all US Government executive branch employees in that country (except those under the command of a US area military commander). The security of the diplomatic post is the CoM's direct responsibility. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011)

> The U.S. Ambassador to a foreign country, for example, is the Chief of the U.S. Mission (CoM) in that country. Other CoMs include the Chiefs of permanent U.S. Missions to international organizations (e.g., the U.S. Mission to International Organizations in Vienna), the Principal Officers of Consulates General, and the U.S. Interest Section in the Swiss Embassy in Havana.

> The CoM has full responsibility and authority for the direction, coordination, and supervision of all USG executive branch employees in country and at international organizations, regardless of their employment categories or location, except those under command of a U.S. area military commander or on the staff of an international organization.

Chief of Station (CoS). The senior United States intelligence officer in a foreign country, and is the direct representative of the Director National Intelligence, to whom the officer reports through the Director Central Intelligence Agency. Usually the senior representative of the Central Intelligence Agency assigned to a US Mission. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Choke Point. A narrow passage--such as a bridge, tunnel, or Metro station--used as a surveillance or countersurveillance tool for channeling the opposing force or monitoring their passage. (CI Centre Glossary)

CHROME. Acronym for *Counterintelligence and Human Intelligence Requirements-Reporting and Operations Management Environment*. Interoperable, synchronized information technology architecture to replace and retire legacy software systems to accelerate workflow, increase efficiency, and broaden intelligence sharing within DoD and across the IC. (DoD FCIP Strategy FY 2013-2017)

Church Committee (aka the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities). A U.S. Senate committee chaired by Senator Frank Church (D-ID) in 1975. A precursor to the U.S. Senate Select Committee on Intelligence (SSCI), the committee investigated intelligence gathering by the CIA, FBI, and NSA after certain activities had been revealed by the Watergate affair. (Wikipedia at <http://en.wikipedia.org/wiki/Church_Committee>)

> In 1975 and 1976, the Church Committee published fourteen reports on the formation of U.S. intelligence agencies, their operations, and the alleged abuses of law and of power that they had committed, together with recommendations for reform, some of which were put in place. Under recommendations and pressure by this committee, President Gerald Ford issued Executive Order 11905 (ultimately replaced in 1981 by President Reagan's Executive Order 12333).
>
> Regarding counterintelligence see Book I *Foreign and Military Intelligence*, pp. 163-178
>
> Copies of the Church Committee reports at the following two web sites:
> -- <http://www.intelligence.senate.gov/churchcommittee.html>
> -- <http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm>

CI. See *counterintelligence*.

CI-21. Counterintelligence for the 21st Century. (See White House Fact Sheet, "The PDD on CI-21: Counterintelligence for the 21st Century" – copy at <http://www.fas.org/irp/offdocs/pdd/pdd-75.htm>)

> Designed to provide a national counterintelligence system which is predictive and proactive, one that includes integrated oversight of national CI activities across government and the private sector. Established: 1) the National CI Policy Board of Directors (Dir FBI, Dep SECDEF, DDCI, and DoJ Representative); 2) the National CI Executive (NCIX); and the Office of the National CI Executive.
>
> _____
>
> *"The general premise behind CI-21 is to try and determine what are America's true equities, and then extend this interagency cooperation in a systematic way to try and better protect those assets and deter acts of espionage that target them. We can no longer afford to focus our counterintelligence efforts only after an incident has sparked a full criminal case, because at that point it's too late. The damage has already been done."*
>
> -- DCI George Tenet quoted in "Anti-Terror Alliance," *Government Executive Magazine*, 1 Feb 2001
>
> _____

"CI-21 is a manifestation of a process… we all began to realize that the threats to U.S. security were changing in a way that our traditional organizations and structures couldn't match… Globalization and technology were lowering traditional boundaries between what constitutes an international or domestic threat, and terrorists, drug cartels, spies and hackers were all leaping those boundaries with impunity."

-- John MacGaffin, Former ADDO, CIA and Former FBI Consultant who spearhead CI-21

CI Campaign. See *DoD Counterintelligence Campaign*.

CI Mission Tasking Authority. See *Counterintelligence Mission Tasking Authority*.

Cipher. Any cryptographic system in which arbitrary symbols (or groups of symbols) represent units of plain text of regular length, usually single letters; units of plain text are rearranged; or both, in accordance with certain predetermined rules. (JP 1-02) Also see *code; cipher pad*.

Cipher Pad. A small thin pad of paper sheets having nonrepetitive key, usually machine printed. A sheet is used once for enciphering and another sheet used once for deciphering a communication. Occasionally called a one-time pad (OTP). (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

CISO Acronym for Counterintelligence Staff Officer. Within DoD, term rescinded.

Note: within DoD this term replaced by "*Command CI Coordinating Authority*" or CCICA.

CIR. Acronym for Counterintelligence Incident Report.

Civil Authorities. Those elected and appointed officers and employees who constitute the government of the United States, the governments of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, United States territories, and political subdivisions thereof.
(JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

Civil Aviation Intelligence. Activities undertaken to understand how trends in the global civil aviation industry impact U.S. interests; or detect, analyze, monitor, and warn of illicit activity or threats to the United States, its allies, or its interests involving civil aviation. (DoDI 3115.14, Civil Aviation Intelligence, 29 Jul 2011)

Civil Disturbance. *Within DoD: None -- term removed from JP 1-02.*

Previous defined in JP 3-28, Civil Support (14 Sep 2007) as: Group acts of violence and disorder prejudicial to public law and order.

Civilian Internee. A civilian who is interned during armed conflict, occupation, or other military operation for security reasons, for protection, or because he or she committed an offense against the detaining power. (JP 3-63, Detainee Operations, 30 May 2008)

Clandestine. Any activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy or concealment. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) See *clandestine collection; clandestine intelligence; clandestine intelligence activity; clandestine intelligence collection clandestine operation; covert.*

-- Also, any HUMINT [Human Intelligence] or other activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy or concealment. (ICD 304, HUMINT, 1 Mar 2007 and DoDD S-5200.37, Management & Execution of Defense HUMINT, 9 Feb 2009)

-- Also, any illicit/illegal activity that is designed not to be detected by anyone, including a local security service. Concealed, hidden, secret, or surreptitious operation conducted without the knowledge of anyone but the organization conducting the operation or investigation. (CI Community Lexicon)

-- Also, method of conducting operations with secrecy by design. Differs from covert in that covert conceals the identity of the sponsor, whereas clandestine conceals the identity of the operation. (National HUMINT Glossary)

-- Also, secret or hidden activity conducted with secrecy by design. (ICS Glossary, 1978)

Clandestine, from the Latin *clam*, "secretly, in private."

Words have meaning… clandestine and covert are not synonymous

"I don't take lightly the distinction between clandestine and covert…
It makes all the difference in the world."

-- Senator Jay Rockefeller, Senate Select Committee on Intelligence

Clandestine Collection. The acquisition of protected intelligence information in a way designed to protect the source, and conceal the operation, identity of operators and sources, and actual methodologies employed. (Previously in DoDI S-5240.17, CI collection, 12 Jan 2009) Also see *clandestine intelligence; clandestine intelligence collection.*

Clandestine Intelligence. Intelligence information collected by clandestine sources. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Clandestine Intelligence Activity. An activity conducted by or on behalf of a foreign power for intelligence purposes or for the purpose of affecting political or governmental processes if the activity is conducted in a manner designed to conceal from the U.S. Government the nature or fact of such activity or the role of such foreign power; also, any activity conducted in support of such activity. (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

Clandestine Intelligence Collection. The acquisition of protected intelligence information in a way designed to conceal the nature of the operation and protect the source. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the acquisition of protected intelligence information in a way designed to protect the source. (National HUMINT Glossary)

Clandestine Operation. An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

-- Also, activities to accomplish intelligence, CI, or similar activities in such a way as to maintain secrecy or concealment especially for the purpose of deception or subversion. (CI Community Lexicon)

-- Also, a pre-planned secret intelligence information collection activity, technical operation, or covert political, economic, propaganda, or paramilitary action conducted so as to assure the secrecy of the operation; encompasses clandestine collection, counterintelligence, and covert action. (National HUMINT Glossary)

-- Also, any HUMINT or other activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy or concealment. (DHE-M 3301.002, Vol II, Collection Operations, 23 Nov 2010)

Clandestine operations are sometimes incorrectly referred to as "covert operations." Although both are secret and sensitive activities, the terms are not interchangeable. See c*overt operation*.

Clandestine Nuclear Threat. A nuclear or radiological attack by anyone for any purpose, against the United States and/or U.S. military operations, and delivered by means other than (military) missiles or aircraft. A large subset of this threat is the smuggling of nuclear weapons, devices, or materials for use against the United States. (DSB Report, Jun 2004)

Today, it would be easy for adversaries to introduce and detonate a nuclear explosive clandestinely in the United States.

-- Defense Science Board Report (June 2004)*

*Copy of "Report of the Defense Science Board Task Force Report on Preventing and Defending Against Clandestine Nuclear Attack," June 2004 available at: <http://www.acq.osd.mil/dsb/reports/ADA429042.pdf>

Clandestine Service. See *National Clandestine Service (NCS); Defense Clandestine Service (DCS).*

Classification. The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Classification—Driving Security

The classification system is designed primarily to protect the confidentiality of certain military, foreign policy, and intelligence information. It deals only with a small slice of the government' information that requires protection although it drives the government's security apparatus and most of its costs.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, pp.7

Classified Information. Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, information or material designated and clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statue or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security. (50 USC § 426[1])

Classified Information Procedures Act (CIPA). The tool with which the proper protection of classified information may be ensured in indicted cases. After a criminal indictment becomes public, the prosecutor remains responsible for taking reasonable precautions against the unauthorized disclosure of classified information during the case. This responsibility applies both when the government intends to use classified information in its case-in-chief as well as when the defendant seeks to use classified information in his/her defense. (18 USC, App III, Sec 1-16) Also see *graymail*.

Congress enacted CIPA (Public Law 96-456) in 1980. The procedural protections of CIPA protect unnecessary disclosure of classified information. The primary purpose was to limit the practice of "graymail" by criminal defendants in possession of sensitive government secrets.

"Gray mail" refers to the threat by a criminal defendant to disclose classified information during the course of a trial. The gray mailing defendant essentially presented the government with a "Hobson's choice": either allow disclosure of the classified information or dismiss the indictment.

CIPA is a procedural statute that balances the right of a criminal defendant with the right of the sovereign to know in advance of a potential threat from a criminal prosecution to its national security. CIPA's provisions are designed to prevent unnecessary or inadvertent disclosures of classified information and to advise the government of the national security "cost" of going forward.

See: <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm02054.htm>

Classified Military Information (CMI). Information requiring protection in the interest of national security and is limited to three classifications: TOP SECRET, SECRET and CONFIDENTIAL as described in Executive Order 13526, *Classified National Security Information* (previously EO 12958 13526) and which is under the control or jurisdiction of the DoD or its Departments or Agencies.

Basic USG policy provided in National Security Decision Memorandum (NSDM) 119 "Disclosure of Classified United States Military Information to Foreign Governments and International Organizations": CMI is a national security asset which must be conserved and protected and which must be shared with foreign governments and international organizations only where there is a clearly defined advantage to the U.S.

Copy of NSDM 119 at: <http://www.nixonlibrary.gov/virtuallibrary/documents/nsdm/nsdm_119.pdf>

Classified National Intelligence (CNI). National intelligence as defined in 50 USC 401a(5), classified pursuant to EO 13526. (ICD 703, Protection of Classified National Intelligence Including Sensitive Compartmented Information, 21 Jun 2013) Also see *Sensitive Compartmented Information*.

Protection of CNI, including SCI, is also achieved through adherence to counterintelligence (CI) and security practices.

-- ICD 703, *Protection of Classified National Intelligence, including Sensitive Compartmented Information*, 21 Jun 2013, p. 2

Clean. [Tradecraft jargon] To be free of hostile surveillance. (*A Spy's Journey*)

Clean Phone. Tradecraft jargon which typically refers to a disposable, pre-paid cellular telephone that cannot be traced back to the original retail purchaser or subsequent user(s).

Clearance. Formal security determination by an authorized adjudicative office that an individual is authorized access, on a need to know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL). (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Cleared Contractor (CC). A person or facility operating under the National Industrial Security Program (NISP), that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level (and all lower levels). There are approximately 8500 cleared contractors with over 13,000 facilities. (DSS - Glossary to Insider Threat Awareness Course)

The Defense Security Service (DSS) refers to "cleared contractors" as they support DoD as well as other U.S. Government Departments and Agencies. DSS oversees the protection of U.S. and foreign classified information and technologies in the hands of industry under the National Industrial Security Program (NISP). "The NISP applies to all Executive Branch Departments and Agencies and to all cleared contractor facilities located within the United States" (para 1-102, NISPOM).

Cleared Defense Contractor (CDC). A company or academic institution (i.e., university or college) that has entered into a security agreement with the DoD, and was granted a facility (security) clearance enabling the entity to be eligible for access to classified information of a certain category, as well as all lower categories. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

-- Also, a subset of contractors cleared under the NISP who have contracts with the Department of Defense. Therefore, not all cleared contractors have contracts with DoD. (DSS - Glossary to Insider Threat Awareness Course)

Click-jacking. Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed “Like” and “Share” buttons on social networking sites. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks>)

Coalition. An arrangement between two or more nations for common action. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *alliance*; *multinational.*

Coast Guard Counterintelligence Service (CGCIS). Component of Coast Guard Intelligence that provides full-spectrum counterintelligence support to the U.S. Coast Guard. Office symbol: CG-2-CI.

> *CGCIS preserves the operational integrity of the Coast Guard by shielding its operations, personnel, systems, facilities and information from Foreign Intelligence and Security Services (FISS), and the intelligence efforts of terrorist organizations, drug trafficking elements and other organized crime groups, and adversaries, and insider threats. CGCIS supports the identification, understanding, neutralization, and exploitation of the operations of FISS and of non-state actors who employ intelligence tradecraft. CGCIS manages the Foreign Visitor Program, providing tailored foreign intelligence threat and awareness briefings specific to foreigners visiting Coast Guard commands. CGCIS also conducts foreign travel briefs and debriefs, providing tailored foreign intelligence threat and awareness briefings on FISS, terrorism, and criminal threats, and health concerns to educate Coast Guard personnel traveling to high-threat countries.*
>
> -- Coast Guard Publication 2-0, *Intelligence*, May 2010

Code. 1) Any system of communication in which arbitrary groups of symbols represent units of plain text of varying length. Codes may be used for brevity or for security; 2) a cryptosystem in which the cryptographic equivalents (usually called "code groups"), typically consisting of letters or digits (or both) in otherwise meaningless combinations, are substituted for plain text elements which are primarily words, phrases, or sentences. (Previously in JP 1-02) Also see *cipher*.

-- Also, system of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a system of communication in which arbitrary groups of symbols represent units of plain text. Codes may be used for brevity or for security. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

> *“There is no sharp theoretical line between codes and ciphers; [a] useful distinction is that code operates on linguistic entities, dividing its raw material into meaningful elements and cipher does not.”*
>
> -- David Kahn, *The Code Breakers* (1967)

Code Book. Document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Code Word. A single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans, activities or operations classified CONFIDENTIAL or higher. (DoDI 5205.11, Management, Administration, and Oversight of DoD Special Access Programs, 6 Feb 2013)

-- Also, a single classified word assigned to represent a specific SAP or portions thereof. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

-- Also, 1) A word that has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation; and 2) A cryptonym used to identify sensitive intelligence data. (JP 1-02 and JP 3-50, Personnel Recovery, 20 Dec 2011)

-- Also, a prearranged word used in communication or conversation to disguise the identity of someone or something or to convey a meaning other than its conventional meaning. (AFOSI Manual 71-142, 9 Jun 2000) Also see *nickname*.

Cold Pitch. Recruitment approach without prior development or, in some cases, contact. (National HUMINT Glossary)

> *The confrontational "cold pitch" was one of the riskiest methods, putting great psychological pressure on a target, and often failed. Even when successful, it often produced agents whose handlers had to maintain constant pressure on them to stay involved. When such agents had a chance to cut their ties—when they were assigned to new posts or when communications with their contacts became risky—they often took it.*
>
> -- Victor Cherkashin, KGB Counterintelligence Officer and author of *Spy Handler* (2005)
>
> ---
>
> *Nobody likes cold pitches because they're the worst technique in the profession of intelligence. It's going up to somebody whom you don't know and asking them to do the equivalent of going to bed with you. It's a very intimate, and if you're not developing it from a practical interrelationship human kind of way, 99.9 percent of the folks will say no.*
>
> -- Michael T. Rochford, Chief, Espionage Section, Counterintelligence Division, FBI as quoted in *The Secrets of the FBI* (2011) by Ronald Kessler, p. 125

Cold War. Term generally used to describe the long-term, but nonshooting, conflict or state of tension between the United States and the Soviet Union that lasted from the close of World War II in 1945 until the collapse of the Soviet Union in 1991. (*Encyclopedia of the CIA*, 2003)

COLISEUM. See *Community On-Line Intelligence System for End-Users and Managers*.

Collaborating Analytical Center (CAC). An intelligence organization that has responsibility to support and assist a Responsible Analytical Center (RAC) produce an intelligence product to answer a specific COCOM Intelligence Task List (ITL) task or sub-task. CACs may provide all-source analysis, application of analysis, or single-source analysis, exploitation, or reporting. DoD organizations that may serve as CACs include: Combat Support Agencies (DIA, NSA, NGA), the COCOM JIOCs, and the Service Intelligence Centers (NGIC, ONI, NASIC & MCIA). (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007)

Collateral. All national security information classified Confidential, Secret, or Top Secret under the provisions of an Executive Order for which special systems of compartmentation (such as SCI or SAPs) are not formally required. (DoDI 5200.01, 9 Oct 2008)

Collation. The organizing of relevant information in a coherent way, looking at source and context. It includes evaluating the information for accuracy, completeness, and meaning. (Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*, 2004)

Collection. In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012) Also see *counterintelligence collection*; *clandestine intelligence collection; intelligence collection; military counterintelligence collection*.

-- Also, the acquisition of information to meet an intelligence requirement. (ICD 300, 3 Oct 2006)

> ICD 300 (*Management, Integration, and Oversight of Intelligence Collection and Cover Action*, 3 Oct 2006) establishes DNI policy to integrate, prioritize, and maximize IC collection capabilities and activities to produce timely and useful national intelligence information for policymakers, Defense, and other intelligence consumers.

-- Also, the identification, location, and recording and storing of information— typically from an original source and using both human and technological means—for input into the Intelligence Cycle for the purpose of meeting a defined tactical or strategic intelligence goal. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, the exploitation of sources by collection agencies, and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. (National HUMINT Glossary)

-- Also, the acquisition of information by any means and its delivery to the proper intelligence processing unit for use in the production of intelligence. (Senate Report 94-755, Book I, 26 Apr 1976)

"*Collection is the gathering of valued information, much of it by clandestine means.*"
-- Roy Godson, Dirty Tricks or Trump Card: US Covert Action and Counterintelligence (1995), p.1

"*The collection of information is the foundation of everything that the Intelligence Community does. While successful collection cannot ensure a good analytical product, the failure to collect… turns analysis into guesswork*."
-- *WMD Report* (2005); p. 351

EO 12333, *US Intelligence Activities*, directs that IC elements use the least intrusive collection techniques feasible within the United States or directed against US persons abroad (para 2.4 - Collection Techniques).

Collection Agency. Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Collection Asset. A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Collection Emphasis. Identifies new short- to intermediate-term information needs in response to unforeseen situations, emerging crises, or contingencies. It can be used to register additional or refined requirements in connection with a unique collection opportunity. (DoD CI Collection Integrated Working Group Handbook 1-02, 8 Aug 2006)

Collection Management (CM). In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and re-tasking, as required. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

CM has two distinct functions: collection requirements management (CRM) and collection operations management (COM). CRM established the collection need and COM provides the "how to" for conducting the actual collection. See *collection requirements management* and *collection operations management.*

"The matters that interest an intelligence service are so numerous and diverse that some order must be established in the process of collecting information."
-- Allen W. Dulles, *The Craft of Intelligence* (2006), p.75

Collection Management Authority (CMA). Within DoD, CMA constitutes the authority to establish, prioritize, and validate theater collection requirements, establish sensor tasking guidance, and develop theater-wide collection policies. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Collection Manager. An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Collection Operations Management (COM). The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *collection management*; *collection requirements management*.

> COM is the process by which it is determined **"how"** a requirement will be answered within an intelligence discipline and "who" will execute the collection activity.
>
> ---
>
> *"Essentially, CRM is what gets done in the collection cycle, while COM is how it gets done."*
> -- ODNI, *U.S. National Intelligence – An Overview 2011*

Collection Plan. A systematic scheme to optimize the employment of all available collection capabilities and associated processing, exploitation, and dissemination resources to satisfy specific information requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

> The collection plan determines how a collection requirement will be satisfied.

Collection Planning. A continuous process that coordinates and integrates the efforts of all collection units and agencies. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Collection Posture. The current status of collection assets and resources to satisfy identified information requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Collection Requirement. A valid need to close a specific gap in intelligence holdings in direct response to a request for information (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *intelligence requirement; information requirements*.

-- Also, 1) An intelligence need considered in the allocation of intelligence resources. Within the Department of Defense, these collection requirements fulfill the essential elements of information and other intelligence needs of a commander, or an agency; or 2) An established intelligence need, validated against the appropriate allocation of intelligence resources (as a requirement) to fulfill the essential elements of information and other intelligence needs of an intelligence consumer. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Collection Requirements Management (CRM). The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either the direct tasking of assets over which the collection manager has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *collection management; collection operations management*.

> CRM is the process by which it is determined **"what"** will be collected and by "which" intelligence discipline. CRM defines "what" intelligence systems must collect and focuses on the requirements of the customer; it is all-source oriented and advocates "what" information is necessary for collection.

Collection Resource. A collection system, platform, or capability that is not assigned or attached to a specific unit or echelon which must be requested and coordinated through the chain of command. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Collection Strategy. An analytical approach used by collection managers to determine which intelligence disciplines can be applied to satisfy information requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Collection Support Brief (CSB). A supplement to a collection requirement on key country topics, technical subjects, and other complex issues. It provides more detailed tutorial information for HUMINT collectors regarding technical developments, organizations, facilities, and personalities associated with the collection topic. (DHE-M 3301.002, Vol II, Collection Operations, 23 Nov 2010)

Collector. A person who acquires information or services from a source. (HDI Lexicon, Apr 2008)

Combat Intelligence. *Within DoD: None – term removed from JP 1-02 per JP 2-0 Joint Intelligence 22 Oct 2013.*

> Previously defined in JP 1-02 as: that knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations.

Combat Support Agency (CSA). A Department of Defense agency so designated by Congress or the Secretary of Defense that supports military combat operations. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Combatant Command (COCOM) A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Combatant Command (command authority). Nontransferable command authority, which cannot be delegated, of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013) Also see *Unified Command Plan*.

Combatant Commander (CCDR). A commander of one of the unified or specified combatant commands established by the President. (JP 1-02) Also see *Unified Command Plan*.

Combating Terrorism (CbT). Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. (JP 1-02 and JP 3-26, Counterterrorism, 13 Nov 2009)

-- Also, within DoD, encompasses all actions taken to oppose terrorism throughout the entire threat spectrum including terrorist use of CBRNE devices. Actions taken include AT, counterterrorism, terrorism consequence management, and intelligence support (collection, analysis, and dissemination of terrorism-related information). (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

Combat Support Agency (CSA). A Department of Defense agency so designated by Congress or the Secretary of Defense that supports military combat operations. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Command and Control (C2). The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Command Counterintelligence Coordinating Authority (CCICA). The senior command representative to conduct and exercise staff coordination authority over CI activities. Develops and implements the Combatant Command's CI strategy and plans, serves as the focal point for CI issues impacting the command, identifies command resource requirements, and coordinates CI support to the command. Formerly known as "CI Staff Officer" [or CISO]. (DoDI 5240.10, CI in the Combatant Commands and Other DoD Components, 5 Oct 2011 with change 1 dated 15 Oct 2013)

Note: this term is approved for inclusion in the next edition of JP 1-02.

-- Also, the Combatant Commander's senior representative for CI. The CCICA serves as the authoritative point of contact for the Combatant Command on CI issues and activities and assists in exercising the command's CI activities. JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Counterintelligence Coordinating Authority (CICA)*.

The CCICA is a CI subject matter expert and the senior CI adviser to the Combatant Command. DoD Instruction 5240.10 directs that the CICCA shall be either a military O5/O6 or civilian equivalent, and shall have CI experience [not further defined].

For additional information see JP 2.01.2, *CI & HUMINT in Joint Operations*, 11 Mar 2011 (para 2a)

Commander's Critical Information Requirement (CCIR). An information requirement identified by the commander as being critical to facilitating timely decision-making. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Committee of Foreign Investment in the United States (CFIUS). An interagency committee that serves the President in overseeing the national security implications of foreign investments. (Department of Treasury website at <http://www.treas.gov/offices/international-affairs/exon-florio/>)

CFIUS has 12 members under the chairmanship of the Secretary of Treasury consisting of: the Secretaries of State, Defense, Commerce, and Homeland Security, the Attorney General, Director OMB, Director of the Office of Science and Technology Policy, Assistant to the President for National Security Affairs, Assistant to the President for Economic Policy, US Trade Representative, and Chairman of the Council of Economic Advisers.

-- Department of Treasury website (cited above)

Originally established in 1975 by EO 11858 mainly to monitor and evaluate the impact of foreign investment in the United States. In 1988, EO 12661 designated CFIUS to receive notices of foreign acquisitions of U.S. companies, to determine whether a particular acquisition has national security issues sufficient to warrant an investigation and to undertake an investigation, if necessary, and to submit a report and recommendation to the President at the conclusion of an investigation.

On 26 July 2077, *the Foreign Investment and National Security Act of 2007* (PL 110-49) was enacted. The act was implemented by EO 13456 and addresses many issues, e.g., Congressional notification requirements; more stringent rules for the review and formal investigation of transactions, especially those involving foreign governments or critical infrastructure assets; requires senior-level involvement in various required certifications and reports, limiting the agencies' delegation authority; established the membership of CFIUS by statute; and created a defined role for the Director of National Intelligence as an ex-officio member who must evaluate the transaction's national security implications.

Also see CRS Report: <http://www.fas.org/sgp/crs/natsec/RL33388.pdf>

Common Operational Picture (COP). A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

-- Also, (Army) A single display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command. (ADRP 6-0, Mission Command, May 2012)

Communications Cover. Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Communications Intelligence (COMINT). Technical information and intelligence derived from foreign communications by other than the intended recipients. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *signals intelligence.*

-- Also, the capture of information, either encrypted or in "plaintext," exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purpose of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, or analysis of the substantive meaning of the communication. COMINT is a sub-discipline of SIGINT. (ODNI, U.S. National Intelligence – An Overview 2011)

> COMINT is a sub-category of signals intelligence that engages in dealing with messages or voice information derived from the interception of foreign communications. It is produced by the collection and processing of foreign communications passed by radio, wire or other electromagnetic means, and by the processing of foreign encrypted communications, however transmitted. Collection comprises search, intercept, and direction finding.
>
> ---
>
> *Communications Intelligence or COMINT: technical and intelligence information derived from foreign communications by other than intended recipients. COMINT activities… those activities that produce COMINT by the collection and processing of foreign communications passed by radio, wire, or other electromagnetic means… and by processing foreign encrypted communications, however transmitted. Collection comprises search, intercept and direct finding. Processing comprises range estimation, transmitter, operator identification, signal analysis, traffic analysis, cryptanalysis, decryption study of plain text, the fusion of these activities and the reporting of results.*
>
> -- NSCID 6, Signals Intelligence, 17 Feb 1972 (redacted copy, complete original version is TOP SECRET) Available at: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/docs/doc05.pdf
>
> ---
>
> *[T]here 'is' something special about communications intelligence… in a nutshell, its special value lies in the fact that this kind of intelligence is generally accurate, reliable, 'authentic,' continuous, and most of all, 'timely'.*
>
> -- NSA, A History of U.S. Communications Security (U) [Vol I], revised July 1973, p.9; originally classified SECRET/NORFORN//COMINT, declassified by NSA 10 Dec 2008)

Communications Security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (JP 1-02 and JP 6-0, Joint Communications Systems, 10 Jun 2010)

-- Also, protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, emissions security, and jamming resistance) to telecommunications and to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to COMSEC information or materials. (DoDD 4640.6 Communications Security Telephone Monitoring and Recording, 26 Jun 1981)

-- Also, measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (DoDD 5100.20, NSA, 26 Jan 2010)

-- Also, a component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material. (CNSS Instruction No, 4009, National IA Glossary, 26 Apr 2010)

Communications Security Monitoring. The act of listening to, copying, or recording transmissions of one's own circuits (or when specially agreed, e.g., in allied exercises, those of friendly forces) to provide material for communications security analysis in order to determine the degree of security being provided to those transmissions. In particular, the purposes include providing a basis for advising commanders on the security risks resulting from their transmissions, improving the security of communications, and planning and conducting manipulative communications deception operations. (previously in JP 1-02)

Community On-Line Intelligence System for End-Users and Managers (COLISEUM). The management system for production requirements and requests for information. CI production. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

-- Also, an analysis requirements management tool used throughout the DIE for tasking and managing requirements for finished intelligence production. (DoDI 3020.51, Intelligence Support to DCIP, 23 Jun 2011)

-- Also, the primary production requirements management system for the Defense Intelligence Analysis Program (DIAP). It supports the DIAP mission to consolidate and gain synergism of DoD intelligence production resources by automating the basic production requirement process defined in the DIAP and its key operational concepts. (DIA DIAP)

-- Also, an analysis requirement management tool used throughout the Defense Intelligence Community to register and track requests for information/analytical requirements, search for existing intelligence, and manage/account for analytical resources. It is a web-based application available through Intelink. (Joint Military Intelligence Training Center, *Fundamentals of COLISEUM 5.0*, Jun 2008)

> *Defense CI Components shall use the CI-approved electronic archiving system to validate, task, and disseminate production requirements for CI analysis. The approved system is the primary method to communicate analysis and production requirements within the DoD CI enterprise. Defense CI Components without access to the approved system may use COLISEUM.*
>
> -- DoDI 5140.18, *CI Analysis & Production*, 17 Nov 2009

Compartmentation. The principle of controlling access to sensitive information so that it is available only to those individuals or organizational components with an official "need-to-know" and only to the extent required for the performance of assigned responsibilities. (National HUMINT Glossary) Also see *Bigot List*.

-- Also, establishment and management of an organization so that information about the personnel, internal organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

-- Also, management of an intelligence service so that information about personnel, organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties. (FBI FCI Terms)

-- Also, the practice of establishing specials channels for handling sensitive intelligence information. The channels are limited to individuals with a specific need for such information and who are therefore given special security clearances in order to have access to it. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, the process of strictly limiting the number of people who are aware of a given intelligence operation…. Only personnel with an absolute "need to know" should be admitted into the compartment. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

> The primary purpose of compartmentation is security, to protect extremely sensitive information from compromise.
>
> _____
>
> ***An intelligence service that is careless about compartmentation pays the price.***
> -- James M. Olson, Former Chief of CIA Counterintelligence
>
> _____
>
> ***Effective compartmentation is fundamental to all secret activity….***
> -- Richard Helms, Former Director CIA (1966-1973)
> (see Richard Helms with William Hood, *A Look Over My Shoulder*, 2003, pp.184-185)
>
> _____
>
> ***[It's]…essential to practice strict compartmentation in counterintelligence investigations.***
> -- Colonel Stuart A. Herrington, US Army (Ret)
> (see *Traitors Among Us: Inside the Spy Catcher's World*,1999, pp.272-273)

Compartmented Intelligence. National intelligence placed in a DNI-approved control system to ensure handling by specifically identified and access approved individuals. (IC Standard 700-1, 4 Apr 2008)

-- Also, national intelligence information under a control system and only available to designated individuals. (National Intelligence: A Consumer's Guide - 2009).

> *Compartmented intelligence became institutionalized during World War II [SIGINT, e.g., ULTRA, MAGIC, etc.]…. Compartmentalizing information is the way they restrict what is known.*
> -- William E. Burrows, *Deep Black* (1986)
>
> _____
>
> *In the secret operations canon it is axiomatic that the probability of leaks escalates exponentially each time a classified document is exposed to another person…. Effective compartmentation is fundamental to all secret activity.*
> -- Richard Helms (Former DCI), *A Look Over My Shoulder* (2003)

Complaint-type Investigation. A counterintelligence investigation in which sabotage, espionage, treason, sedition, subversive activity, or disaffection is suspected. (JP 1-02)

Complex Catastrophe. Any natural or man-made incident, including cyberspace attack, power grid failure, and terrorism, which results in cascading failures of multiple, interdependent, critical, life-sustaining infrastructure sectors and causes extraordinary levels of mass casualties, damage or disruption severely affecting the population, environment, economy, public health, national morale, response efforts, and/or government functions. (Deputy Secretary of Defense Memorandum, 19 February 2013 cited in JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013) Also see *catastrophic event*.

Compromise. A communication or physical transfer of classified information to an unauthorized recipient. (DoDD 5200.1, DoD Information Security Program, 13 Dec 1996)

-- Also, an unauthorized disclosure of classified information. (DoDM 5200.01-Vol 1, DoD Information Security, 24 Feb 2012 and DoD 5220.22-M, NISPOM, 28 Feb 2006)

-- Also, the known or suspected exposure of clandestine personnel, installations, or other assets or of classified information or material, to an unauthorized person. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the disclosure or release of classified information to unauthorized person(s). (IC Standard 700-1, 4 Apr 2008

-- Also, type of incident where information is disclosed to unauthorized individuals or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a known or suspected exposure of clandestine personnel, installations, or other assets, or of classified information or material, to an unauthorized person. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Compromised. A term applied to classified matter, knowledge of which has, in whole or in part, passed to an unauthorized person or persons, or which has been subject to risk of such passing. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, when an operation, asset, or agent is uncovered and cannot remain secret. (CI Centre Glossary)

Compromising Emanations. Unintentional emissions that could disclose information being transmitted, received, or handled by any information-processing equipment. (ICS Glossary) Also see *TEMPEST; TEMPEST Test.*

-- Also, unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled or otherwise processed by information system equipment. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010; also NSTISSI 7002)

Computer Forensics. The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, the scientific, systematic inspection and analysis of digital media and its contents to gather information on the facts and circumstances which may connect an incident to a threat to national security or other computer use that is contrary to security of information systems or may indicative of espionage. The objectives are to perform a structured investigation, maintain the proper chain of evidence, reconstruct the activities of a computer user, and preserve the integrity of the data. (AR 381-20, Army CI Program, 25 May 2010)

Computer Intrusion. *Within DoD: None – term removed from JP 1-02 per JP 3-13, Cyberspace Operations, 5 Feb 2013.*

> Previously defined in JP 1-02 as: an incident of unauthorized access to data or an automated information system.

Computer Intrusion Detection. *Within DoD: None – term removed from JP 1-02 per JP 3-13, Cyberspace Operations, 5 Feb 2013.*

> Previously defined in JP 1-02 as: the process of identifying that a computer intrusion has been attempted, is occurring, or has occurred.

Computer Network. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010 with change 1 dated 16 Oct 2013)

Computer Network Attack (CNA). Operations to manipulate, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (DCID 7/3, Information Operations and IC Related Activities (U), 1 Jul 1999, updated 5 Jun 2003)

> *Within DoD: None – term removed from JP 1-02 per JP 3-13, 27 Nov 2012.*
>
> Defined in the previous edition of JP 3-13, *Information Operations*, dated 13 Feb 2006, as: Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND). Efforts to defend against the computer network operations of others, especially that directed against U.S. and allied computers and networks. (DCID 7/3, Information Operations and IC Related Activities (U), 1 Jul 1999, updated 5 Jun 2003)

> *Within DoD: None – term removed from JP 1-02 per JP 3-13, 27 Nov 2012.*
>
> Previously defined as: Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.

Computer Network Exploitation (CNE). Intelligence collection and enabling operations to gather data from target or adversary automated information systems or networks. (DCID 7/3, Information Operations and IC Related Activities (U), 1 Jul 1999, updated 5 Jun 2003)

> *Within DoD: None – term removed from JP 1-02 per JP 3-13, 27 Nov 2012).*
>
> Previously defined as: Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

Computer Network Operations (CNO). *Within DoD: None – term removed from JP 1-02 per JP 3-13, 27 Nov 2012.*

> Previously defined as: comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

Computer Security (COMUSEC). The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010) Also see *Information Security (INFOSEC); Cybersecurity.*

Computer Trespasser. A person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; see 18 USC 2510 (21)(a). (AR 381-20, Army CI Program, 25 May 2010)

Computer Virus. A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. (US Army TRADOC DCSINT Handbook 1.02, 15 Aug 2007)

-- Also, a computer program that can copy itself and infect a computer without permission or knowledge of the user. (Wikipedia; accessed 2 Oct 2007)

Concealed Monitoring. Targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner. Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted without interruption for a substantial period of time. (DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect US Persons, Dec 1982)

> Concealed monitoring includes, but is not limited to the use of microphones, video cameras, beepers, beacons, transponders, and GPS locators.
>
> Within DoD, if there is a reasonable expectation of privacy, a Procedure 6 is required IAW DoD 5240.1-R. Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,

Concealment. The act of remaining hidden. (DSS Glossary)

Concealment Device (CD). A container designed to hide materials. (HDI Lexicon, April 2008)

-- Also, innocuous object designed or adapted as a container for secreting any selected material or equipment. Also called containers. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, any one of a variety of innocuous devices used to secretly store and transport materials relating to an operation. (CI Centre Glossary)

-- Also, an object modified or fabricated to contain either a device or intelligence materials for the purpose of covert storage, transport, placement within a target, or dead-dropping. (Spycraft)

Concept of Intelligence Operations. Within the Department of Defense, a verbal or graphic statement, in broad outline, of an intelligence directorate's assumptions or intent in regard to intelligence support of an operation or series of operations. (JP 2.0, Joint Intelligence, 22 Oct 2013)

Concept of Operations (CONOPS). A verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Concept Plan (CONPLAN). In the context of joint operation planning level 3 planning detail, an operation plan in an abbreviated format that may require considerable expansion or alteration to convert it into a complete operation plan or operation order. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Conduits. Within military deception, conduits are information or intelligence gateways to the deception target. Examples of conduits include: foreign intelligence and security services, intelligence collection platforms, open-source intelligence, news media—foreign and domestic. (JP 3-13.4, Military Deception, 26 Jan 2012) See *military deception*.

Confidential. Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. (EO 13526, Classified National Security Information, 31 Dec 2009) Also see *security classification.*

Confidential Source. Any individual or organization that provides information to the U.S. Government on matters pertaining to national security and expects, in return, that the information or relationship, or both, will be held in confidence. This definition is not to be confused with "intelligence source" as used in the Human Intelligence Community. (IC Standard 700-1, 4 Apr 2008)

-- Also, any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence. (EO 13526, Classified National Security Information, 31 Dec 2009)

-- Also [within AFOSI], any individual whose identity is being protected, with whom AFOSI establishes a formal managed relationship, and whose AFOSI directed activities result in the gathering of information or testimonial or physical evidence. This does not include those individuals who provide information as a result of their official duties or one time witness to an incident or crime. (AFOSI Manual 71-118, Vol I, Confidential Source Management, 3 Oct 2002)

Confusion Agent. An individual dispatched by his sponsor to confound the intelligence or counterintelligence apparatus of another country rather than to collect and transmit information. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- *Within DoD: None – term removed from JP 1-02 (rescinded 11 Mar 2011).*

> Previously defined in JP 1-02 as: an individual who is dispatched by the sponsor for the primary purpose of confounding the intelligence or counterintelligence apparatus of another country rather than for the purpose of collecting and transmitting information.

Congressional Intelligence Committees. The Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). Also see *SSCI; HPSCI*.

> The 1980 Intelligence Oversight Act charged the SSCI and HPSCI with authorizing the programs of US intelligence agencies and overseeing their activities.
> -- SSCI website at <http://intelligence.senate.gov/> and HPSCI at <http://intelligence.house.gov/>

Consensual Monitoring. Monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication. (Attorney General's Guidelines for Domestic FBI Operations, 29 Sep 2008)

Consolidated Adjudications Facility (CAF). The DoD CAF, under the direction of the Washington Headquarters Services (WHS)—a DoD Field Activity—grants, denies, or revokes eligibility for access to classified information and eligibility for occupancy of sensitive positions, and supports the use of automated and consolidated adjudicative processes to the maximum extent practicable in accordance with DoDD 5220.6 (Defense Industrial Personnel Security Clearance Review Program) and DoD Regulation 5200.2-R (Personnel Security Program).

> DoD established the DoD CAF to consolidate resources and standardize adjudicative processes. On May 3, 2012, the Deputy SECDEF directed a complete consolidation of the functions, resources, and assets of the Army Central Clearance Facility, Department of the Navy CAF, Air Force CAF, Joint Staff CAF, Washington Headquarters (WHS) CAF, Defense Industrial Security Clearance Office (DISCO), and the Defense Office of Hearings and Appeals (DOHA) into a single organization under the authority, direction and control of the Director of Administration and Management. The DoD CAF is located on Fort Meade, MD.

Constraint. In the context of joint operation planning, a requirement placed on the command by a higher command that dictates an action, thus restricting freedom of action. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Contact Report (CR). A report of an operational event; a format providing the officer the ability to document routine aspects of operational activities not otherwise covered by other intelligence or operational reporting. (National HUMINT Glossary)

-- Also, a report used during the conduct of source operations to document the circumstances of, and establish a historical report of the operation. (Army FM 2.22-2, Counterintelligence, Oct 2009)

Contamination. Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Continental United States (CONUS). United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Contingency. A situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect US interests. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Contingency Planning Guidance (CPG). Secretary of Defense written guidance, approved by the President, for the Chairman of the Joint Chiefs of Staff, which focuses the guidance given in the national security strategy and Defense Planning Guidance, and is the principal source document for the Joint Strategic Capabilities Plan. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Contingency Operation. A military operation that is either designated by the Secretary of Defense as a contingency operation or becomes a contingency operation as a matter of law (Title 10, USC §101[a][13] and JP1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Continuity of Government (COG). A coordinated effort within the Federal Government's executive branch to ensure that National Essential Functions continue to be performed during a Catastrophic Emergency. (NSPD 51, National Continuity Program, 9 May 2007)

-- Also, a coordinated effort within the Executive Branch that ensures the continuation of minimum essential functions in any emergency situation, including catastrophic emergencies that impair or threaten day-to-day operations of departments/agencies within the branch. COG activities involve ensuring the continuity of minimum essential functions utilizing infrastructures outside the Washington Metropolitan Area (WMA) and must be capable of implementation with and without warning. (NIP - *FY 2009 Congressional Budget Justification* Book, redacted version)*

* Copy available at: <http://www.fas.org/irp/dni/cbjb-2009.pdf > (accessed 24 Jan 2013.

Continuous Evaluation. Means reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information. (EO 13467, 2 Jul 2008 & DoDI 5200.02, DoD Personnel Sceurity Program, 21 Mar 2014)

All personnel in national security positions shall be subject to continuous evaluation.
-- DoDI 5200.02, DoD Personnel Security Program, 21 Mar 2014 (encl 3, para 6)

Control. [As used in intelligence human source operations], the capacity of a case officer (and his service) to generate, alter, or halt agent behavior by using or indicating his capacity to use physical or psychological means of leverage. (Source: John P. Dimmer, Jr., “Observations on the Double Agent,” *Studies in Intelligence*, vol. 6, no. 1 (Winter 1962), pp 57-72. Declassified, originally classified SECRET)

-- Also, [in intelligence usage,] physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. (JP 1-02)

-- Also, physical or psychological pressure exerted on an agent to ensure that he or she responds to directions from an intelligence agency or service. (Spy Book)

> *"A case officer does not control an agent the way he controls an automobile [or] the way a policeman controls an informer. The intelligence officer who thinks of control in absolutes of black and white does his operations a disservice; the areas of gray predominate."*
> -- John P. Dimmer, Jr., CIA Operations Officer (1962)

Control of Compromising Emanations (aka TEMPEST). TEMPEST Countermeasures are designed to prevent exploitation of compromising emanations by containing them within the equipment or IS [inspectable space] of the facility processing classified information. (AR 381-14, Technical Counterintelligence, 30 Sep 2002)

Controlled Information. 1) Information conveyed to an adversary in a deception operation to evoke desired appreciations; or 2) Information and indicators deliberately conveyed or denied to foreign targets to evoke invalid official estimates that result in foreign official actions advantageous to US interests and objectives. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Ops, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Controlled Source. In counterintelligence use, a person employed by or under the control of an intelligence activity and responding to intelligence tasking. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *source; control; controlled source operation*.

Controlled Source Operation (CSO). A type of offensive counterintelligence operation (OFCO); see DoDI S-5240.09, OFCO, 29 Oct 2008 (*under revision*).

Controlled Technical Services (CTS). The controlled use of technology to enhance counterintelligence and human intelligence activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Ops, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> *CTS include asset communications, validation tools, tailored form factors, and technology or tools used with sources or CI and HUMINT officers to enhance their collection efforts. CTS are a support function of CI and HIMINT and are not independent operations.*
> -- JP 2.01.2, *CI & HUMINT in Joint Operations*, 11 Mar 2011 w/ chg 1 (p. II-15)

Controlled Unclassified Information (CUI). Unclassified information that does not meet the standards for National Security Classification under Executive Order 12958 but is (1) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. (White House Memo, subj: Designation and Sharing of Controlled Unclassified Information, dated 7 May 2008)

> All federal agencies routinely generate, use, store, and share information that, while not appropriate for "classification" under EO 12958 or other authority, nevertheless requires some level of protection from unauthorized access and release. Currently this information is identified by over 100 unique markings and handling regimes, such as "Law Enforcement Sensitive," "FOUO," etc.
>
> An Interagency Task Force reviewed the CUI framework and recommended that the definition of CUI should be simplified to: *All unclassified information for which, pursuant to statute, regulation, or departmental or agency policy, there is a compelling requirement for safeguarding and/or dissemination controls*.
>
> See *Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information*, 25 August 2009, at <http://www.dhs.gov/xlibrary/assets/cui_task_force_rpt.pdf>

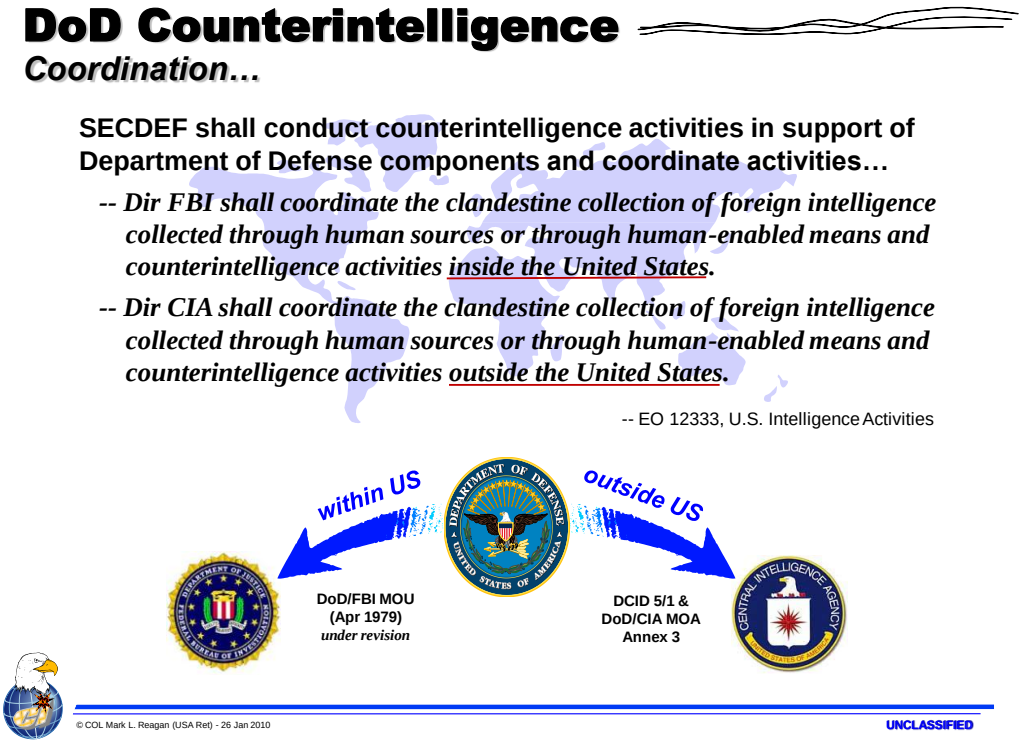
Cooperative Contact. An asset validation term referring to an individual who wittingly responds to tasking in certain areas, but is unwilling to enter into a controlled clandestine relationship. (National HUMINT Glossary)

Cooperative Detainee. A detainee who has established a pattern of answering all questions truthfully and unconditionally and, in fact, answers all questions truthfully and unconditionally. A detainee is not cooperative if the detainee refuses to answer, avoids answering, or falsely answers questions, or if the detainee is intentionally deceptive. A detainee who fluctuates between cooperation and resistance is not cooperative. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

Co-Opted Worker or Co-Optee. A national of a country, but not an officer or employee of that country's intelligence service, who assists that service on a temporary or opportunity basis. (ICS Glossary & CI Community Lexicon)

Coordination. The process of sharing information regarding planned activity, affording potentially affected parties the opportunity to comment, prior to undertaking action. The process of coordination does not infer seeking authorization for action. (DoDD S-5200.37, Management and Execution of Defense HUMINT (U), 9 Feb 2009)

-- Also, the process of sharing operational information and deconflicting activities prior to undertaking a proposed action. Coordination does not require approval or disapproval of the proposed action. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations (U), 9 Jan 2013 w/ chg 1, dated 13 Jun 2013)



EO 12333 directs that the Director FBI coordinates CI activities inside the U.S. and that Director CIA coordinates CI activities outside the U.S. For coordination of DoD CI activities see:

-- **DoD/FBI MOU**: Memorandum of Understanding between the FBI and DoD Governing Information Sharing, Operation Coordination, and Investigative Responsibilities, 2 Aug 2011
+ Annex A - Counterterrorism Information Sharing, 14 Mar 2012
+ Annex B - Counterintelligence Investigative Information Sharing, 9 Dec 2011
+ Annex C - *To be Published* -- Coordinating Counterintelligence Activities
+ Annex TBD - *To be Published* -- Joint Terrorism Task Force (JTTF)

Note: The DoD/FBI MOU (Aug 2011), along with Annexes A, B, and future annexes covering Counterintelligence and Counterterrorism Jurisdiction and Operational Activities, when approved, supersede

the MOA Between the Attorney General and the Secretary of Defense, "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation (U), dated 5 April 1979 and the 1996 supplement thereto, "MOU Regarding Coordination of Counterintelligence Matters."

The DoD/FBI MOU (2011) defines ***Operational Coordination*** as: *"The solicitation of inputs prior to undertaking a proposed action, with the understanding that no such action will be taken until any identified objections have been resolved."*

-- **DoD/CIA MOA:** Annex 3 to the Memorandum of Agreement Between the Central Intelligence Agency and the Department of Defense, "MOA Between CIA and DoD Regarding CI Activities Abroad (U)," 6 Dec 2007, classified SECRET//NOFORN

Note: Annex 3 streamlines the coordination process by assigning primary responsibility for deconfliction to DoD CI field elements and the local Chief of Station/Chief of Base and defines "coordination" as the process of sharing operational information and deconflicting activities prior to undertaking a proposed action. (USD/I Memo, subj: Procedures for Coordination of Counterintelligence Activities Outside the United States, 4 Jan 2008).

For coordination regarding HUMINT activities see ICD 304, *Human Intelligence*, 6 Mar 2008

Coordinating Authority. The commander or individual who has the authority to require consultation between the specific functions or activities involving forces of two or more Services, joint force components, or forces of the same Service or agencies, but does not have the authority to compel agreement. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Counter Surveillance. Measures or actions taken when under verified or suspected surveillance. (DoDI S-5240.15, FPRG, 20 Oct 2010) Also see *countersurveillance*; *surveillance*; *surveillance detection.*

Counter Threat Finance (CTF). Efforts to stop money that funds terrorism, proliferation, narcotics networks, espionage, WMD networks, trafficking in persons, weapons trafficking, precursor chemical smuggling, and other activities that generate revenue through illicit trafficking networks. (*A Guide to Counter Threat Finance Intelligence* by Marilyn B. Peterson, 2009) Also see *threat finance*.

Commander, U.S. Special Operations Command is the DoD CTF lead component for synchronizing DoD CTF activities.

For DoD policy see DoDD 5205.14, *DoD Counter Threat Finance Policy*, 19 Aug 2010 (w/ chg 1 dated 16 Nov 2012).

-- CTF Activities and Capabilities [within DoD]. DoD activities and capabilities, apart from those included under DoD CTFI [Counter Threat Intelligence], to deny, disrupt, destroy, or defeat finance systems and networks that negatively affect U.S. interests in compliance with all existing authorities and procedures. This includes those activities and capabilities undertaken with other Government agencies and/or partner nations. DoD CTF counters financing used to engage in terrorist activities and illicit networks that traffic narcotics, WMDs, improvised explosive devices, other weapons, persons, precursor chemicals, and related activities that support an adversary's ability to negatively affect U.S. interests. (DoDD 5205.14, DoD Counter Threat Finance Policy, 19 Aug 2010)

-- CTF Intelligence (CTFI) [within DoD]. DoD intelligence actions, including those undertaken with other USG agencies and/or coalition partners, that involve the collection, processing, integration, evaluation, analysis, interpretation, production, and dissemination of intelligence products in support of DoD CTF activities and capabilities. (DoDD 5205.14, DoD Counter Threat Finance Policy, 19 Aug 2010)

Counterdeception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. *Counterdeception* does not include the intelligence function of identifying foreign deception operations. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006) Also see *deception*; *military deception*.

-- Also, the detection of deception. (Textbook of Political-Military Counterdeception: Basic Principles & Methods, August 2007)

In principle, it should always be possible to unmask a deception.
-- R.V. Jones, *Intelligence and Deception* (1981)

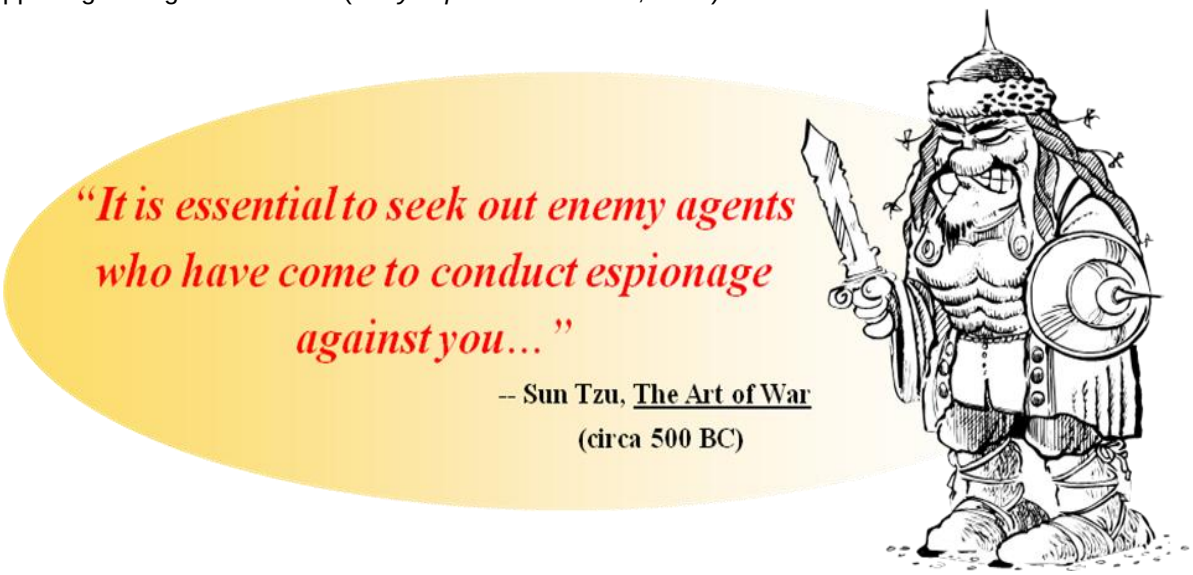
Ideal counterdeception reveals the truth behind the lie, the face beneath the mask, the reality under the camouflage.
-- Barton Whaley, *Textbook of Political-Military Counterdeception: Basic Principles & Methods* (2007)

Counterespionage (CE). That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *counterintelligence*.

-- Also, actions undertaken to investigate specific allegations or circumstances and to acquire information concerning a person or persons involved in the violation of US espionage laws. (National HUMINT Glossary)

-- Also, those aggressive, comprehensive, and coordinated CI defensive and offensive endeavors worldwide designed to detect, identify, assess, and counter, neutralize, penetrate, or exploit the foreign intelligence threat to the Department of Defense (AR 381-20, Army CI Program, 25 May 2010)

-- Also, the act of conducting counterintelligence operations that involve the penetration of an opposing intelligence service. (*Encyclopedia of the CIA*, 2003)



Counterespionage is often touted as the aristocratic sector of secret operations.
-- Harry Rositzke, *CIA's Secret Operations* (1977)

Counterespionage… is a widely misunderstood branch of secret operations…. CE is an offensive operation, a means of obtaining intelligence about the opposition by using—or, more usually, attempting to use—the opposition's operations. CE is a form of secret intelligence operation, but it is a form so esoteric, so complex and important as to stand by itself.
-- Christopher Felix (James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Counterespionage (CE) is the offensive, or aggressive, side of counterintelligence. It involves the identification of a specific adversary and a knowledge of the specific operation he is conducting. Counterespionage personnel must then attempt to counter these operations by infiltrating the hostile service (called penetration) and through various forms of manipulation. Ideally, the thrust of the hostile operation is turned back against the enemy.

-- Senate Report # 94-755 (aka Church Committee Report), Book I, 26 April 1976, p. 166

Counterespionage is like putting a virus into the bloodstream of the enemy.

-- Robin W. Winks, *Cloak and Glown: Scholars in the Secret War* (1987), p. 422

Counterfeit Material. An item that is an unauthorized copy or substitute that has been identified, marked, or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source. (DoDI 4140.67, DoD Counterfeit Prevention Policy, 26 Apr 2013) Also see *suspect counterfeit*.

For general background information see Senate Armed Services Committee Report 112-167, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, 21 May 2012.

Copy at: http://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

Counterguerrilla Operations. Operations and activities conducted by armed forces, paramilitary forces, or nonmilitary agencies against guerrillas. (JP 1-02 and JP 3-24, Counterinsurgency, 22 Nov 2013)

Counterinsurgency (COIN). Comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes. (JP 3-24, Counterinsurgency, 22 Nov 2013)

...the success of a counterinsurgency depends less on defeating the terrorist, guerrilla, or military tactics of the insurgents than on uncovering and undermining the secret network and neutralizing its violent tactics. …The pivotal elements of counterinsurgency are intelligence and counterintelligence.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 165

Counterintelligence (CI). Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities. (Executive Order 12333, as amended 30 July 2008 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *counterespionage*.

Counterintelligence... the core mission simply stated --

Combating Adversarial Intelligence Threats

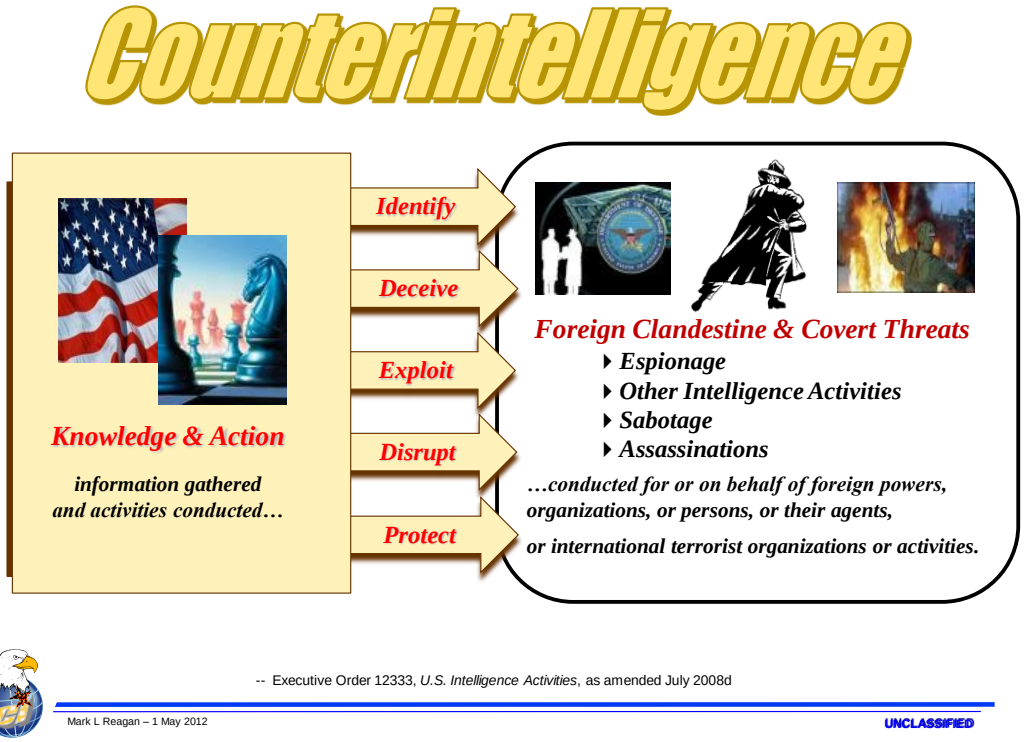
-- COL Mark L. Reagan (USA Ret)

For DoD counterintelligence policy, see DoD Directive O-5240.02, *Counterintelligence*

-- Also, information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (50 USC §401a)

Counterintelligence: [noun] intelligence activities concerned with identifying and countering the threat to security posed by hostile intelligence organizations or by individuals engaged in espionage or sabotage or subversion or terrorism.

hyperdictionary



CI "embraces all activities, human and technical, whether at home or abroad, that are undertaken to identify, assess, neutralize and exploit foreign intelligence threats… counterintelligence is inherently a strategic, national security instrument."

-- Hon. Michelle Van Cleave, NCIX, 18 Nov 2004

-- Also, intelligence activity, with its resultant product, devoted to destroying the effectiveness of inimical foreign intelligence activities and undertaken to protect the security of the nation and its personnel, information, and installations against espionage, sabotage, and subversion. Includes the process of procuring, developing, recording, and disseminating information concerning hostile clandestine activity and of penetrating, manipulating, or repressing individuals, groups, or organizations conducting such activity. (National Security Council Intelligence Directive [NSCID] No. 5, 17 Feb 1972)

-- Also, encompasses actions taken to detect and counteract foreign intelligence activity that adversely affects U.S. national security interest. (WMD Report, 31 Mar 2005)

-- Also, counterintelligence involves all those defensive and offensive activities conducted at home and abroad to protect against traditional and emerging foreign intelligence and international terrorist threats to the national security and to the national defense. (DHE-M 3301.002, Defense HUMINT Enterprise Manual, Vol II: Collection Operations, 23 Nov 2010)

-- Also, counters or neutralizes foreign intelligence and security services (FISS) and international terrorist organizations (ITO) intelligence collection efforts. It does this through collection, CI investigations, operations, analysis, production, and functional and technical services. CI includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies. It is the key intelligence community contributor to the protection of U.S. interests and equities. CI helps identify EEFIs [essential elements of friendly information] by identifying vulnerabilities to threat collection and actions taken to counter collection and operations against U.S. forces. (Army FM 2-0, Intelligence, 23 Mar 2010)

-- Also, the total action taken… by which information is gathered and activities are conducted to protect that agency against espionage, theft of materials, sabotage, assignations, or other intelligence activities conducted by, or on behalf of, hostile foreign governments or other "threatening" foreign organizations (terrorist groups, rogue military units, etc.). (*Encyclopedia of the CIA*, 2003)

-- Also, CI is a discipline and mindset that identifies, analyzes and neutralizes the efforts of others who seek to interfere with our [CIA's] ability to collect and analyze intelligence. (CIA/CIC, circa Mar 2010)

Counterintelligence's core mission can be simply stated as combating adversarial intelligence threats. It is the business of identifying and combating foreign intelligence threats through ***knowledge* and *action*** -- knowledge of and action in countering global adversarial intelligence threats posed by a variety of intelligence entities directed by foreign states, as well as non-state actors, such as transnational terrorist groups.

CI is an integral component of U.S. Intelligence—historically and doctrinally, as well as by statute, executive order and policy. CI is an "intelligence activity" in accordance with the National Security Act of 1947 and EO 12333, which both specifically define "intelligence" as including counterintelligence and foreign intelligence. CI is *intelligence activity* focused on undermining the effectiveness of -- as well as exploiting -- adversary intelligence activities directed against US national security interests. Counterintelligence is one word in the United States -- it is <u>not</u> counter intelligence (two words) or counter-intelligence (hyphenated).

CI is often confused with the foreign intelligence (FI) collection discipline referred to as human intelligence or HUMINT. Although CI and HUMINT are both intelligence activities that operate in the human domain -- ***they are distinctly different…different missions, different authorities, each focused on different content, as well as outcomes.***

The need for CI knowledge and action is much different from the need for FI collection. FI collection values the information above all, whereas CI insists on acting on that information-- *a totally different operational dynamic*.

FI [foreign intelligence] is the task of producing and analyzing otherwise unobtainable intelligence (i.e., "stealing secrets); CI focuses on preventing others from stealing secrets….

-- Andre Le Gallo, "Covert Action: A Vital Option in U.S. National Security Policy, *International Journal of Intelligence and Counterintelligence*, Vol 18 No 2 (Summer 2005), p. 354

[Foreign] intelligence is, in essence, the gathering and analysis of secret information about other nations. Its opposite twin, security, is the protection of one's own secrets. Counterintelligence seeks to protect both of the elements from foreign intelligence activities.

-- *American Counterintelligence and Security for the 21st Century*, The Institute of World Politics

---

Knowledge and <u>Action</u>…

CI *"is a strategic instrument available to states to protect themselves and advance their interests in the struggle for power, wealth, and influence. …But the end product, the mission of counterintelligence, is action—action to protect against foreigners and action to manipulate foreigners in the service of national goals."*

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995)

The primary mission of counterintelligence is to identify, neutralize, and exploit the intelligence or secret infrastructure of others. It is by its very nature both a defensive and offensive tool. … Offensively, counterintelligence helps to advance strategy and policy through knowledge about adversary intelligence and exploit an adversary's vulnerabilities to weaken or manipulate them to advantage. … But only counterintelligence… has the mission and the capabilities to understand, defend against, and exploit an adversary's secret intelligence.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence*, with new introduction by the author (paperback 2001), p. xxviii

---

CI wages "nothing less than a secret war against antagonist intelligence services."
-- U.S. Senate Report 94-755, Book I, 26 April 1976, p. 163

-- Also, CI encompasses information collections, analysis, investigations and operations conducted to identify and neutralize espionage and foreign intelligence activities, the intelligence-related activities of terrorists, and adversary efforts to degrade, manipulate or covertly influence U.S. intelligence, political processes, policy or public opinion. (NIPF [U], Jul 2006)

CI works closely with intelligence, security, infrastructure protections and law enforcement to ensure an integrated approach to the protection of U.S. forces, our intelligence and national assets, U.S. research, development and technology, and the U.S. economy.

CI is composed of both offensive and defensive elements. Offensive CI includes the penetration and deception of adversary groups. Defensive CI involves protecting vital U.S. national security related information from being obtained or manipulated by an adversary's intelligence organizations, activities and operations. This two-pronged approach forms a comprehensive CI strategy that is informed by collection results and feeds more effective CI operations.

Counterintelligence is a universal constant that should be factored in whenever U.S. intelligence or national security capabilities are deployed or when we are targeted by our adversaries. 'Every' U.S. intelligence capability and requirement needs to be protected and 'every' intelligence threat deployed against us should be countered by effective offensive and defensive CI.

-- NIPF - Intelligence Topic Definitions and Information Needs (U), July 2006

-- Also, CI may also be thought of as ***knowledge*** needed for the protection and preservation of the military, economic, and productive strength of the United States, including the security of the Government in domestic and foreign affairs against or from espionage, sabotage, and all other similar clandestine activities designed to weaken or destroy the United States. (Report of the Commission on Government Security - 1957, as cited in Church Committee Report, 26 April 1976, p. 163, footnote 1)

Counterintelligence (CI) is a special form of intelligence activity, separate and distinct from other disciplines. Its purpose is to discover hostile foreign intelligence operations and destroy their effectiveness. This objective involves the protection of the United State Government against infiltration by foreign agents, as well as the control and manipulation of adversary intelligence operations. An effort is made to both discern and decive [sic] the plans and intentions of enemy intelligence services.

Defined more formally, counterintelligence is an intelligence activity dedicated to undermining the effectiveness of hostile intelligence services.

-- Senate Report 94-755 (aka Church Committee Report), 26 April 1976 (p. 163)

Counterintelligence – Senate Report 94-755

Counterintelligence: Activities conducted to destroy the effectiveness of foreign intelligence operations and to protect information against espionage, individuals against subversion, and installations against sabotage. The term also refers to information developed by or used in counterintelligence operations. See counterespionage, countersabotage, and countersubversion [below].

Counterespionage: Those aspects of counterintelligence concerned with aggressive operations against another intelligence service to reduce its effectiveness, or to detect and neutralize foreign espionage. This is done by identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities in order to destroy. Neutralize, exploit, or prevent such espionage activities.

Countersabotage: That aspect of counterintelligence designed to detect, destroy, neutralize, or prevent sabotage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting sabotage activities.

Countersubversion: That part of counterintelligence designed to destroy the effectiveness of subversive activities through the detection, identification, exploitation, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or capable of conducting such activities.

-- Senate Report 94-755 (aka Church Committee Report), Book I – Glossary, 26 April 1976, p. 620.

Counterintelligence Activities. [An alternate term for] one or more of the five functions of counterintelligence: operations, investigations, collection, analysis & production, and functional services. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007; JP 1-02; and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *counterintelligence functions.*

Counterintelligence Activities in Cyberspace. CI activities in cyberspace include those forensics examinations of DoD affiliated information systems and other approved virtual or on-line activities to identify, disrupt, neutralize, penetrate, or exploit FIEs [Foreign Intelligence Entities]. DoD CI activities in cyberspace do not include Offensive Computer Operations as defined in NSPD-38 or the collection and processing of technical and intelligence information derived from foreign communications by other than an intended recipient. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010 with chg 1)

For additional information see --

1) JP 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations (U)*, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011 (para 3f, p. III-17, "CI Activities in Cyberspace").
2) *The DoD Strategy for Counterintelligence in Cyberspace* (28 Aug 2009).
3) *The United States Government-Wide Cyber Counterintelligence Plan - 2008* (classified).

Cyberspace is a Venue

Counterintelligence Analysis. The methodical process of examining and evaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of foreign powers, international terrorists, and other entities. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 20 Dec 2010) Also see *counterintelligence production*.

CI Function: CI Analysis & Production…

Analysis & Production

Assimilating, evaluating, interpreting, and disseminating information of CI relevancy – *a critical enabler providing insights into clandestine & covert threats*

Astute analysis is [a] critical enabler… Strategic analysis allows DoD CI to understand today's risk environment. …[it] allows the Department to learn and use an adversary's pressure points to influence its actions.

-- DoD Counterintelligence Strategy - FY 2004

"It is not enough, of course, simply to collect information. Thoughtful analysis is vital to sound decisionmaking."

-- President Ronald Reagan (4 Dec 1981)

"Analysis – Collecting information is one thing. Making sense of it and using it to frustrate and exploit foreign services is another."

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 81

Counterintelligence Analysis – the Queen of the Counterintelligence Chessboard

Intelligence Community analytical tradecraft standards established in ICD 203, *Analytical Standards*, serve to guide the writing of intelligence analysis and apply to counterintelligence analysis.

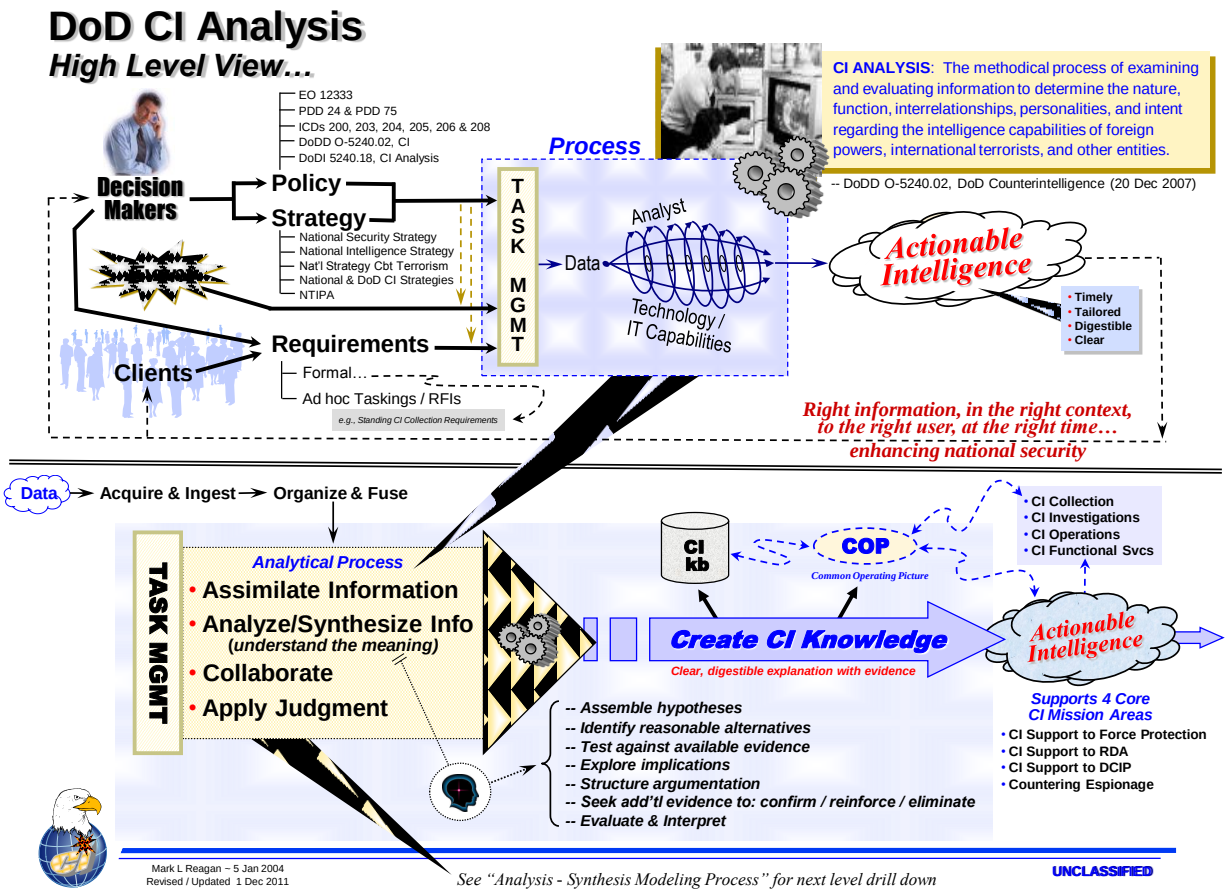
"Effective counterintelligence analysis is a tall order. Good macro-analysis is not synonymous with journalism, or narrative description, or even investigations. Macro-counterintelligence analysis is meant to be explanatory, systematic, empirical, cumulative, reliable, comprehensive, integrated, and policy relevant. Analysis should discover and connect the seemingly disconnected, illuminate hidden relationships, identify unseen linkages, reveal patterns of activity and behavior heretofore unobserved. Good counterintelligence analysis should provide reliable knowledge and authoritative judgments to policymakers and operators. The product of counterintelligence and security analysis is understanding and explanation, and if possible, to answer the questions how and why."

-- Kenneth E, deGraffenreid, *Countering Hostile Intelligence Activities as a Strategic Threat* (1989)

CI analysis drives collections, enhances CI investigative activity, shapes operations, enables mission execution, and informs decision makers

- Also, the process of examining and evaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of state and non-state actors and other entities and activities of CI interest. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, a step in the process of producing timely, accurate, and relevant assessments regarding the actual and potential foreign intelligence and international terrorist threat to Department of Defense in which the collected information is subjected to review to identify significant facts for subsequent interpretation. (AR 381-20, Army CI Program, 25 May 2010)



Counterintelligence Analysis – the Queen of the Counterintelligence Chessboard

Analysis – Collecting information is one thing.
Making sense of it and using it to frustrate and exploit foreign services is another.
-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 81

CI Analysis… look at the details and see the passion

I can't possibly overstate the importance of good research. Everyone goes through life dropping crumbs. If you can recognize the crumbs, you can trace a path all the way back from your death certificate to the dinner and a movie that resulted in you in the first place. But research is an art, not a science, because anyone who knows what they're doing can find the crumbs, the wheres, whats, and whos. The art is in the whys: the ability to read between the crumbs, not to mix metaphors. For every event, there is a cause and effect. For every crime, a motive. And for every motive, a passion. The art of research is the ability to look at the details, and see the passion.

-- Daryl Zero, *The Zero Effect* (1998)

Analysis… often raises more questions than it answers. …remember of the basic principle: All action, whether human or physical, disturbs the environment is some way. Find that disturbance and you have a key to the action.

For analysis to play its proper CI role it must be able to survey all of the intelligence data available to one's own government, and it must be able to somehow direct the rest of CI.

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), pp. 330-331

For a "snap shot" of CI analysis see Irvin D. Sugg, Jr., *Basic Counterintelligence Analysis in a Nutshell: Quick Reference Guide*, Joint Counterintelligence Training Academy (JCITA), n.d. Copy available at: <http://www.ntis.gov/search/product.aspx?ABBR=PB2010105593>

Counterintelligence Analysis and Production Council (CIAPC). The principal forum for coordinating CI analysis and production requirements, discussing CI analysis and production priorities within the enterprise, and discussing other IC issues. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

CIAPC Membership: The Director, Defense CI & HUMINT Center (DCHC), appoints the Chair. Core membership includes the DCHC analysis and production enterprise manager and the managers of the Defense CI Component analysis and production elements. The Chair may expand membership, to include other full-time or permanent part-time Federal employees.

Counterintelligence Analysis and Production Element. The element within a Defense CI Component that performs CI analysis in any form; produces a CI analytical product in any of the categories of CI analysis; or responds to requests for CI analysis from an internal organization and/or from organizations external to the Defense CI Component. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Counterintelligence Analysis Centers. See *ACIC, ICON, MTAC* for DoD CI Analysis Centers. .

Counterintelligence Analysis Report. A document produced by a CI analysis and production element stating the results of analysis regarding a relevant CI topic, event, situation, or development, and containing the characteristics outlined in [DoDI 5240.18] Appendix 2 to Enclosure 3. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Counterintelligence Analytical Product. Any document that contains the work of, is supported by, collaborated on, or produced by a CI analyst at any echelon within a Defense CI Component. It may or may not include CI production. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Objectives of CI analytical products are to: 1) Outline, describe, or illustrate the threat posed by an Foreign Intelligence Entity (FIE) to installations, personnel, assets, operations, or resources; 2) Identify opportunities to conduct offensive CI operations (OFCO) targeting a FIE; and 3) Identify CI investigative opportunities.

CI analytical products seek to satisfy a core CI production requirement to identify people, organizations, locations, activities, and resources associated with a FIE or a target of a FIE.

Within DoD, CI analytical products are categorized based on the purpose of the product, analytical effort, the production timeline, and other distinguishing characteristics. The primary categories of CI analytical products are: 1) Assessment, 2) Analysis Report, 3) Threat Advisory, and 4) Functional Support. Associated analytical products with CI collections, investigations and operations are summarized below.

-- ***Analytical products associated with CI collections are:***

Collection Support Brief. Provides near-comprehensive background detail on a collection issue to guide and enhance collection efforts. (DoDI 5240.18, 17 Nov 2009)

Collection Source Evaluation. An evaluation of a source to determine if the information provided is valuable and credible and to ascertain the reliability and veracity of the source. (DoDI 5240.18, 17 Nov 2009)

Collection Emphasis. Supplements a standing collection requirement and identifies areas of emphasis or information gaps to the CI collector. (DoDI 5240.18, 17 Nov 2009)

Source-Directed Requirement. Established by a CI analysts based on knowledge of a source's access and placement to necessary information. (DoDI 5240.18, 17 Nov 2009)

IIR Evaluation. An analyst's evaluation of how well an IIR satisfied the intelligence requirement for which it was collected. (DoDI 5240.18, 17 Nov 2009)

-- Analytical products associated with CI investigations are:

Investigative Analysis Report. An evaluation of all available information obtained during a CI inquiry to determine if an investigation is warranted; an evaluation of an on-going CI investigation to develop leads, identify trends, patterns, or anomalies in furtherance of the investigative effort; or produced at the conclusion of a CI investigation to identify previously unknown methods of operation, describe lessons learned, and to support damage assessments when initiated. (DoDI 5240.18, 17 Nov 2009)

Investigative Source Evaluation. An evaluation of a source to determine if the information provided is valuable and credible, and to ascertain the reliability and veracity of the source. (DoDI 5240.18, 17 Nov 2009)

Investigative Support Package. An evaluation of all available information pertaining to an unknown subject CI inquiry or investigation in an effort to identify a person, place, or thing of CI interest based on analysis of the information. (DoDI 5240.18, 17 Nov 2009)

-- Analytical products associated with CI operations are:

Operational Analysis Report. An evaluation of information from a variety of sources to determine if favorable conditions are present for initiation of a CI operation and the report may offer suggestions as to the type of asset and/or the access and placement required to meet the foreign essential elements of information requirements. (DoDI 5240.18, 17 Nov 2009)

Operational Asset Evaluation. Evaluates an asset's reliability and veracity in a CI operation. (DoDI 5240.18, 17 Nov 2009)

Operational Support Package. Comprehensive analysis of all available intelligence on a target of interest to a Defense CI Component or determined to be of interest to DoD CI. It details the significance of the target, relates it to strategic objectives, identifies desired effects, and suggests methods of engagement to achieve desired results. (DoDI 5240.18, 17 Nov 2009)

Counterintelligence Assessment. A document produced by a CI analysis and production element stating the in-depth and comprehensive results of analysis regarding a relevant CI topic, event, situation, or development, and contains the characteristics outlined in [DoDI 5140.18] Appendix 2 to Enclosure 3. (DoDI 5140.18, CI Analysis & Production, 17 Nov 2009)

-- Also, an analysis of the actual or potential foreign intelligence and international terrorist threat to DoD, with the objective of protecting personnel, plans, information. Research and technology, critical infrastructure, and other national security interests. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, a DoD Component's comprehensive analysis or study of a relevant CI topic, event, situation, issue, or development. When conducted in support of an RDA program with CPI [Critical Program Information], the assessment describes the threat a foreign entity (person, representative, corporation, government, military, commercial, etc.) represents to the CPI/system assessed. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008, w/ change 1 dated 28 Dec 2010)

> The CI assessment is multidisciplinary as it includes an analysis of the diverse foreign collection modalities available, the relative effectiveness of each, and capability of the foreign entity to collect information about research efforts, the technology, and/or system under development. The assessment may include the impact to the DoD if the technology is compromised and be complimentary to, integrated with, or independent of the TTRA provided by the Defense Intelligence Community.
>
> -- DoDI 5200.39, *CPI Protection within DoD*, 16 Jul 2008, w/ chg 1 dated 28 Dec 2010

Counterintelligence Awareness. An individual's level of comprehension as to the FIE [foreign intelligence entity] threat, methods, indicators, and reporting requirements. (DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 2013)

-- Also, a state of being aware of the sensitivity of classified information one possesses, collaterally aware of the many modes of operation of hostile intelligence persons and others whose interests are inimical to the United States while being able to recognize attempts to compromise one's information, and the actions one should take, when one suspects he has been approached, to impart the necessary facts to trained counterintelligence personnel. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

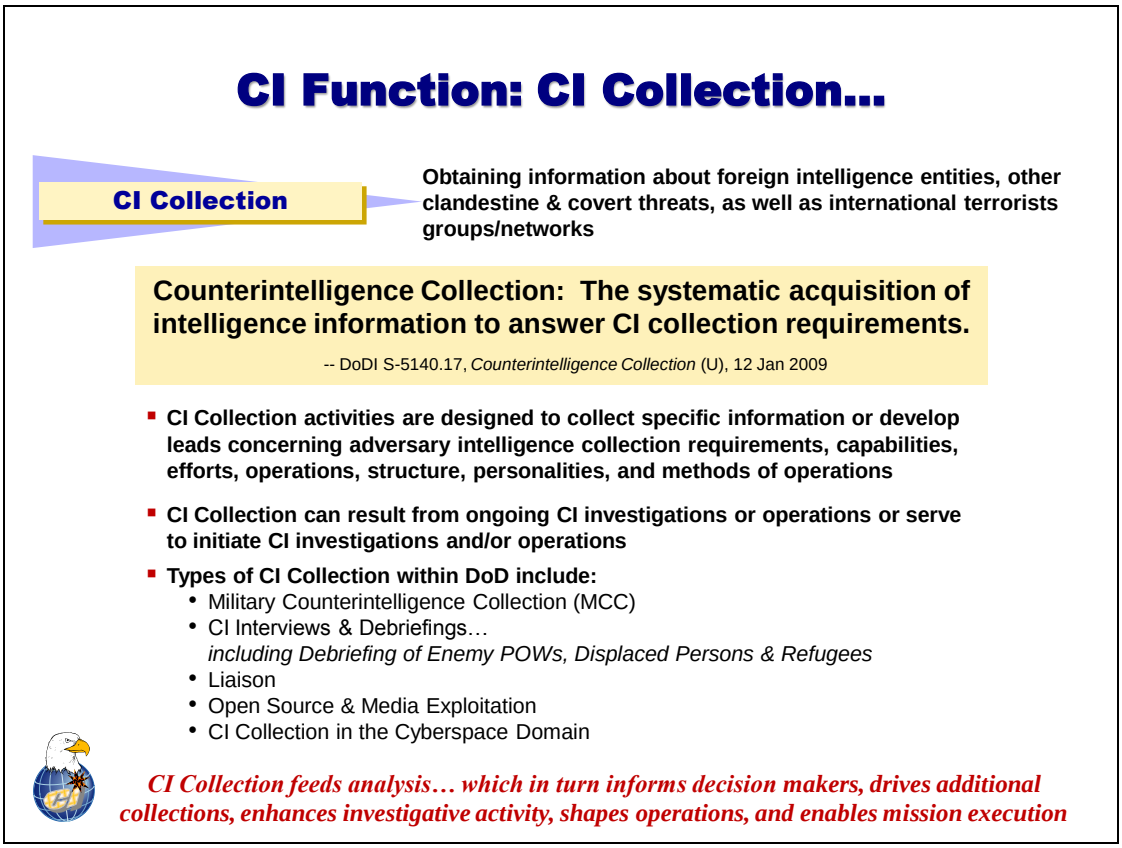
Counterintelligence Awareness Products. A DoD Component's analysis of a CI topic, event, situation, issue, or development. These products differ from an assessment in that they are often time sensitive, are published as needed or annually, and normally do not require extensive research to produce. Products of this nature ensure a consistent flow of appropriately classified or categorized threat information is available to the community to increase awareness and action as appropriate. The Defense Security Service *"Technology Collection Trends in Defense Industry"* and the Office of the National Counterintelligence Executive *"Annual Report to Congress on Foreign Economic Espionage"* are examples of products meeting this objective. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008, w/ chg 1 dated 28 Dec 2010)

Counterintelligence Campaign (CI Campaign). See *DoD Counterintelligence Campaign*.

Counterintelligence Collection. The systematic acquisition of intelligence information to answer CI collection requirements. (DoDI S-5140.17, CI Collection Activities, 14 Mar 2014) Also see *Counterintelligence Collection Activities*; *Military Counterintelligence Collection*.

> See "Counterintelligence Collection Methods" addressed in Appendix C, Joint Publication 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations (U),* 16 Mar 2011 w/ chg 1 dated 26 Aug 2011.
>
> Director DIA is the Defense CI Collection Manager.

-- Also, the systematic acquisition of information (through investigations, operations, or liaison) concerning espionage, sabotage, terrorism, other intelligence activities or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons that are directed against or threaten Department of Defense interests. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations (U),16 Mar 2011 w/ chg 1 dated 26 Aug 2011)



See DoDI S-5240.17, (U) *CI Collection Activities,* 14 Mar 2014 for DoD policy and additional information.

Counterintelligence Collection Activities (CCA): CI collection activities to include military CI collection, CI questioning of EPWs and detainees, CI debriefings, liaison, open source and media exploitation, and CI collection in cyberspace. (DoDI S-5140.17, CI Collection Activities, 14 Mar 2014) Also see *Counterintelligence Collection; Military Counterintelligence Collection*.

Counterintelligence Collection in Cyberspace. The use of cyber means as the primary tradecraft methodology to engage in targeting and collecting cyber based FIE [Foreign Intelligence Entity] activities. CI Collection in cyberspace may include the use of authorized non-attributable Internet connections, development and use of national cyber personas, use of authorized obfuscation techniques, as well as appropriate digital tradecraft and cover. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010 with change 1 dated 16 Oct 2013)

Counterintelligence Collection Operations. Intelligence collection operations that use human sources and CI resources to answer validated CI requirements. CI collection operations are deliberate, planned activities primarily using human sources to satisfy one or more validated CI information requirements. (DoD CI Collection Integrated Working Group Handbook 1-02, 8 Aug 2006)

Counterintelligence Controlled Source Operation (CI CSO). A type of offensive counterintelligence operation (OFCO); see DoDI S-5240.09, OFCO, 29 Oct 2008 for detailed information.

Counterintelligence Coordinating Authority (CICA). A designated CI representative in country, the CICA coordinates, deconflicts, and/or synchronizes all joint CI issues in the country with the Service CI elements assigned to or operating within that country, and with the US embassy or consulate. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Command Counterintelligence Coordinating Authority (CCICA).*

Counterintelligence Cyber Investigation. An investigation using techniques that identify and interdict the misuse of DoD information systems by a trusted insider or an external intruder. These investigations may involve computer intrusions, exceeding authorized network access, denial of service attacks, or the introduction of a virus or a malicious code. (Previously defined in DoDI 5240.19, CI Support to the Defense Critical Infrastructure Program, 27 Aug 2007 with change 1 dated 28 Dec 2010)

Counterintelligence Effects-Based Operations (CI EBO). As applied to counterintelligence, effects-based operations is a process for obtaining a desired strategic outcome of effect on adversary intelligence activities through the synergistic, multiplicative, and cumulative application of the full range of CI capabilities at the tactical, operational and strategic levels, to include leveraging non-CI capabilities. Successful CI effects-based operations rest on an explicit linking of CI actions to desired strategic outcomes. CI effects-based operations proactively shape the battlespace in our war against adversary intelligence activities and terrorist networks through the robust execution of *full-spectrum* CI capabilities across the entire spectrum of conflict in an orchestrated and synchronized manner to achieve national, departmental, and combatant commander objectives. (COL Mark L. Reagan, USA Ret)

Counterintelligence Enhancement Act of 2002. The act facilitates enhancement of US counterintelligence activities by: (1) enabling the counterintelligence community of the US Government to fulfill better its mission of identifying, assessing, prioritizing, and countering the intelligence threats to the United States; (2) ensuring that the counterintelligence community of the US Government acts in an efficient and effective manner; and (3) providing for the integration of all the US CI activities. The act also established the National Counterintelligence Executive (NCIX), the National CI Policy Board and the Office of the National CI Executive (ONCIX) which replaced the National Counterintelligence Center (NACIC). (§§ 901-904 PL 107-306)

> The act is available at <http://www.ncix.gov/publications/law/index.html>

Counterintelligence Equity. Facts or circumstances connecting an incident, event, or person to an actual or potential intelligence or terrorist threat to Army or DoD personnel, programs, plans, operations, installations, systems, technology, or security. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence Flags. Indicators that should alert a source handler to suspicious action that may bring the source's bona fides into question. (DoDI S-3325.07, Guidance for the Conduct of DoD Human Source Validation (U), 22 Jun 2009.)

> "CI Flags" are different from reportable CI indicators and behaviors as addressed in DoD Directive 5240.06,CI Awareness and Reporting (CAIR, 17 May 2011 w/ chg 1 dated 30 May 2013; see *potential espionage indicators*.

Counterintelligence Force Protection Detachment. See Force Protection Detachment (FPD).

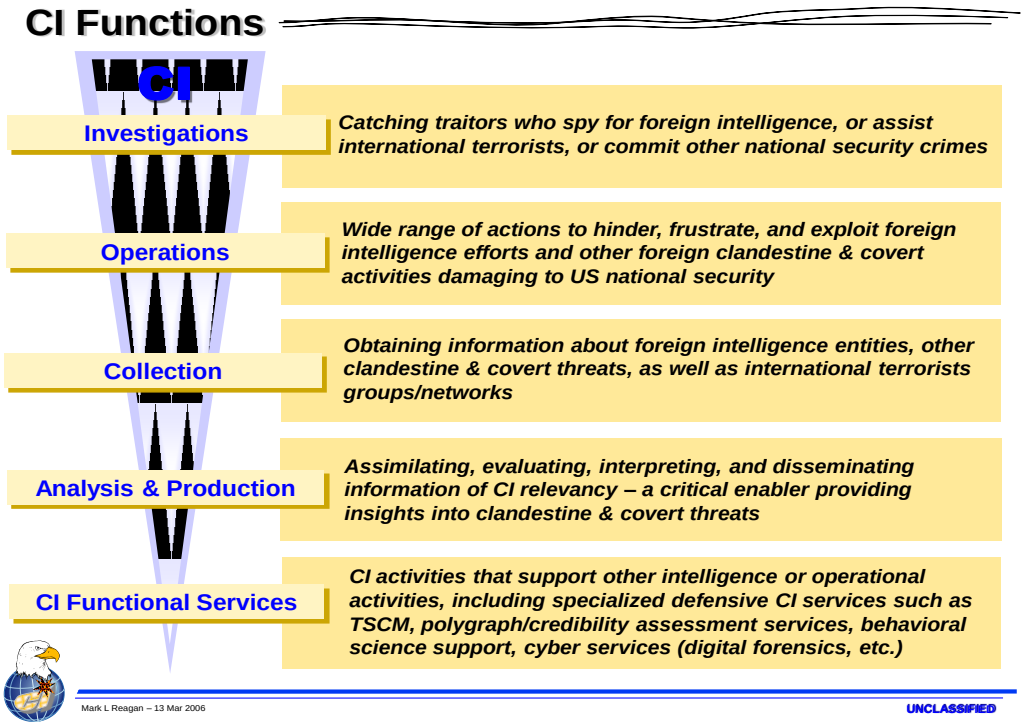
Counterintelligence Force Protection Source Operations (CFSO). Overt source collection activities of an expedient nature intended to identify threats to the command in support of the commander's force protection mission. (Marine Corps Doctrinal Publication 2-6 [previously 2-14], Counterintelligence, 5 Sep 2000, p. 2-3)

Counterintelligence Functions. The five functions of counterintelligence: operations, investigations, collection, analysis & production, and functional services. (JP 1-02) Also see *CI Activities.*

CI functions are interrelated, mutually supporting, and can be derived from one another.

Functions vs. Missions: *"Functions differ from CI missions in that missions focus on end results to be accomplished, rather than on the means for accomplishment. "*
-- Mission Area Analysis of DoD Counterintelligence, Institute for Defense Analyses, May 1999, p.7

CI functions are useful terms of reference to describe "what is done"
CI missions focus on the "end result" to be accomplished



Counterintelligence Functional Services (CIFS). CI activities that support other intelligence or DoD operations by providing specialized defensive CI services to identify and counter the intelligence capabilities and activities of terrorists, foreign powers, and other entities directed against US national security. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 30 Dec 2010)

-- Also, activities engaged in by personnel trained in CI and conducted to detect espionage, sabotage, terrorism, or related intelligence activities of an FIE directed against the DoD, and that enable one or more of the CI functions (investigations, collection, operations, or analysis and production). (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

-- Also, CI activities that support other intelligence or DoD operational activities, providing specialized defensive CI services to identify and counter terrorism, espionage, sabotage, and related activities of Foreign Intelligence Entities. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

For DoD Policy see DoD Instruction, *Counterintelligence Functional Services (CIFS),* 27 Aug 2012.

For more in-depth information regarding CI functional services see Department of Defense, CI Functional Services Integrated Working Group Handbook, *Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Functional Services*, 19 Feb 2009. This handbook further defines CI functional services as: those activities that are not unique to other CI functions and that support other CI functions and missions; specialized services, which are not inherently CI but support the CI mission and functions.

Within DoD, CI functional services consist of basic CI activities (including espionage detection and CI support to military operations) and specialized services (e.g., polygraph/credibility assessments, TSCM, behavioral science support, cyber services).

Counterintelligence Functional Support Plan (CI FSP). Director Defense CI and HUMINT Center is responsible for preparation of CI FSPs as part of the Intelligence Planning process (CJCSM 3314.01). Format for CI FSPS is provided at enclosure E to CJCSM 3314.01, Intelligence Planning, 28 Feb 2008.

Counterintelligence Inquiry. An examination of the facts surrounding an incident of potential CI interest, to determine if a CI investigation is necessary. (DoDD 5240.02, CI, 20 Dec 2007 with change 1 dated 30 Dec 2010) Also see *counterintelligence investigation*.

For information regarding CI inquiries within DoD see: 1) DoDI O-5240.21, CI Inquires, 14 May 2009, which provides DoD policy and outlines the procedures for initiating and conducting CI Inquires; and 2) DoD, CI Functional Services Integrated Working Group Handbook, *Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Functional Services (U)*, 19 Feb 2009.

According to the DoD handbook on CI functional services, *"[w]ithin DoD a CI inquiry does not require "investigative authority" as it is not a CI investigation."* A **CI inquiry** is designed to gather information, identify and/or verify the credibility of potential sources and subjects(s) of CI interest, and to recommend appropriate action if the inquiry does not resolve the matter. The goal is to establish or refute a **reasonable belief** that a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged is spying, or committing espionage, sabotage, or other national security crimes (e.g., treason), or international terrorist activities. Establishment of *reasonable belief* provides the basis for opening a CI investigation. Once a *reasonable belief* is established the matter must be referred to the appropriate Military Department CI organization and/or the FBI [see Section 811 referral]. Refer to the definition of *reasonable belief*.

The DoD handbook stresses that *"[w]ithin DoD, only Military Department CI organizations have CI investigative authority and may, accordingly, use the intrusive techniques provided for in Procedures 5 through 13 of DoD 5240.1-R…. It is absolutely vital that CI personnel obtain guidance from their own organization's legal counsel as to what specific investigative techniques and activities are allowable in their organization and approval from their organization's leadership to employ those techniques in the course of CI activity."*

A CI Inquiry is not a CI investigation, but it can provide the basis for a CI investigation.

Counterintelligence Insider Threat (CI InT). A person who uses their authorized access to DoD facilities, systems, equipment, information or infrastructure to damage, disrupt operations, compromise DoD information or commit espionage on behalf of an FIE [Foreign Intelligence Entity]. (DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 2013)

-- Also, a person, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of an FIE [foreign intelligence entity]. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 with change 1 dated 15 Oct 2013) Also see *insider, insider threat*.

CI is one critical component in countering "insider threats," the other components are security, information assurance (IA), law enforcement, and antiterrorism/force protection.

CI Insider Threat Program Elements:
-- CI Analysis of Information Technology Auditing & Monitoring
-- CI Insider Threat Awareness & Training
-- Foreign Travel and Contact Reporting and Analysis
-- Polygraph & Credibility Assessment
-- Personnel Security, Evaluation, Analysis, and Reporting
-- Security Incident Reporting & Evaluation
-- Proactive CI Initiatives

For additional information see DoDI 5240.26, *Countering Espionage, International Terrorism, and Counterintelligence Insider Threat*, 4 May 2012

Insider threat detection should be a comprehensive US Government (USG) effort dedicated to countering potential threats and mitigating damage that could result from unauthorized disclosure of information, espionage, terrorism, and other national security crimes.
-- U.S. Government Threat Detection Guide - 2011

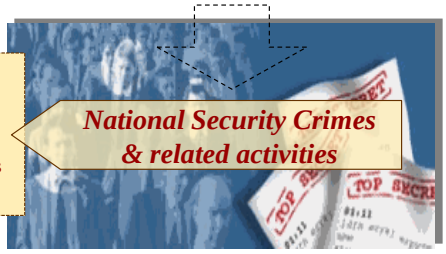
Counterintelligence Investigation. Formal investigative activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities, and to determine actions required to neutralize such acts. (DoDI 5240.04, CI Investigations, 4 Feb 2009 with change 1 dated 15 Oct 2013) Also see *counterintelligence inquiry, investigation.*

CI Function: *CI Investigations…*

Investigations

Investigating national security threats… includes catching traitors who spy for foreign intelligence, or assist international terrorists, or commit other national security crimes

- Espionage - Spying - Treason - Sedition - Subversion
- Aiding the Enemy by providing intelligence to the enemy
- International Terrorist Activities or material support to
- Unreported contact with foreign intelligence entities or ITOs
- Unauthorized disclosure of classified information/material



FBI
- **Assessments**
- **Preliminary Investigation**
- **Full Investigation**

-- FBI Domestic Investigations & Operations Guide, 15 Oct 2011

DoD
- **CI Inquiry**
- **CI Investigation**

-- DoDI O-5240.21, CI Inquires, 14 May 2009
-- DoDI 5240.04, CI Investigations, 2 Feb 2009

Army
- **Limited CI Assessments**
- **Preliminary CI Investigation**
- **Full Field CI Investigation**

-- AR 381-20, Army CI Program (U), 25 May 2010

By far the hardest part of any CI case is to realize that the case exists—that some person, some thing, has the enemy's hidden hand in it.
-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 326

CI investigations are undertaken to determine whether a particular person is acting for or on behalf of a foreign power or international terrorist organization or whether an event is related to foreign intelligence or international terrorism.

CI investigations focus on resolving allegations of known or suspected acts that may constitute national security crimes under U.S. law or Uniform Code of Military Justice.

The agencies responsible for the investigation and ultimate referral for prosecution of violations of US espionage law (primarily Sections 792-798, Chap 37 of Title 18) are the FBI and the CI components of the military services that participate in the DoD Foreign CI Program (FCIP).

DoD Policy: *The Secretaries of the Military Departments exercise authority, direction, and control over CI investigations and attendant matters for their respective personnel.*

-- Para 5.10.3, DoDD O-5240.02, Counterintelligence, 20 Dec 2007 w/ chg 1 dated 30 Dec 2010

CI investigations are conducted following appropriate legal standards and in a manner which will not jeopardize the potential for prosecution.

Within DoD, DIA's Office of Counterintelligence (DXC) exercises administrative and management oversight of all DoD national security investigations. All significant CI activities must be reported promptly to the DXC IAW DoDD O-5240.02 (see encl 4 for significant CI reporting criteria).

-- Also, inquiries and other activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power for espionage, treason, spying, sedition, subversion, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 30 Dec 2010)

-- Also, includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for the purposes of conducting espionage and other intelligence activities, sabotage, assassinations, treason, international terrorist activities, and actions to neutralize such acts. (DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,* 7 Dec 1982)

-- Also, an official, systematic search for facts to determine whether a person(s) is engaged in activities that may be injurious to U.S. national security or advantageous to a foreign power. (JP 1-02 and JP 2.01.2, CI & HUMINT in Joint Operations,11 Mar 2011 w/ chg 1, dated 26 Aug 2011)

-- Also, the systematic collection of information regarding a person or group which is, or may be, engaged in espionage or other clandestine intelligence activity, sabotage, or international terrorist activities conducted for, or on behalf of, foreign powers, organizations, or persons. (CI Community Lexicon)

The first priority for all CI investigative situations is to assess for possible exploitation.

-- Army FM 2-22.2, *Counterintelligence*, October 2009

CI investigations focus on resolving allegations of known or suspected acts that may constitute national security crimes under U.S. law or Uniform Code of Military Justice (UCMJ). Investigative actions must preserve the potential for legal action and when appropriate exploit threatening intelligence collection directed against DoD. In simple terms, CI investigations seek to *identify spies and put them out of business.* CI investigations are about discovering the facts and conveying them to decision makers, while maintaining a full range of options, including apprehension, prosecution, expulsion, as well as exploitation.

"*The ultimate objective of… [DoD] CI investigations… is to detect, identify, exploit and neutralize the intelligence collection threat posed by foreign intelligence and security services and foreign terrorist groups. […] The most significant objectives of CI investigations are to minimize or prevent the loss of sensitive and classified defense information to foreign governments, and to prevent, preempt, or disrupt foreign terrorist attacks against… DoD interests*"

-- 902d MI Group Investigations Handbook, Jun 2012, p.19

"*CI investigation is an art form carried out by experts. It is not science, and throwing money and unqualified personnel or helpers at such s problem does not guarantee or even improve the chances of success. In many cases, quite the opposite results is achieved—analytical chaos with no resolution.*"

-- Sandra Grimes and Jeanne Vertefeuille, *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed*, 2012, p. 189

Credentialed CI Special Agents use specialized investigative techniques and methodologies to gather intelligence (facts/evidence) about known and/or suspected acts that may constitute National Security crimes, e.g., espionage, treason, spying, etc. All investigative activities are conducted within guidelines established in applicable departmental policy/directives, Attorney General Guidelines, and U.S. federal statutes.

DoD CI investigations are conducted in a manner to "preserve" the potential for prosecution of all culpable parties identified. Although all national security investigations are conducted in a manner to preserve the potential for prosecution, this purpose is secondary to the CI mission of detecting, identifying, fully determining the extent of, and neutralizing/disrupting national security threats to the DoD and U.S. national security.

CI investigative results also contribute to the identification and elimination of security vulnerabilities; identification of current foreign intelligence tradecraft, agent handlers/operatives and their support networks; assessment of damage to DoD and National Security; and improvement of the overall DoD security posture, as well as assisting decision makers in risk management decisions.

DoD CI investigations are conducted in accordance with DoDI 5240.04, *CI Investigations*. The DoD agencies responsible for CI investigations and the ultimate referral for prosecution of violations of US espionage law (primarily §§ 792-798, Chap 37, Title 18 USC) are the CI components of the military departments, i.e., NCIS, AFOSI, and Army CI.

See Stuart A. Herrington, *Traitors among Us: Inside the Spy Catcher's World* (1999), for an excellent unclassified overview of two CI investigations concerning Clyde Conrad and James Hall.

Other interesting reads on CI investigative cases include –

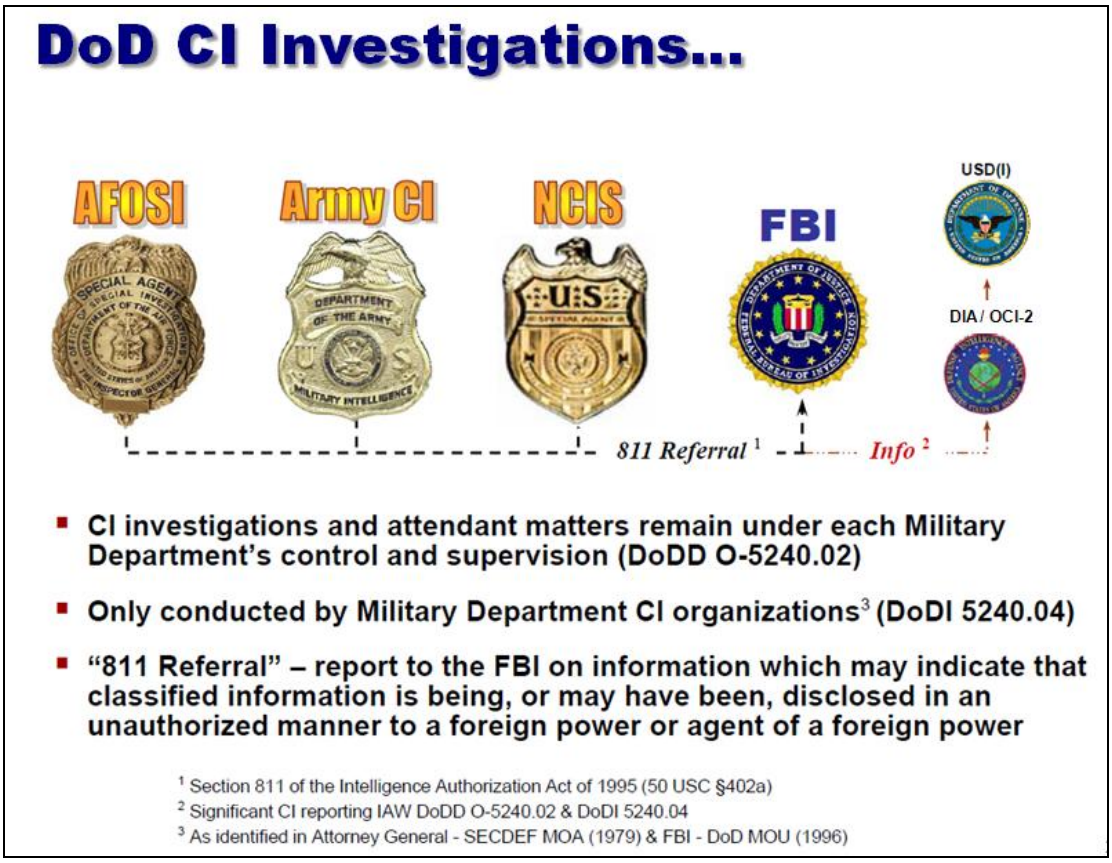
-- Scott W. Carmichael, *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy* (2007)

-- Sandra Grimes and Jeanne Vertefeuille, *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed* (2012).

Spy catching… the surgery of counterintelligence

The thankless and exhausting task of tracking down
a traitor always seems much easier in retrospect than in prospect.
The clues always seem so obvious—but only after the hunt has caught its prey.

-- Markus Wolf, Former Director HVA, East German Intelligence Service (1958-1987)



Counterintelligence Investigative Source Operation. See *Investigative Source Operation (ISO).*

Counterintelligence Mission. Exploit and defeat adversarial intelligence activities directed against US interests; protect the integrity of the US intelligence system; provide incisive, actionable intelligence to decision makers at all levels; protect vital national assets from adversarial intelligence activities; and neutralize and exploit adversarial intelligence activities targeting the armed forces. (ONCIX website: <http://www.ncix.gov/about/mission.html>)

Counterintelligence Missions. DoD CI responsibilities to support force protection; research, development, and acquisition; defense critical infrastructure; and countering espionage. (DoDD 5240.16, DoD CI Functional Services, 27 Aug 2012 with change 1 dated 15 Oct 2013)

CI Missions *vs.* CI Functions

"Functions differ from CI missions in that missions focus on end results to be accomplished, rather than on the means for accomplishment."
-- *Mission Area Analysis of DoD Counterintelligence*, Institute for Defense Analyses, May 1999, p.7

Missions focus on the "end result" to be accomplished
Functions are useful terms of reference to describe "what is done"

DoD Counterintelligence Missions

+ Countering Espionage
+ Counterintelligence Support to Force Protection (FP)
+ Counterintelligence Support to Research, Development, and Acquisition (RDA)
+ Counterintelligence Support to Defense Critical Infrastructure (DCI)

Note: The Army identified four primary CI mission areas in FM 2-22.2 as:
+ Counterespionage
+ CI Support to Force Protection
+ CI Support to Research, Development, and Acquisition
+ Cyber CI

See Army FM 2-22.2, *Counterintelligence*, Oct 2009 and ADRP 2-0, *Intelligence*, Aug 2012

Counterintelligence Mission Manager. The National Counterintelligence Executive (NCIX) serves as the Mission Manager for Counterintelligence IAW Intelligence Community Directive (ICD) 900. Also see *mission managers.*

Counterintelligence Mission Tasking Authority (CI MTA). The authority to task a Military Service CI organizations' headquarters or a Defense Agency's organic CI element to execute a specific CI mission or conduct a CI function within that organization's CI charter. (DoDD O-5240.02, CI, 20 Dec 2007)

Director, Defense CI & HUMINT Center, exercises CI MTA to ensure the effective integration and synchronization of the DoD CI community (para 5.2.3, DoDD O-5240.02).

Counterintelligence Operational Concept/Proposal. The document used to propose an offensive counterintelligence operation (OFCO) which serves as the basis for the planning, review, and approval process. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence Operational Leads (CIOLs). Interagency CI referrals from CIA operations; generally produced and disseminated by the Counterespionage Group (CEG), Counterintelligence Center (CIC) at CIA headquarters. (902d MI Group Investigative Handbook, Jun 2012 2007, p.62)

Counterintelligence Operational Tasking Authority (CIOTA). The levying of CI requirements specific to joint military activities and operations. Counterintelligence operational tasking authority is exercised through supporting components. (JP 1-02)

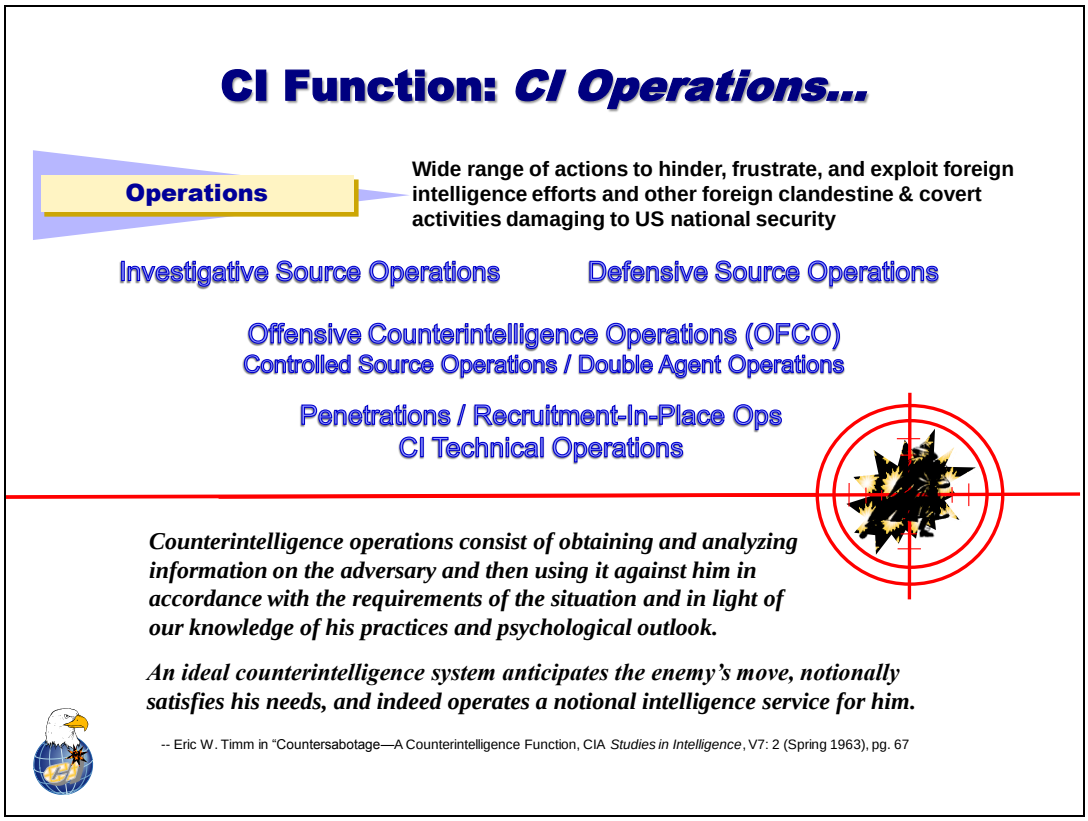
Term previously in DoDI 5240.10, dated 14 May 2004 and JP 2-01.2, dated 13 Jun 2006.

Counterintelligence Operations. Proactive activities designed to identify, exploit, neutralize, or deter foreign intelligence collection and terrorist activities directed against the United States. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Offensive Counterintelligence Operation (OFCO); recruitment-in-place (RIP); penetration; penetration operation.*

-- Also, operations/efforts intended to negate, confuse, deceive, subvert, monitor, or control the clandestine collection operations of foreign governments or agencies. (CI Community Lexicon)

"While much of the daily work of counterintelligence is laborious and humdrum, its complex and subtle operations are very much like a giant chess game that uses the whole world as its board."

-- Allen Dulles, Former DCI
The Craft of Intelligence (1963)



Counterintelligence Operations—one of five CI functions—are conducted to:
-- manipulate, disrupt, neutralize and or destroy the effectiveness of foreign intelligence activities;
-- recruit or induce defection of foreign intelligence officers and personnel;
-- collect threat information on foreign intelligence operations, modus operandi, intelligence requirements, targeting, objectives, personalities, communications, capabilities, limitations, and vulnerabilities;
-- provide information and operations databases to support decision makers;
-- provide CI support to clandestine human intelligence operations;
-- identify past, ongoing or planned espionage;
-- support force protection, operations other than war and peacekeeping;
-- acquire foreign intelligence espionage equipment for analysis and countermeasures development;
-- develop operational data, threat data and espionage leads for future CI operations, investigations, and projects and develop the potential of these leads to enhance DoD security overall; and
-- support specific [Service], Chairman Joint Chiefs of Staff, DoD and national plans.

Source: JP 1-02 and SEVNAVINST 3850.2C, *Department of Navy Counterintelligence*, 20 Jul 2005

Counterintelligence Production. The process of analyzing all-source information concerning espionage or other multidiscipline intelligence collection threats, sabotage, terrorism, and other related threats to US military commanders, the DoD, and the US Intelligence Community and developing it into a final product that is disseminated. Counterintelligence production is used in formulating security policy, plans, and operations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the creation of finished intelligence products incorporating CI analysis in to known or anticipated CI concerns. (DoDD 5240.02, CI, 20 Dec 2007 with change 1 dated 30 Dec 2010)

-- Also, the creation of finished intelligence products incorporating CI analysis in response to known or anticipated customer CI concerns. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, the conversion of analyzed CI information into intelligence products in support of known or anticipated user requirements. (DIA Instruction 5240.002, DIA CI Activities, 15 Jun 2005)

Counterintelligence Programs. Capabilities and activities established within an organization for the purposes of identifying, deceiving, exploiting, disrupting, or protecting against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of FIEs [Foreign Intelligence Entities]. (ICD 750, Counterintelligence Programs, 5 Jul 2013)

Counterintelligence Recruitment Lead (CIRL). An individual being assessed for possible use in a counterintelligence operation, investigation, or project as a controlled source. (AR 381-47, Offensive Counterintelligence Operations, 17 Mar 2006)

Counterintelligence-scope Polygraph (CSP). A screening polygraph examination that uses relevant questions limited to prescribed CI issues. (DoDI 5210.91, PCA Procedures, 12 Aug 2010 with change 1 dated 15 Oct 2013)

Counterintelligence Screening. A systematic process for obtaining information of CI interest from a specific person or target audience. (FM 2-22.2, Counterintelligence, Oct 2009)

> CI screening normally is non-confrontational – ***it is NOT an interrogation***. See Chapter 4, *CI Collection Program* of FM 2-22.2, Counterintelligence, Oct 2009 (page 4-5 through 4-7).
>
> CI screening should not use any of the "interrogation methods" defined in FM 2-22.3, *Human Intelligence Collector Operations*.

Counterintelligence Special Agent. Within DoD, US Government personnel (military and civilian employees) who have successfully completed an approved Counterintelligence Special Agent course of instruction, who are authorized to be issued CI Badge and Credentials (B&Cs), and who are assigned to conduct CI investigations and/or operations. .

> Within the US Army: military personnel holding the military occupational specialty (MOS) 35L, 351L, or 35E as a primary or additional specialty, and selective civilian employees in the GS-0132 career field; see AR 381-20, Army CI Program (U).

Counterintelligence Special Operations Concept (CISOC). The document used to propose a defensive counterintelligence operation, special investigative activity. Or counterintelligence source operation which serves as the basis for the planning, review, and approval process. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence Staff Officer (CISO). This term replaced by "*Command CI Coordinating Authority*" or CCICA; see DoDI 5240.10, CI in the Combatant Commands and Other DoD Components, 5 Oct 2011.

Counterintelligence Support. Conducting counterintelligence activities to protect against espionage and other foreign intelligence activities, sabotage, international terrorist activities, or assassinations conducted for or on behalf of foreign powers, organizations, or persons. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *counterintelligence*.

-- Also, the application of knowledge regarding the foreign intelligence and international terrorist threat to assist commanders, program managers, and agency heads to identify the insider threat and to protect information or technology vital to the national defense, including the force, technology, critical infrastructure, and information systems. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence Support Plan (CISP). A formal and living plan describing activities conducted by a Defense CI Component in support of a DoD RDA [Research, Development and Acquisition] program or activity with CPI [critical program information], at DoD-affiliated RDT&E facilities, and at essential CDCs [cleared defense contractor] where CPI resides. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

-- Also, a formal plan that outlines and describes the CI support to be provided to research and development facilities, RDA [Research, Development and Acquisition] programs with CPI [critical program information], and CPI resident at cleared Defense contractor facilities. CISPs are coordinated with and approved by the RDA Director, Program Executive Office, or Program Manager, as appropriate, and are an appendix to the PPP. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008, with change 1 dated 28 Dec 2010)

Defense CI Components use a CISP to integrate CI activities into RDA, manage, and document non-investigative or non-operational activities conducted. See Appendix 2 to Encl 3 of DoD Instruction O-5240.24, *CI Activities Supporting RDA*, 8 June 2001 (pp. 22-23) for specifics to include elements of a CISP.

Note: A CISP takes precedence over a *DCIP CI Coverage Plan* at supported locations where a CISP is required in accordance with DoD Instruction 5240.24, *Counterintelligence Activities Supporting RDA*.

Counterintelligence Support to HUMINT. [CI activities which] prevents the detection, neutralization or manipulation of strategic U.S. DoD HUMINT collection activities by foreign intelligence or security servives. (DIA Instruction 5240.002, *DIA Counterintelligence Activities*, 15 Jun 2005)

For additional information see Appendix D, *Counterintelligence Support to Human Intelligence (U),* JP 2-01.2, *CI & HUMINT in Joint Operations (U),* 16 Mar 2011 with chg 1 dated 26 Aug 2011

Counterintelligence Targets. CI targets include personalities, organizations, and installations (PO&I) of intelligence or CI interest, which must be seized, exploited, neutralized or protected. Also see Black List, Gray List, White List. (USMC, MCWP 2-6 [previously 2-14], Counterintelligence, 5 Sep 2000)

Counterintelligence Technical Services (CITS). Encompasses Technical Surveillance Countermeasures (TSCM) and Technical Support to Counterintelligence (TSCI). TSCM is used to detect the presence of technical surveillance devices and hazards and to identify technical security vulnerabilities that put the surveyed facility at risk. TSCI provides technical surveillance and countersurveillance in support of CI activities. Also see *Technical Surveillance Countermeasures*.

Counterintelligence Threat (CI Threat). The capability and intent of one entity to detect and counteract another's intelligence activities – the objective is to undermine the effectiveness of opposing intelligence activities.

To date, the term "CI Threat" remains undefined officially by DoD or IC policy. CI threat is often misused when actually referring to the "intelligence collection threat."

The "CI Threat" includes all activities undertaken by an adversary to identify, disrupt, manipulate, exploit, and/or destroy the effectiveness of friendly intelligence operations/activities. Specifically, CI threats are actions one country/entity directs against another's intelligence operations and other clandestine/covert activities. Hence the CI threat to US intelligence is the capability and intent of any entity to detect and counteract U.S. intelligence activities -- separate and distinct from intelligence threats. "CI threats" are not analogous to the threats of interest to counterintelligence.

From the US perspective -- the CI threat is foreign counterintelligence or security services efforts to counter -- detect, disrupt, neutralize, and exploit -- US intelligence activities or other US clandestine/covert activities.

Counterintelligence Training. Institutional training in knowledge, skills, abilities, and core competencies unique to CI missions and functions. (DoDI 3305.11, DoD CI Training, 19 Mar 2007)

-- Also, instructions and applied exercises offered through various media and methods for the acquisition, retention, and enhancement of skills, knowledge, and abilities required to counter or neutralize: intelligence collection efforts; other intelligence activities; sabotage; and terrorist activities and assassination efforts on behalf of foreign powers. (DoDI 3305.12, Intelligence and Counterintelligence Training of Non-US Persons, 25 Oct 2007 w/ chg 2 dated 15 Oct 2013)

Counterproliferation (CP). Those actions (e.g., detect and monitor, prepare to conduct counter-proliferation operations, offensive operations, weapons of mass destruction, active defense, and passive defense) taken to defeat the threat and/or use of weapons of mass destruction against the United States, our military forces, friends, and allies. (JP 1-02 and JP 3-40, Combating WMD, 10 Jun 2009)

-- Also, the activity by United States government intended to prevent the proliferation of nuclear, chemical and biological capabilities to other nations. (HPSCI Report, 27 Jul 2006)

Countermeasure. Anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, action, device, procedure, technique, or other measure that reduces or eliminates one or more vulnerabilities. (DoD Insider Threat IPT Final Report, 24 Apr 2000)

-- Also, [in TEMPEST usage] action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment that electronically processes information (NSTISSI 7002, TEMPEST Glossary, 17 Mar 1995).

Countermeasures. That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

-- Also, defensive security programs and activities which seek to protect against both foreign intelligence collection efforts and unauthorized access to, or disclosure of, protected facilities, information, and material. (AR 380-20, Army CI Program, 25 May 2010)

-- Also, the employment of devices and/or techniques that has as its objective the impairment of the operational effectiveness of an adversary's activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities. (DSS Glossary)

-- Also, the employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities. (*Draft* DoDI 5200.39, CPI Identification and Protection within RDA Programs)

-- Also, [in polygraph and credibility assessment usage] those strategies employed by examinees to affect PCA testing by the intentional application of physical, mental, pharmacological, or behavioral tactics. (DoDI 5210.21, PCA Procedures, 12 Aug 2010 w/ chg 1 dated 15 Oct 2013)

Counterproliferation. Those actions taken to defeat the threat and/or use of weapons of mass destruction against the United States, our forces, friends, allies, and partners. (JP 1-02 and JP 3-40, Combating WMD, 10 Jun 2009)

Countersurveillance. All measures, active or passive, taken to counteract hostile surveillance. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010) Also see *counter surveillance; surveillance detection.*

-- Also,…security techniques designed to detect, prevent, or deceive hostile observation of friendly operations or activities. (CI Community Lexicon)

-- Also, the total action taken to detect and frustrate hostile surveillance. (*Encyclopedia of the CIA*, 2003)

-- Also, [Counter Surveillance]. Measures or actions taken when under verified or suspected surveillance. (DoDI S-5240.15, FPRG, 20 Oct 2010 with change 1 dated 16 Oct 2013)

-- Also, the process of detecting and mitigating hostile surveillance (Stratfor - Global Intelligence)

> *An effective CS [countersurveillance] program depends on knowing two "secrets": first, hostile surveillance is vulnerable to detection because those performing it are not always as sophisticated in their tradecraft as commonly perceived; and second, hostile surveillance can be manipulated and the operatives forced into making errors that will reveal their presence.*
>
> *…CS can be performed by a person who is aware of his or her surroundings and who is watching for people who violate the principles of TEDD.* At a more advanced level, the single person can use surveillance detection routes (SDRs) to draw out surveillance.*
>
> ** The U.S. government uses the acronym TEDD to illustrate the principles one can use to identify surveillance. So, a person who sees someone repeatedly over Time, in different Environments and over Distance, or one who displays poor Demeanor can assume he or she is under surveillance. Surveillants who exhibit poor demeanor, meaning they act unnaturally, can look blatantly suspicious, though they also can be lurkers -- those who have no reason for being where they are or for doing what they are doing. Sometimes they exhibit almost imperceptible behaviors that the target senses more than observes. Other giveaways include moving when the target moves, communicating when the target moves, avoiding eye contact with the target, making sudden turns or stops, or even using hand signals to communicate with other members of a surveillance team.*
>
> -- Fred Burton, "The Secrets of Countersurveillance," *Security Weekly*, Stratfor, 6 Jun 20007; article on line at: <http://www.stratfor.com/secrets_countersurveillance>

Counterterrorism (CT). Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks. (JP 1-02 and JP 3-26, Counterterrorism, 13 Nov 2009) Also see antiterrorism; *terrorism; combating terrorism*.

-- Also, the practices, tactics, techniques, and strategies adopted to prevent or respond to terrorist threats or acts, both real and suspected. (ODNI, U.S. National Intelligence – An Overview 2011)

> Also see *National Strategy for Counterterrorism*, June 2011 at
> < http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf >

Country Clearance. Clearance for official U.S. Government representative travel to a foreign country granted through the cognizant U.S. Embassy or U.S. Mission. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

Country Team. The senior, in-country, US coordinating and supervising body, headed by the chief of the US diplomatic mission, and composed of the senior member of each represented US department or agency, as desired by the chief of the US diplomatic mission. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

Courier. Person who carries an item or information from one person or place to another. The courier may or may not be aware of the nature of the item or information being transported. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, a messenger responsible for the secure physical transmission and delivery of documents and materials. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Cover. A protective guise used by a person, organization, or installation to conceal true affiliation with clandestine or other sensitive activities. (DoDD S-5105.61, DoD Cover and Cover Support Activities (U), 6 May 2010) Also see *cover for action; cover for status*.

-- Also, the concealment of true identity, purpose, or organizational affiliation with assertions of false information as part of, or in support of, official duties to carry out authorized activities and lawful operations. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

-- Also In intelligence usage, those measures necessary to give protection to a person, plan, operation, formation, or installation from enemy intelligence effort and leakage of information. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, actions to conceal actual friendly intentions, capabilities, operations, and other activities by providing a plausible yet erroneous explanation of the observable. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a verifiable and documented protective guise used by a person, organization, or installation to conceal true identity or affiliation. (HDI Lexicon, April 2008)

-- Also, a protective guise used by a person, organization, or installation to prevent identification with clandestine activities and to conceal the true affiliation of personnel and the true sponsorship of their activities. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, protective action taken to mask or conceal an operation or activity from an adversary. (DSS Glossary)

-- Also, a protective guise used by an individual, organization, or installation to prevent identification with intelligence activities. To hide, conceal, obscure, or otherwise protect the exact identity of an individual, unit, or activity. Supported with or without documentation and backstopping depending on the sensitivity and scope of the operation. *Cover* can be anything that masks the true nature of an activity. (CI Community Lexicon)

> DoD cover may be used to protect the Department of Defense, its intelligence sources and methods, and its clandestine tactics, techniques, and procedures from exposure to the enemy and overt association with sensitive activities. The fact that DoD uses cover to protect its activities is unclassified.
>
> For DoD policy see DoDD S-5105.61, *DoD Cover and Cover Support Activities (U),* 6 May 2010.

Cover shields secret activities from the opposition

Good cover *…reaches into the mind of the opponent, thinks as he would think, and then creates a combination of fact and fancy, of actual arrangements and contrived impressions, which the opposing mind is prepared to believe…. Cover takes an infinite variety of forms.*

The best cover is that which contains the least notional and the maximum possible legitimate material…. ***Perfect cover is an ideal, rarely achieved in practice.***

-- Christopher Felix (James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Special Cover Measures…

There are many valid reasons for the special cover measures used by some military and intelligence organizations, such as potentially life-threatening, high-risk, covert operations and intelligence and counterintelligence investigations or operations.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, p.19

Cover for Action. A logical reason for doing the specific action involved. (CI Community Lexicon)

-- Also, a verifiable and documented protective guise used to disguise the true intent of an individual, organization, or activity and to provide a credible explanation as to participation in a particular activity. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010) Also see *cover for status*.

> *Cover for Action. This cover, combined with the use of appropriate clandestine tradecraft techniques (e.g. alias, disguise, darkness, surveillance detection routes to and from meetings, etc.) is what provides cover and security for clandestine meetings.*
>
> -- F.W. Rustmann, Jr., "Debunking the CIA Case Officer Myth," *Association of Former Intelligence Officers (AFIO) Newsletter* (Fall 2003), <http://ctcintl.com/Debunk.htm>; accessed 7 Mar 2011

Cover for Status. A logical and backstopped reason for being in an area or processing a particular item at a particular time. (CI Community Lexicon) Also see *cover for action*.

-- Also, a verifiable and documented protective guise used to legitimize an individual's, organization's, or activity's extended presence in a particular area. (Defense HUMINT Enterprise Manual 3301.002, Vol II, Collection Operations, 23 Nov 2010)

> *Cover for Status. This is the cover that permits [a case officer] to live and work in a particular country. If the case officer is under official cover, this means he must blend into the environment of an embassy or other official US installation abroad.*
>
> -- F.W. Rustmann, Jr., "Debunking the CIA Case Officer Myth," *Association of Former Intelligence Officers (AFIO) Newsletter* (Fall 2003), <http://ctcintl.com/Debunk.htm>; accessed 7 Mar 2011

Cover Legend. A contrived scenario or story designed to explain an organizational or personal background and past or present activities, in terms intended to protect or conceal involvement in a clandestine or otherwise sensitive activity. It incorporates as much truth as possible. It must be plausible. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

-- Also, a contrived scenario, designed to explain an organizational or personal background and past or present activities, in terms intended to protect and/or conceal involvement in a clandestine or otherwise sensitive activity. It incorporates as much truth as possible. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010) Also see *cover story*.

Cover Mechanism. Any documentary, oral, technical, fiscal, logistical, or other means provided to backstop a cover. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

Cover Stop. A stop made while under surveillance that provides an ostensibly innocent reason for a trip. (CI Centre Glossary and Spy Dust)

Cover Story. Coherent and plausible account of background, residence, employment, activities, access, etc., furnished to an individual to substantiate whatever claims are necessary to successfully carry out an operation. The difference between a cover story and a legend is that a legend is furnished to an illegal or agent by FIS. (AFOSI Manual 71-142, OFCO, 9 Jun 2000) Also see *cover legend*.

-- Also, the background legend you have developed to explain who you are and why you are where you are. (*A Spy's Journey*)

> *The cover story is most frequently used to explain the visible evidences of a clandestine operation or to provide an explanation when an operations encounters difficulties.*
>
> *…cover stories in general: they should not be too precise or too detailed, and they should not be forthcoming too quickly or all at once. …To be too precise in a cover story qualitatively increases the chances of repudiation of the story; to be too detailed increases those chances quantitatively.*
>
> -- Christopher Felix (aka James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Cover Support Activities. All measures taken to develop, coordinate, approve, activate, operate, and terminate cover. (DoDD S-5105.61, DoD Cover and Cover Support Activities (U), 6 May 2010)

Cover Within Cover. A credible confession to an act that is less serious than espionage and will explain all actions under suspicion by foreign intelligence services. (Words of Intelligence, 2nd Edition, 2011)

Covering Agent. [As used within US Army] a CI Agent who provides dedicated full or part time counterintelligence support, education, and liaison to an organization, agency, or research, development, and acquisition program. (AR 381-20, Army CI Program, 25 May 2010)

Covert. A method of conducting operations that hides the true intent, affiliation or relationship of its participants. Differs from clandestine in that covert conceals the identity of the sponsor, whereas clandestine conceals the identity of the operation. (National HUMINT Glossary) See *clandestine; covert action; covert operation*.

Covert, from the Latin *cooperire*, "to cover," means "concealed, hidden, under cover, not avowed."

Covert and clandestine are not synonymous!

Covert Action. Activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly. Covert action **does not include** activities the primary purpose of which is to acquire intelligence, **traditional counterintelligence activities** [*emphasis added*], traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities. (Section 503e, National Security Act of 1947 [50 USC §413b]) Also see *covert; covert operation; finding; special activities.*

Covert action should not be confused with missionary work.

-- Henry Kissinger
as cited in James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006), p. 33

…the overt foreign activities of the US Government must be supplemented by covert operations

NSC Directive 10/2 (dated 18 Jun 1948)
as cited in Warner, *CIA Under Truman* (1994)

Covert actions are designed to avoid revealing the role of the United States in their planning or execution. EO 12333 (as amended 30 Jul 2008) directs that no agency except CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective.

EO 12333 limits covert action, i.e., "no covert action may be conducted which is intended to influence US political processes, public opinion, policies, or media. " (EO 12333, para 2.13)

Covert action by DoD must be directed by the President, subsequently approved by the Secretary of Defense, and executed in accordance with applicable law.

Evolution of Covert Action

[I]n December 1947, the National Security Council issued a series of classified directives specifying and expanding the CIA's covert mission. The first of these directives, NSC-4-A, authorized the Director of Central Intelligence (DCI) to conduct covert psychological operations consistent with United States policy and in coordination with the Departments of State and Defense. A later directive, NSC 10/2, authorized the CIA to conduct covert political and paramilitary operations. […] The United States should ,maintain the option of reacting in the future to a grave, unforeseen threat to United States national security through covert means.

-- Church Committee – 1976 (Senate Report 94-755, Book I, 26 April 1976)

Covert action must be consistent with and supportive of national policy and must be placed appropriately within a national security policy framework. Covert action must never be used as a substitute for policy.

-- National Security Decision Directive 159, 18 Jan 1985 (originally Top Secret-Sensitive, declassified)

Covert actions are… legally distinct from clandestine missions: 'clandestine' refers to the tactical secrecy of the operation itself, 'covert' refers to the secrecy of the sponsor. ...covert action can include a wide range of activity, from propaganda and disinformation to political influence operations, economic destabilization, and paramilitary operations. Historically, the Central Intelligence Agency (CIA) has been the main agent of US covert action….

-- Jennifer D. Kinne, "Covert Action and the Pentagon," *Intelligence and National Security*, Vol. 22 No. 1, February 2007, pp. 57-58

Covert action, or to use the British term, *special political action*, is the attempt by a government or group to influence events in another state or territory without revealing its own involvement. …Covert action is really an American term-of-art that came into use after World War II.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 2

Typically, covert actions are carried out by the CIA with such assistance as may be necessary by other elements of the intelligence Community as directed by the President. U.S. law requires that all covert actions be approved prior to their execution by the President in a written 'finding' and that notification be provided to the two intelligence committees in Congress. Covert actions may involve political, economic, propaganda, or paramilitary activities.

-- WMD Report, 31 Mar 2005

Covert action is often called the "dirty tricks" side of spying. It consists of sabotage, subversion, paramilitary operations, political action, psychological; operations, and black propaganda. It is not always pretty. Covert action has historically been a relatively small part of the CIA's overall activity, but it is certainly the aspect of U.S. spying that has been the most controversial.

-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

The three basic types of covert action are perception management (historically known as propaganda), political action (influencing the actions of a foreign leader or government), and paramilitary operations (support to insurgents).

-- Duane R. Clarridge, *A Spy For All Season: My Life in the CIA* (1997), p. 410

Covert action is not intelligence. Rather, CA is the most sensitive technique for implanting national security policy. Operating in the space between diplomacy and military force, covert actions are the "third way" of accomplishing a nation's goals.

-- Dr. James E. Steiner (retired CIA), "Restoring the Red Line Between Intelligence and Policy on Cover Action," *International Journal of Intelligence and Counterintelligence*, Vol 19 No 1 (Spring 2006), p. 157

Covert action can serve as a more subtle and surgical tool
than forms of acknowledge employment of U.S. power and influence.

-- WMD Report (31 Mar 2005), p. 33

Security is indispensable to the successful conduct of covert action.
…[A]ccess to information on US covert action policies shall be restricted
to the absolute minimum number of persons possible.

-- President Ronald Reagan, NSSD 159 (18 Jan 1985)

Covert Channel. An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional, or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Covert Channel Analysis. Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Covert Communication (COVCOM). Clandestine, hidden communication that protects both the information being shared and the relationship between the sending and receiving parties. (National HUMINT Glossary)

-- Also, any technique or device used to relay data clandestinely from case officer to agent or agent to case officer. (Spycraft)

-- Also, an agent's spy gear for communicating with his case officer. (*A Spy's Journey*)

Covert Operation. An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. (JP 1-02 and JP 3-05, Special Operations, 18 Apr 2011) Also see *covert; covert action, clandestine operation.*

Covert refers to the secrecy of the sponsor

Clandestine operations are sometimes incorrectly referred to as "covert operations." Although both are secret and sensitive activities, the terms are not interchangeable. See *clandestine operation*.

"*Avowal of a covert operation, however implicit, is a hostile act, and it is wise never to indulge in hostile acts unless one is able and prepared to back them up."*

-- Christopher Felix (aka James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

A 1948 National Security Council Intelligence Directive defined *covert operations* as actions by the U.S. against foreign states "which are so planned and executed that any U.S. Government responsibility for them is not evident to unauthorized persons and that if uncovered the U.S. Government can plausibly disclaim any responsibility for them."

"Covert action is the term that describes our efforts to influence the course of events in a foreign country without our role being known….[it] has always been assigned to the CIA to perform, by means of unattributable propaganda, sub rosa political action, or secret paramilitary support."

-- Stansfield Turner, Former Director Central Intelligence Agency

CPI. See *Critical Program Information*.

Credentials [Counterintelligence]. An official document or set of documents presenting evidence of the identity, authority, and status of the bearer and for use in conducting authorized CI activities. (DoDI 5240.25, Counterintelligence Badge and Credentials, 30 Mar 2011 with change 1 dated 15 Oct 2013) Also see *badge; special agent*.

-- Also, official documents which identify the bearer as a representative of a specific agency or department of the U.S. Government.

Credible Information. Information disclosed or obtained by a criminal investigator that, considering its source and nature and all the circumstances, is believable enough that a trained criminal investigator can state the information is true. (DoDI 5505.7, Titling & Indexing Subjects of Criminal Investigations in DoD, 27 Jan 2012)

-- Also, information disclosed to or obtained by an investigator that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to indicate that criminal activity has occurred and would cause a reasonable investigator under similar circumstances to pursue further the facts of the case to determine whether a criminal act occurred or may have occurred. (AR 195-2, Criminal Investigation Activities, 15 May 2009)

Credibility Assessment. The multi-disciplinary field of existing, as well as potential, techniques and procedures to assess truthfulness that relies on physiological reactions and behavioral measures to test the agreement between an individual's memories and statements. (DoDD 5210.48, Polygraph and Credibility Assessment Program, 25 Jan 2007 with change 2 dated 15 Nov 2013)

Criminal Intelligence (CRIMINT). Law enforcement information derived from the analysis of information collected through investigations, forensics, crime scene and evidentiary processes to establish intent, history, capability, vulnerability, and modus operandi of threat and criminal elements. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

-- Also, a category of police intelligence derived from the collection, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities of supported organizations. (ATTP 3-39.20, Police Intelligence Operations, Jul 2010)

-- Also, information compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. (National Criminal Intelligence Sharing Plan, Oct 2003)

For DoD Policy see DoDI 5525.18, Law Enforcement Criminal Intelligence in DoD (Note: does not apply to counterintelligence personnel).

CRIMINT gathering is a fundamental and essential element in the all-encompassing duties of all DoD Law Enforcement Agencies. CRIMINT can aid in crime prevention, threat disruption, offender pursuit and apprehension, and evidence capture necessary for conviction.

Criminal Investigation. Investigation into alleged or apparent violations of law undertaken for purposes which include the collection of evidence in support of potential criminal prosecution. (DoDI 5505.7, Titling & Indexing Subjects of Criminal Investigations in DoD, 27 Jan 2012)

-- Also, the process of searching, collecting, preparing, identifying, and presenting evidence to prove the truth or falsity of an issue of law. (US Army, FM 3-19.13, Law Enforcement Investigations, Jan 2005)

Criminal investigation is both an art and a science.

In science, the absolute truth is often achieved. Experience has shown that in criminal investigations a less decisive hypothesis may sometimes be all that is possible to achieve.

A criminal investigation is the process of searching, collecting, preparing, identifying, and presenting evidence to prove the truth or falsity of an issue of law.

Objectives of Criminal Investigations:
- 1) *Determine if a crime was committed;*
- 2) *Collect information and evidence legally to identify who was responsible;*
- 3) *Apprehend the person responsible;*
- 4) *Recover stolen property;*
- 5) *Present the best possible case to the prosecutor; and*
- 6) *Provide clear, concise testimony.*

-- US Army, FM 3-19.13, *Law Enforcement Investigations*, Jan 2005

A criminal investigation is normally initiated when objective facts and circumstances reasonably indicate a crime has been, is being or will be committed. A criminal investigation is normally limited to: who committed the act; secure evidence to establish the elements of the offense; and support prosecution.

Also see *Crime Scene Investigation: A Guide for Law Enforcement*, Sep 3013; available on line at <http://www.nist.gov/oles/csiguide.cfm>

Criminal Investigative Information. Information compiled in the course of a criminal investigation. (AR 195-2, Criminal Investigation Activities, 15 May 2009)

Criminal Investigation Task Force (CITF). The DoD CITF is a strategic-level organization with a mission to develop and fuse police intelligence with MI [military intelligence] for the purpose of building criminal cases against terrorist criminals that have attacked U.S. interests. (ATTP 3-39.20, Police Intelligence Operations, Jul 2010)

The CITF conducts complicated criminal investigations targeting terrorists and complex criminal organizations. These cases typically cross international borders and involve criminals captured as a result of military operations, requiring coordination with international police and intelligence agencies. The CITF combines USACIDC special agents (and criminal investigators from other Services), police and intelligence analysts, and attorneys into teams. These teams synchronize and fuse information and intelligence from all available sources to conduct criminal investigations that enable criminal prosecution in U.S. or host nation legal systems.

-- ATTP 3-39.20 (FM 3-19.50), Police Intelligence Operations, July 2010

Criminal Offense. Any criminal act or omission as defined and prohibited by the Uniform Code of Military Justice, the United States Code, State and local codes, foreign law, or international law or treaty. As used herein, this term does not include military offenses as defined below. In the case of juveniles, this term refers to those acts which, if committed by an adult, would be subject to criminal sanctions. (AR 195-2, Criminal Investigation Activities, 15 May 2009)

Crisis. An incident or situation involving a threat to the United States, its citizens, military forces, possessions, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of US military forces and resources is contemplated in order to achieve national objectives. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Crisis Action Planning (CAP). The Adaptive Planning and Execution System process involving the time-sensitive development of joint operation plans and operation orders for the deployment, employment, and sustainment of assigned and allocated forces and resources in response to an imminent crisis. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Crisis Management (CrM). Measures, normally executed under federal law, to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or an act of terrorism. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

CRITIC. Critical information messages sent over the CRITICOMM System that must be delivered to the President within 10 minutes upon recognition. (DoDD 5100.20, NSA, 26 Jan 2010)

Critical Asset. A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, *Defense Critical Asset*: an asset of such extraordinary importance to DoD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its mission. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

-- Also, any asset (person, group, relationship, instrument, installation, process or supply at the disposition of an organization for use in an operational or support role) whose loss or compromise would have a negative impact on the capability of a department or agency to carry out its mission; or may have a negative impact the ability of another U.S. Government department or agency to conduct its mission; or could result in substantial economic loss; or which may have a negative impact on the national security of the U.S. (ICD 750, Counterintelligence Programs, 5 Jul 2013)

Critical Information (also called CRITIC). Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.(JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, decisions, intentions, or actions of foreign governments, organizations, or individuals that could imminently and materially jeopardize vital U.S. policy, economic, informational, or military interests to such an extent that the immediate attention of the President and the National Security Council may be required. (DoDD 5100.20, NSA, 26 Jan 2010)

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a deliberating impact on the security, national economic security, national public health and safety, or any combination of those matters. (Critical Infrastructures Protection Act of 2002 and USA Patriot Act §1016)

-- Physical or virtual systems and assets that if compromised by a physical or cyberspace incident negatively impact the national security, economic stability, public confidence, health, or safety of the United States. (DoD Strategy for Operating in Cyberspace, May 2011)

-- Also, [within DoD] infrastructure deemed essential to DoD operations or the functioning of a critical asset.

Nation's critical infrastructure and key resources, as set forth in the 2006 National Infrastructure Protection Plan (NIPP) includes the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

-- Cited in the *National Strategy for Homeland Security*

Failure of critical assets degrades or disrupts operations; cascading failures of critical infrastructure assets within and across infrastructures may lead to mission failure

-- DoD Critical Infrastructure Protection Strategy, April 2003

Copy of the 2009 *National Infrastructure Protection Plan* (NIPP) at:
<http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>

Critical Infrastructure and Key Resources (CI/KR). The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. (JP 3-27, Homeland Defense, 29 Jul 2013)

Critical Infrastructure Protection (CIP). Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013) Also see *Defense Critical Infrastructure*.

PDD-63 set as a national goal the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber). Also see PPD-21, Critical Infrastructure Security and Resilience, 12 Feb 2013. PPD-21 identifies 16 critical infrastructure sectors; DoD is the sector-specific agency for the Defense Industrial Base (DIB).

For DoD policy see DoDD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*.

Critical Intelligence. Intelligence that is crucial and requires the immediate attention of the commander. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Critical National Asset (CNA). Any information, policies, plans, technologies, or capabilities that, if acquired (stolen), modified, or manipulated by an adversary, would seriously threaten US national or economic security. (NIP - *FY 2009 Congressional Budget Justification Book*, redacted version)*

* Copy available at: <http://www.fas.org/irp/dni/cbjb-2009.pdf> (accessed 24 Jan 2013).

Critical Program Information (CPI). Elements or components of an RDA [research, development & acquisition] program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008 w/ change 1 dated 28 Dec 2010)

Note: DoDI 5200.39 is under revision, proposed revised definition for CPI: *U.S. capability elements that contribute to the warfigthers' technical advantage throughout the life cycle, which if compromised or subject to unauthorized disclosure, decrease the advantage. U.S. capability elements may include, but are not limited to, technologies and algorithms residing on the system, its training equipment, or maintenance support equipment.*

It is DoD policy (IAW DoDI 5200.39) to provide uncompromised and secure military systems to the warfighter by performing comprehensive protection of CPI through the integrated and synchronized application of Counterintelligence, Intelligence, Security, systems engineering, and other defensive counter-measures to mitigate risk.

Failure to apply consistent protection of CPI may result in the loss of confidentiality, integrity, or availability of CPI, resulting in the impairment of the warfighter's capability and DoD's technological superiority.

CPI includes: information about applications, capabilities, processes, and end-items; elements or components critical to a military system or network mission effectiveness; and technology that would reduce the US technological advantage if it came under foreign control.

CPI information shall be identified early in the research, technology development and acquisition processes, but no later than when a DoD Agency or military component demonstrates an application for the technology in an operational setting, in support of a transition agreement with a pre-systems acquisition or acquisition program, or in exceptional cases, at the discretion of the laboratory/technical director.

Critical Technology. Technology or technologies essential to the design, development, production, operation, application, or maintenance of an article or service which makes or could make a significant contribution to the military potential of any country, including the United States. This includes, but is not limited to, design and manufacturing know-how, technical data, keystone equipment, and inspection and test equipment. (DoDI 2040.02, International Transfers of Technology, Articles and Services, 10 Jul 2008) Also see *dual-use, technology*.

DoD Policy – Critical Technology

Dual-use and defense-related technology shall be treated as valuable national security resources, to be protected and transferred only in pursuit of national security and foreign policy objectives. Those objectives include ensuring that: critical U.S. military technological advantages are preserved; transfers which could prove detrimental to U.S. security interests are controlled and limited; proliferation of weapons of mass destruction and their means of delivery are prevented; and diversion of defense-related goods to terrorists is prevented.

See DoDI 2040.02, *International Transfers of Technology, Articles and Services*, 10 Jul 2008.

Critical Thinking. A deliberate meta-cognitive (thinking about thinking) and cognitive (thinking) act whereby a person reflects on the quality of the reasoning process simultaneously while reasoning to a conclusion. The thinker has two equally important goals: coming to a solution and improving the way she or he reasons. (David T. Moore, *Critical Thinking and Intelligence Analysis*)

-- Also, intellectual discipline of rigorously weighing evidence and assumptions, and assessing multiple hypotheses resulting in accurate, persuasive, and policy-relevant conclusions. (DIA, 2012-2017 Defense Intelligence Agency Strategy)

> *Critical Thinking and Intelligence Analysis*, National Defense Intelligence College occasional paper no. 14, March 2007.
> Copy available at <http://www.au.af.mil/au/awc/awcgate/dia/ndic_moore_crit_analysis_hires.pdf>
>
> Also see The Foundation for Critical Thinking, www.criticialthinking.org, *The Thinker's Guide to Analytical Thinking*, 2007.

Criticality. [In critical infrastructure usage] a metric used to describe the consequence of loss of an asset, based on the effect the incapacitation or destruction of the asset would have on DoD operations and the ability of the Department of Defense to fulfill its missions. (DoDI 3020.45, DCIP Management, 21 Apr 2008)

Cross-cuing. The use of one intelligence source to initiate the collection against a particular target with another intelligence collector. Also see *cueing.*

> *CI and HUMINT provide unique opportunities for enabling and cross-cuing other intelligence disciplines or capabilities. CI and HUMINT sources can enable other intelligence collection disciplines or provide time sensitive "tip off" information to cue other collection capabilities.*
> -- JP 2-01.2, *CI & HUMINT in Joint Operations*, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011, para 3b (p. V-2)

Cryptanalysis. The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption. (JP 1-02)

Cryptography. The art and science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. (DoDD 5100.20, NSA, 26 Jan 2010)

Cryptology. The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. (JP 1-02)

-- Also, the branch of knowledge that treats the principles of cryptography and cryptanalytics; and the activities involved in producing signals intelligence (SIGINT) and maintaining communications security (COMSEC). (DoDD 5100.20, NSA, 26 Jan 2010)

Cryptonym. Code name; crypt or crypto for short, always capitalized. …prefixes to code names are used to identify the nature of the clandestine source, [e.g., GT and CK] prefixes were both "diagraph" identifiers for the Soviet and East European program….. The diagraph is used in front of the cryptonym of the source as a more formal way of referring to the subject, not unlike putting "Mr." in front of "Smallwood." (Spy Dust)

-- Also, a false name used in official correspondence to hide the identity of the agent, officer, or operation. (A Spy's Journey)

Cueing. The use of one or more sensor systems to provide data that directs collection by other systems. (term previously defined in FM 2-0, Intelligence, May 2004) Also see *cross-cuing*.

Cultivation. A deliberate and calculated association with a person for the purpose of recruitment, obtaining information, or gaining control. (AFOSI Instruction 71-101, 6 Jun 2000)

-- Also, apparently casual but actually deliberate and calculated effort to gain control of an individual, induce him to furnish information, and agree to recruitment. Cultivation can extend over a considerable periods of time. (FBI FCI Terms)

Cultural Intelligence. Knowledge resulting from all-source analysis of cultural factors, which assists in anticipating the actions of people or groups of people. (National Intelligence: Consumer's Guide - 2009).

Current Intelligence. *Within DoD: None – term removed from JP 1-02 per JP 2-0 Joint Intelligence, 22 Oct 2013.*

> Previously defined as: one of two categories of descriptive intelligence that is concerned with describing the existing situation.

Custodial Interview. Interview conducted of a subject following formal arrest or detention. Subjects are made fully aware of their deprivation of freedom or their "in custody" status. (Army FM 2.22-2, CI, Oct 2009).

Cutout. An intermediary or device used to obviate direct contact between members of a clandestine organization. (JP 1-02)

-- Also, an intermediary used to obviate direct linkage between either the origin or destination of an intelligence operation or action. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, an individual whose services are used to prevent contact and recognition between specific members of an intelligence service with the purpose of providing compartmentation and security. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, a mechanism or person that acts as a compartment between the members of an operation but which allows them to pass material or messages securely. (CI Centre Glossary)

Cyber. 1) Any process, program, or protocol relating to the use of the Internet or an intranet, automatic data processing or transmission, or telecommunication via the Internet or an intranet; and 2) any matter relating to, or involving the use of, computers or computer networks. (Cybersecurity Act of 2009)

Cyber Attack. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *cyber espionage, cyber threat*.

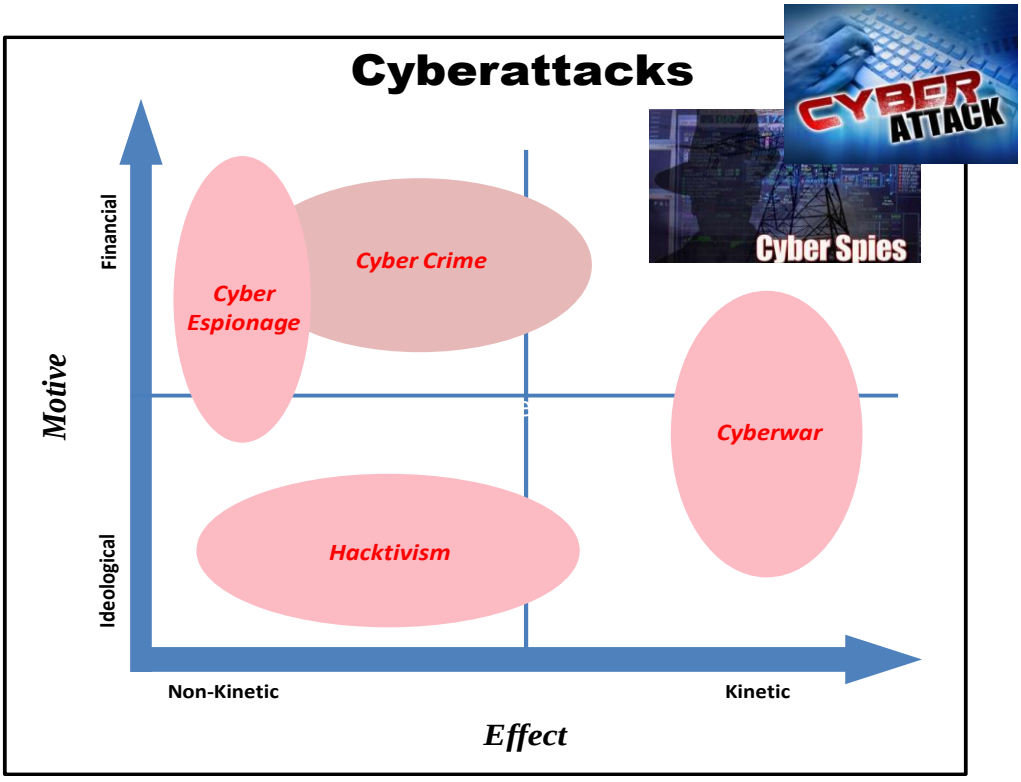
> *Disruptive and destructive cyber attacks are becoming a part of conflict between states, within states, and among nonstate actors. The borderless nature of cyberspace means anyone, anywhere in the world, can use cyber to affect someone else. … The rise of cyber is the most striking development in the post-9/11 national security landscape.*
>
> -- General Martin E. Dempsey (USA), Chairman of the Joint Chiefs of Staff, June 2013
> (Quoted in *Army* Magazine, August 2013, p. 8)
>
> ---
>
> ***Cyber attack** is a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data. It might range from a denial-of-service operation that temporarily prevents access to a website, to an attack on a power turbine that causes physical damage and an outage lasting for days.*
>
> -- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 12 Mar 2013
>
> ---

Existential Cyber Attack *is defined as an attack that is capable of causing sufficient wide scale damage for the government potentially to lose control of the country, including loss or damage to significant portions of military and critical infrastructure: power generation, communications, fuel and transportation, emergency services, financial services, etc.*

-- Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Jan 2013; copy at: <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

Also see P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know* (2014)

-- Also, Cyberattack: deliberate disruption of a computer system or network and functions delivered or supported by it. (National Research Council - 2009)



Adapted from: Eric Rosenbach and Robert Belk, "U.S. Cybersecurity: The Current Threat and Future Challenges," Nicholas Burns and Jonathon Price, Editors., *Securing Cyberspace: A New Domain for National Security*, 2012, Figure 1, p. 44

Cyber attacks are growing in frequency, scale, complexity and destructiveness.

Cyber attacks are a way of life… *since 2006, cyber incidents against the USG increased 782%* (GPO).

Cyber Counterintelligence. Counterintelligence, by any means, where a significant target or tool of the adversarial activity is a computer, computer network, embedded processor or controller, or the information thereon. (The United States Government-Wide Cyber Counterintelligence Plan - 2009 (U)) Also see *counterintelligence activities in cyberspace; cyberspace.*

* Note: Within DoD the term "cyber counterintelligence " to be withdrawn from JP 1-02; see *Counterintelligence Activities in Cyberspace*.

Cyberspace is a venue.

Cyber Effect: The manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. (PDD-20, US Cyber Operations Policy (U), 16 Oct 2012)

Cyber Electromagnetic Activities (CEMA). Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. (Army FM 3-13, Inform and Influence Activities, Jan 2013)

> CEMA consist of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO).
>
> See Army FM 3-38, *Cyber Electromagnetic Activities*, 12 Feb 2014.

Cyber Espionage. Refers to intrusions into networks to access sensitive diplomatic, military, or economic information. (DNI, Worldwide Threat Assessment of the US Intelligence Community, SSCI, 12 Mar 2013) Also see *cyber attack, cyber threat*.

-- Also, the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using illegal exploitation methods on internet, networks or individual computers… (Wikipedia at <http://en.wikipedia.org/wiki/Cyber_espionage>; accessed 5 Jan 2010)

> ***"Counterintelligence…is now a concern for every organization that lives on electronic networks and has secrets to keep. Information is liquid and liquid leaks."***
>
> -- Joel Brenner (former NCIX), America *the Vulnerable,: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, 2011, p. 64.

Cyber Exploitation: Penetration of an adversary's computer system or network to seize information (National Research Council, 2009)

> Essentially an intelligence-gathering activity, e.g., Ghostnet, Operation Aurora. Technically, exploits and attack can be similar, i.e., utilize same access vector and manipulate same vulnerability.
>
> ***"Distinction between intelligence collection and damage to systems is a few key strokes"***
>
> -- Richard A. Clarke, Author of *Cyber War*

Cyber Incident. Any attempted or successful access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or an information system, without lawful authority. (NSPD-54 / HSPD-23)

Cyber Intrusion Damage Assessment. A managed, coordinated, and standardized process conducted to determine the impact on future defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from an intrusion into a DIB unclassified computer system or network. (DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center [DC3], 1 Mar 2010)

Cyber Persona. An identity used in cyberspace to obtain information or influence others, while dissociating the actor's true identity or affiliation. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec10 with change 1 dated 16 Oct 2013)

Cyber Power. The ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power. (Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*, Washington, D.C.: National Defense University, 2009)

> Cyber power can be used to produce preferred outcomes within cyberspace or it can be use cyber instruments to produce preferred outcomes in other domains outside cyberspace.
>
> See "Cyber Power" by Joseph S. Nye, Harvard Kennedy School, May 2010; available online at: belfercenter.ksg.harvard.edu/files/cyber-power.pdf

Cyber Security (or Cybersecurity). Measures taken to protect a computer network, system, or electronic information storage against unauthorized access or attempted access. (DoDI 5205.13, Defense Industrial Base Cyber Security/Information Assurance Activities, 29 Jan 2010 w/ chg 1 dated 21 Sep 2012) Also see *computer security; information security (INFOSEC).*

-- Also, includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

- Also, the ability to protect, defend, and maintain availability, confidentiality, authentication, and integrity of networks, systems, and the data resident therein. (DoD Strategy for Operating in Cyberspace, May 2011)

-- Also, the ability to protect or defend the use of cyberspace from cyber attacks. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation.

-- National Security Strategy - 2010

> *"Cybersecurity vulnerabilities challenge governments, businesses, and individuals worldwide. Attacks have been initiated by individuals, as well as countries. Targets have included government networks, military defenses, companies, or political organizations, depending upon whether the attacker was seeking military intelligence, conducting diplomatic or industrial espionage, or intimidating political activists. In addition, national borders mean little or nothing to cyberattackers, and attributing an attack to a specific location can be difficult, which also makes a response problematic."*
>
> -- CRS Report, *Cybersecurity: Authoritative Reports and Resources*, 25 Oct 2013
> Copy available at: <http://www.fas.org/sgp/crs/misc/R42507.pdf>
>
> ---
>
> "*As long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk."*
>
> -- Rand Report, "Cyberdeterrence and Cyberwar," by Martin C. Libicki (2009)
>
> ---
>
> "*America is being 'invaded,' every hour of every day, by hostile forces using computers…from minor annoyances by young computer hackers to those from sophisticated nations and could cost American lives…the irony is that this new threat stems from the technical sophistication that helps make the US military the strongest in the world."*
>
> -- John Randle, Voice of America, *Future War in Cyberspace*
>
> ---

U.S. military networks *"are constantly under attack. They are probed thousands of times a day. They are scanned millions of times a day. And the frequency and sophistication of attacks are increasing exponentially."*

"The power to disrupt and destroy, once the sole province of nations, now also rests with small groups and individuals, from terrorist groups to organized crime, from hacker activists to teenage hackers, from industrial spies to foreign intelligence services."

-- William Lynn, Deputy Secretary of Defense
(as quoted in "In Cyber War, Most of U.S. Must Defend Itself," by William Matthews, *DefenseNews*, 1 Feb 2010, p. 29)

"Forcing Cybersecurity into a simplified unitary framework limits our choices and underestimates the complexity of the most novel and serious disruptive threat to our national security since the onset of the nuclear age sixty years ago."

-- Michael Chertoff, Former US Secretary of Homeland Security & John M. McConnell, Former DNI
As quoted in *Securing Cyberspace: A new Domain for National Security*, 2012, p. 192

Cyber security within the military is daunting – *"The Department operates over 15,000 networks and 7 million computing devices across hundreds of installations in dozens of countries around the globe."*

-- Zachary J. Lemnios, Assistant Secretary of Defense for Research and Engineering, 20 March 2012
Testimony before the Senate Armed Services Committee hearing on Emerging Threats and Capabilities

---

"In the cyber realm, new exploits can render defenses that seemed effective obsolete in a matter of seconds. Given the speed with which cyber capabilities can be created and the relatively low cost for entry, the potential for possibly far-reaching technological surprise is very high."

-- Dr. James S. Perry, Director of Information Systems Analysis Center at Sandia National Laboratories, 20 March 2012. Testimony before the Senate Armed Services Committee hearing on Emerging Threats and Capabilities

---

"*Repeated cyber intrusions into critical infrastructure demonstrate the need for improved Cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."*

-- EO 13636, *Improving Critical Infrastructure Cybersecurity*, 12 Feb 2013

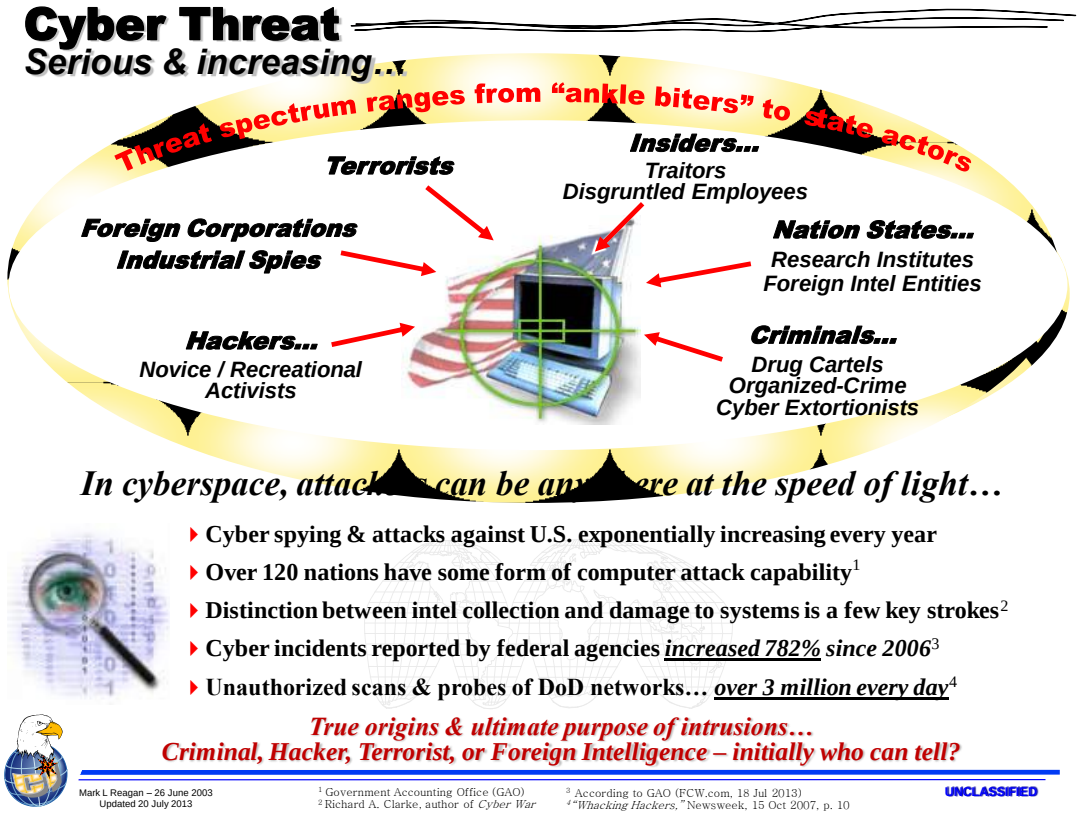
See the "The Comprehensive National Cybersecurity Initiative" at:
<http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>

Also see Committee on National Security Systems, *National Information Assurance (IA) Glossary*, April 2010, <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>

Also see P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know* (2014)

Cyberattacks are possible only because systems have flaws.

Cyber Threat. The cyber threat is characterized in terms of three classes of increasing sophistication: 1) those practitioners who rely on others to develop the malicious code, 2) those who can develop their own tools to exploit publically known vulnerabilities as well as discovering new vulnerabilities, and 3) those who have significant resources and can dedicate them to creating vulnerabilities in systems. (Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Jan 2013) Also see *cyber attack*, cyber espionage, *cyber threat investigation.*



Cyber Threat

"In the United States, we define cyber threats in terms of cyber attacks and cyber espionage. A cyber attack is a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data. It might range from a denial-of-service operation that temporarily prevents access to a website, to an attack on a power turbine that causes physical damage and an outage lasting for days. Cyber espionage refers to intrusions into networks to access sensitive diplomatic, military, or economic information."

-- James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013

The cyber threat the United States faces is increasing in severity and is accessible to a wide range of enemies. *"Most of what we see today is exploitation -- that's theft, stealing secrets, either commercial or military… we know the tools exist to destroy things, to destroy physical property, to destroy networks, to destroy data, maybe even take human lives."*

-- Deputy Defense Secretary William J. Lynn III in a television interview on PBS 14 July 2011

The FBI has noted three primary categories of *cyber threat actors*:

"[1] organized crime groups that are primarily threatening the financial services sector, and they are expanding the scope of their attacks;
[2] state sponsors—foreign governments that are interested in pilfering data, including intellectual property and research and development data from major manufacturers, government agencies, and defense contractors; and
[3] increasingly there are terrorist groups who want to impact this country the same way They did on 9/11 by flying planes into buildings. They are seeking to use the network to challenge the United States by looking at critical infrastructure to disrupt or harm the viability of our way of life."

-- FBI, *The Cyber Threat: Part 1: On the Front Lines With Shawn Henry,* 27 March 2012, http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712/shawn-henry_032712

Foreign intelligence and security services have penetrated numerous computer networks of US Government, business, academic, and private sector entities. Most detected activity has targeted unclassified networks connected to the Internet, but foreign cyber actors are also targeting classified networks.

-- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 12 March 2013, p. 2

[C]omputer network 'exploitation' and 'disruption' activities such as denial-of-service attacks will continue. …the likelihood of a 'destructive' attack that deletes information or renders systems inoperable will increase as malware and attack tradecraft proliferate.

-- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 29 January 2014, p. 1

Cyber Threat Investigation. Any actions taken within the United States, consistent with applicable law and presidential guidance, to determine the identify, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more cyber threat groups or individuals. (NSPD-54 / HSPD-23)

-- Also, actions taken, consistent with applicable law and Presidential guidance, to determine the identify, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more FIEs [Foreign Intelligence Entities], that has attempted to penetrate or has, in fact, penetrated a DoD, IC, or DIB [defense industrial base] information system. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010 with change 1 dated 16 Oct 2013)

Attribution is a major problem in the cyber realm

"***Who: Attribution…*** blurry lines between various types of malicious activity in cyberspace may make it difficult for investigators to attribute an incident to a specific individual or organization. Criminal attribution is a key delineating factor between cybercrime and other cyber threats. When investigating a given threat, law enforcement is challenged with tracing the action to its source and determining whether the actor is a criminal or whether the actor may be a terrorist or state actor posing a potentially greater national security threat."

-- CRS Report R42547, *Cybercrime: Conceptual Issues for Congress & U.S. Law Enforcement*, 23 May 2012

"The damage caused by malicious activity in cyberspace is enormous and unrelenting. Every year, cyber attacks inflict vast damage on our Nation's consumers, businesses, and government agencies. This constant cyber assault has resulted in the theft of millions of Americans' identities; exfiltration of billions of dollars of intellectual property; loss of countless American jobs; vulnerability of critical infrastructure to sabotage; and intrusions into sensitive government networks."

-- Senator Sheldon Whitehouse, 14 April 2011

James Clapper, Director of National Intelligence, noted that *"[t]wo of our greatest strategic challenges regarding cyber threats are: (1) the difficulty of providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, definitively attributing them [emphasis added], and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber attacks; and (2) the highly complex vulnerabilities associated with the IT supply chain for US networks."*

-- Office of the Director of National Intelligence, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence,* 31 Jan 2012, p. 8.

Attribution in cyber is always going to be difficult.
Missiles come with a return address, cyber attacks do not.

-- William Lynn, US Deputy Secrete of Defense
Interview Defense News, 18 July 2011

Cyber Threats. Natural or man-made incidents (intentional or unintentional) that would be detrimental to the cyber domain, or which are dependent on or operate through cyberspace/cyber domain. (Cyber Threats to National Security, Symposium Five, 2011) Also see *cyber threat*.

In the United States, we define cyber threats in terms of cyber attacks and cyber espionage.
-- Hon. James R. Clapper, DNI, Statement for the Record Worldwide Threat assessment of the US Intelligence Community, Senate Committee on Armed Services,18 Apr 2013

Cyber-Terrorism. A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda. (FBI)

-- Also, cyberterrorism: the unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people to further political or social objectives. Actors who engage in these kinds of activities are commonly referred to as cyber terrorists. (Cyber Threats to National Security, Symposium Five, 2011)

Cybercrime. Crime involving use of a computer system or network.

Typically involves data theft (e.g., credit cards, etc.) or transmission (e.g., child porn).

_____

"*Cybercriminals also threaten US economic interests. They are selling tools, via a growing black market, that might enable access to critical infrastructure systems or get into the hands of state and nonstate actors. In addition, a handful of commercial companies sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products. Foreign governments already use some of these tools to target US systems.*"
-- Hon. James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013

Cyberexploitation. Penetration of an adversary's computer system or network to seize information. (National Research Council - 2009)

Essentially an intelligence-gathering activity, e.g., Ghostnet, Operation Aurora.

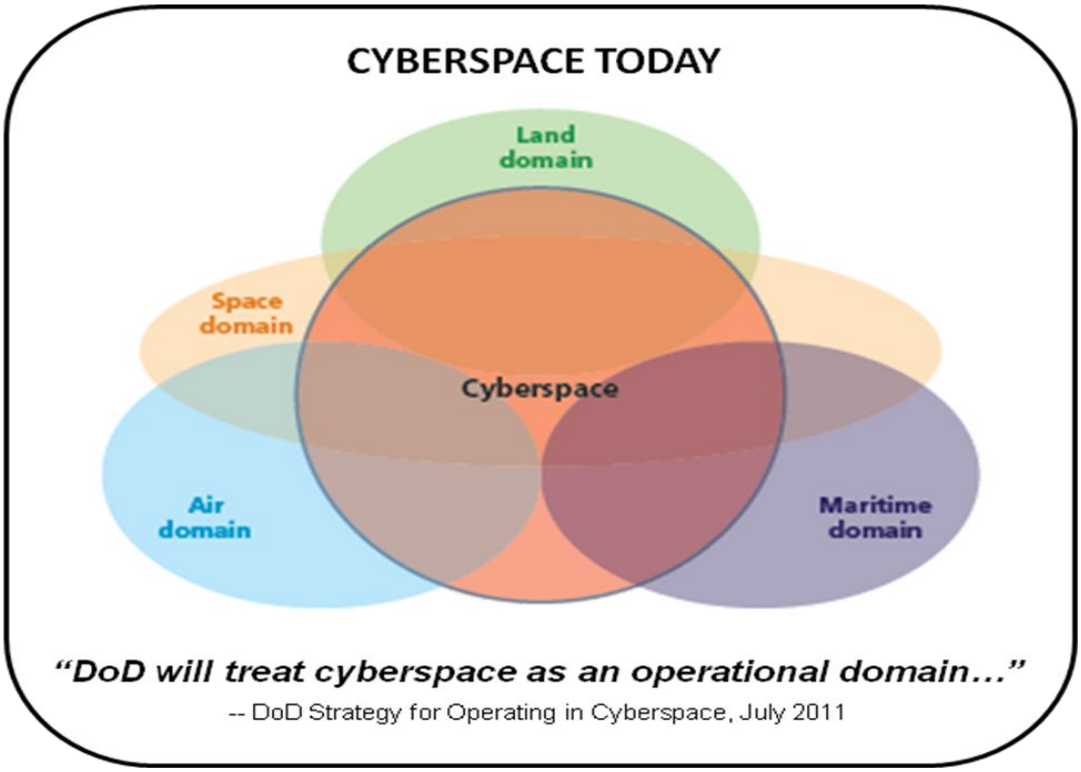
Cyberspace. A global domain within the information environment consisting of the independent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02 and JP 3-12, Cyberspace Operations, 5 Feb 2012) Also see *cyberspace domain*.

-- Also, the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks, and embedded possessors and controllers. (PPD-20, U.S. Cyber Operations Policy (U), 16 Oct 2012)

-- Also, the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded possessors and controllers in critical industries. (NSPD-54 / HSPD-23, 8 Jan 2008)

-- Also, the range of information and resources available through computer networks – especially the Internet. (ODNI Cyberspace Initiative)

-- Also, a global domain within the information environment consisting of the independent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)



-- Adapted from RAND Graphic

In cyberspace, the war has begun…

Cyberspace is a decentralized domain characterized by increasing global connectivity, ubiquity, and mobility, where power can be wielded remotely, instantaneously, inexpensively, and anonymously. This environment presents enormous challenges and unprecedented opportunities…

Cyberspace is a domain that requires man-made technology to enter and exploit. Effects of cyberspace operations can occur simultaneously in many places and they can be precise, broad, enduring and transitory.

Challenges -- Our national security is inextricably linked to the cyberspace domain, where conflict is not limited by geography or time. Cyberspace crosses geographic and jurisdictional boundaries. The expanding use of cyberspace places United States' interests at greater risk from cyber threats and vulnerabilities. Cyber actors can operate globally, within our own borders, and within the borders of our allies and adversaries. The complexity and amount of activity in this evolving domain make it difficult to detect, interdict, and attribute malicious activities.

Threats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies. On the flip side -- cyberspace offers DoD unprecedented opportunities to shape and control the battlespace to achieve national objectives.

Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication. Indeed, adversaries have already taken advantage of computer networks and the power of information technology not only to plan and execute savage acts of terrorism, but also to influence directly the perceptions and will of the U.S. Government and the American population.

-- *The Joint Operating Environment 2010*, US Joint Forces Command

---

"[I]n cyberspace some malicious actors consider that no boundaries exist between military and civilian targets."

-- Congressional Research Service, Report RL32114 (29 Jan 2008)

"…the United States will respond to hostile acts in cyberspace, as we would to any other threat to our country."

-- International Strategy for Cyberspace, May 2011

"Cyberspace is contested every day, every hour, every minute, every second. [The internet] lowers the bar for entry to the espionage game, both for states and for criminal actors. The threat is complex and not easily addressed by just building the security walls higher and higher."

-- Iain Lobban, Chief GCHQ, 13 October 2010

"The myth persists that the United States hasn't been invaded since 1812. I'd like to inform you otherwise. And that is the fact that invasion through cyberspace is now a daily occurrence."

-- Frank Ciffullo, Center for Strategic & International Studies

---

"The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War"

-- Defense Science Board, Jan 2013

For additional information see:

-- DoD website at: <http://www.defense.gov/home/features/2011/0411_cyberstrategy/>
-- *International Strategy for Cyberspace*, May 2011
-- *DoD Strategy for Operating in Cyberspace* (U), May 2011 (classified version)
-- *DoD Strategy for Operating in Cyberspace*, July 2011 (unclassified version)
Copy available at <http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf>
-- ONCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011,* October 2011
-- DSS, *Targeting US Technologies: A Trend Analysis of Reporting from Defense Industry – 2012*
-- Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Jan 2013
Copy at: <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

Cyberspace Domain. A domain characterized by the use of electronics and electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. (Previously defined in DoDI S-5240.17, CI Collection, 12 Jan 2009)

Cyberspace Operations. The employment of cyber capabilities where the primary purpose is to achieve military objectives in or through cyberspace. (JP 1-02; and JP 3-0, Joint Operations, 11 Aug 2011)

Cybervetting. Checking blogs, social media sites, and other Internet-based sources to identify issues of security concern applicable to people holding or seeking positions of trust. (PERSEREC; accessed 9 Jan 2013)

PERSEREC's initial effort regarding cybervetting entailed working with the national security and law enforcement communities to identify the primary legal, privacy, policy, and procedural considerations that should be taken into account when establishing a cybervetting program. Pilot projects are planned to test the efficacy of cybervetting. In addition, a series of CyberPsychology studies are exploring how certain types of activities in cyber environments, such as Second Life, can spill over into negative affects [sic] on workplace reliability, judgment, and other areas of personnel security concern.

-- PERSEREC at <http://www.dhra.mil/perserec/currentinitiatives.html#Cyber> (accessed 9 Jan 2013)

D ==========

Damage. A loss of friendly effectiveness due to adversary action. Synonymous with harm. (DSS Glossary)

Damage Assessment. [In intelligence usage,] a determination of the effect of a compromise of classified information on national security. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007)

-- Also, the analysis of the impact on national security of a disclosure of classified information to an unauthorized person. (IC Standard 700-1, 4 Apr 2008)

-- Also, systematic analysis that determines the impact of a compromise of classified information on the national security of the United States. (CI Community Lexicon)

-- Also, systematic, comprehensive examination of an intentional and/or inadvertent compromise of classified or sensitive information. (ONCIX, Damage Assessment Guide (U), 21 Mar 2008)

> See ONCIX's *Damage Assessment Guide* - October 2009 (U) for a standardized framework and outline of the processes and procedures involved in national-level damage assessment activity.

Damage to the National Security. Harm to the national defense or foreign relations of the United States from unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information. (EO 13526, Classified National Security Information, 29 Dec 2009)

Danger Signals. Prearranged signals or marks on walls, posts, etc., [used] as a communication system between agents or [case] officers to indicate that the opposition or active enemy is nearby, has been tipped off, or has the area under surveillance. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

Dangle. A person controlled by one intelligence service who is made to appear as a lucrative and exploitable target to an opposing intelligence service. (HDI Lexicon, April 2008) Also see *dangle operation; double agent; penetration; provocation.*

-- Also, an asset placed within the professional or personal view of a FIS [Foreign Intelligence Service] officer or agent with the intention of observing the actions of and possibly being recruited by the FIS. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, counterespionage terminology for the process of presenting an individual to a foreign intelligence service in a manner as to encourage his recruitment as an agent; as "to dangle" or a dangle operation. (CIA in D&D Lexicon, 1 May 2002)

-- Also, an individual who deliberately appears available for recruitment. (Encyclopedia of Espionage, Spies, and Secret Operations, 3rd Edition, 2012)

> ***If you wait for the enemy to come to you, you may not know when he does.***
>
> *…If the fish do not swim into your net, you have to give them a lure, a provocation, something that looks like a juicy worm but that has a hook in it.*
>
> -- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)
>
> ---
>
> *…dangles were a doubled-edged sword, whose specter overshadowed every decision to recruit agents we believed to be real. …Fear of them caused both the KGB and CIA to turn away countless volunteers.*
>
> -- Victor Cherkashin, Former KGB Intelligence Officer and author of *Spy Handler* (2005)

Dangle Operation. An operation in which an enticing intelligence target is dangled in front of an opposition service in hopes they will think him or her a bona fide recruit. The dangle is really a double agent. (Spy Dust) Also see *dangle; double agent penetration; provocation*

Database. *Within DoD: None – term removed from JP 1-02.*

> Previously defined in JP 2-0, Joint Intelligence (22 Jun 2007) as: information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files.

Data Mining. A program involving pattern-based queries, searches or other analyses of I or more electronic databases, where -- (a) a department or agency of the Federal Government. or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; (b) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual. or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (c) the purpose of the queries, searches, or other analyses is not solely- (i) the detection of fraud, waste, or abuse in a Government agency or program; or (ii) the security of a Government computer system. (Data Mining Reporting Act, §804(b)(I)(A))

> *This definition limits covered activities to predictive, pattern-based data mining, which is significant because analysis performed within the ODNI and its constituent elements for counterterrorism and similar purposes is often performed using various types of "link analysis" tools.*
>
> *Unlike "pattern-based" tools, these link analysis tools start with a known or suspected terrorist or other subject of foreign intelligence interest and use various methods to uncover links between that known subject and potential associates or other persons with whom that subject is or has been in contact. The Data Mining Reporting Act does not include such analyses within its definition of "data mining" because such analyses are not "pattern-based."*
>
> -- ODNI 2009 Data Mining Report
>
> ---
>
> *Data mining is finding key pieces of intelligence that may be buried in the mass of data available. Data mining uses automated statistical analysis techniques to search for the specific data parameters that intelligence professionals predetermine will answer their information requirements. Data mining can help organize the mass of collected data.*
>
> -- ADRP 2-0, *Intelligence*, Aug 2012, p. 3-6

DCAT. See *Defense Counterintelligence Anomalies Team*.

DCII. See *Defense Central Index of Investigations*.

DCIP. See *Defense Critical Infrastructure Program*.

DCIP Assessment. A comprehensive assessment of a Defense Critical Asset consisting of an in-depth look based on current DoD DCIP Assessment benchmarks. (CJCSI 3209.01, Defense Critical Infrastructure Program, 9 Jan 2012) Also see *Defense Critical Infrastructure Program.*

DCIP CI Coverage Plan. A formally coordinated, comprehensive plan that outlines the CI support to DCA and Tier 1 TCA protection. A DCIP CI coverage plan is prepared by the critical asset manager and identifies the appropriate support of DoD, non-DoD, and other CI elements necessary to the development and validation of DoD-wide CI support to the DCIP. (DoDI 5240.19, CI Support to DCIP, 31 Jan 2014). Also see *Defense Critical Infrastructure Program.*

> If a "CI Support Plan (CISP)" has been developed for the DCIP organization and meets the requirements of the DCIP CI Coverage Plan IAW DoDI 5240.19 (Table 2) then another plan is not required. For CISPs see DoD Instruction 5240.24, *Counterintelligence Activities Supporting RDA*.

DCIP Threat Assessment. A compilation of strategic intelligence information incorporating multi-faceted threats facing DCAs [Defense Critical Assets] and Tier 1 TCAs [Task Critical Assets]. DCIP threat assessments address threats posed to DCAs from domestic and transnational terrorist elements, foreign intelligence and security services, and weapons of mass destruction. (DoDI 5240.19, CI Support to DCIP, 31 Jan 2014) Also see *Defense Critical Infrastructure Program.*

Dead Drop. A clandestine location for transferring material to or from an agent or asset. (National HUMINT Glossary)

-- Also, a place where a person might leave communications or material in concealment for another person. It serves as a cutout between human elements of a clandestine organization. (AFOSI Instruction 71-101, 6 Jun 2000)

-- Also, a place, unattended by witting individuals, to which communications, materials, or equipment can be left by one individual and from which they can be taken by another individual without either meeting or, ordinarily, seeing one another. Also called a dead letter box, or simply drop. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, a prearranged hidden location used for the clandestine exchange of packages, messages, and payments, which avoids the necessity of an intelligence officer and an agent being present at the same time. (FBI -- Affidavit: USA vs. Robert Philip Hanssen, 16 Feb 2001)

-- Also, a secret location where materials can be left in concealment for another party to retrieve. This eliminates the need for direct contact in hostile situations. (CI Centre Glossary)

-- Also, a preferred means of covert communications in denied areas, separates the agent and handler [case officer] by time, but carries the risk of leaving the package unattended in an environment that could change without warning. (Spycraft, p. 61)

-- Also, pre-cased hiding places used by intelligence services to conduct [clandestine] exchanges with agents. (James M. Olson, Fair *Play: The Moral Dilemmas of Spying*, 2006)

-- Also, a predetermined secret location where [case] officers and agents leave messages and other items for undetected collection by other parties. (*Encyclopedia of the CIA*, 2003)

-- Also, a clandestine communications technique, the dead drop allows agents to exchange messages and other items without the need for a meeting that might attract the attention of hostile surveillance. The dead drop is usually an innocuous, prearranged site where a package or film canister can be secreted temporarily so it can be recovered by the addressee. Ideally, the location is sufficiently innocent to enable both parties to visit it, at different times, without compromising themselves. The use of dead drops is standard tradecraft for espionage professionals, and is usually associated with a remote signaling arrangement so both sides can indicate to the other when a particular drop is ready for servicing. The objective is to obviate the need for personal contact that in denied areas is high risk. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Eliminates the need for direct contact…

In intelligence usage, dead drops are used as a clandestine cut-out to avoid personal meetings which can draw attention to the connection between an intelligence officer/agent handler and an agent/asset. As a rule, a dead drop site is not used more than once.

For a detailed description of dead drops and concealment devices, see *Spycraft*, pp. 388-400.

Debriefing. Systematically covering topics and areas with a voluntary source who consents to a formal interview. (Educing Information - Interrogation: Science and Art, Dec 2006) Also see *strategic debriefing*; *educing information; elicitation; intelligence interrogation; interrogation; interview*.

-- Also, the systematic questioning of individuals to procure information to answer specific collection requirements by direct and indirect questioning techniques. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010; also Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

-- Also, [in detainee operations] the process of using direct questions to elicit intelligence information from a cooperative detainee to satisfy intelligence requirements. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

-- Also, interviewing under other than hostile conditions, of an individual who has completed an intelligence assignment or who has, through observation, participation, or personal knowledge, information of intelligence or counterintelligence value or significance. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence debriefings are forms of overt collection entailing the questioning of human sources to satisfy CI requirements.

Debriefings are conducted to obtain CI information acquired by the Component's own employees in the course of their duties. CI debriefings are also used to exploit the opportunity presented by walk-ins and other persons who contact CI elements to provide information of potential CI interest.

-- DoDI S-5240.17, (U) *CI Collection Activities*, 14 Mar 2014 (encl 3, para 2c(1))

Also see Appendix C "Counterintelligence Collection Methods (U)" in JP 2-01.2, *Counterintelligence and Human Intelligence in Joint operations* (U), 16 Mar 2011 w/ chg 1 dated 26 Aug 2011.

Debriefing Operations. Operations conducted to debrief cooperating sources may include refugees, émigrés, displaced persons (DPs), local populace, friendly forces, members of U.S. and foreign governmental and non-governmental organizations, as well as U.S. and foreign personnel employed within the academic, business, or scientific communities. The source may or may not be in custody, and their willingness to cooperate need not be immediate or constant. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Decentralized Execution. Delegation of execution authority to subordinate commanders. (JP 1-02)

Deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006) Also see *counterdeception; deception means; deception in support of OPSEC; denial, military deception.*

-- Also, deliberately manipulating information and perceptions in order to mislead. (Foreign Denial & Deception Committee, 30 Mar 2006)

-- Also, an action intended by an actor to influence the perceptions, decisions, and actions of another. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

-- Also, any attempt—by words or actions—intended to distort another person's or group's perception of reality. (Textbook of Political-Military Counterdeception: Basic Principles & Methods, August 2007)

Deception is a fundamental ingredient of military art.
All warfare is based on deception.
-- Sun Tzu (400-320 B.C.)

Deception is the distortion of perceived reality

"Deception is an instrument of policy…. [It] must be orchestrated to succeed."

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

Analysts should routinely consider that their information base is susceptible to deception-- *the distortion of perceived reality.*

Richard Heuer, author of *Psychology of Intelligence Analysis,* notes that analysts often reject the possibility of deception because they see no evidence of it. He then argues that rejection is not justified under these circumstances. If deception is well planned and properly executed, one should not expect to see evidence of it readily at hand. Rejecting a plausible but unproven hypothesis too early tends to bias the subsequent analysis, because one does not look for the evidence that might support it. The possibility of deception should not be rejected until it is disproved or, at least, until a systematic search for evidence has been made and none has been found.

See *Deception 101 –A Primer on Deception* (2004) by Joseph W. Caddell; available online at: <http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=589>

Also see *Textbook of Political-Military Counterdeception: Basic Principles & Methods* (2007) by Barton Whaley, published by the National Defense Intelligence College.

O, what a tangled web we weave,
When first we practise to deceive!

-- Sir Walter Scott, *Marmion* (1808)

MASKIROVKA

According to a declassified 1983 White House National Security Decision Directive --

The Soviet Union… doctrine of "maskirovka" [called] for the use of camouflage, concealment and deception (CC&D) in defense-related programs and in the conduct of military operations. They define maskirovka as a set of measures to deceive, or mislead, the enemy with respect to Soviet national security capabilities, actions, and intentions. These measures include concealment, simulation, diversionary actions and disinformation.

-- National Security Decision Directive 108, *Soviet Camouflage, Concealment and Deception,* 12 Oct 1983 (declassified). Copy available at <http://www.fas.org/irp/offdocs/nsdd/nsdd-108.pdf>

Deception Channel. A means by which controlled information can be reliably transmitted to the target. (CIA in D&D Lexicon, 1 May 2002)

Feeding the enemy self-destructive information is the oldest of arts…. A successful feed should not be considered an operation in and of itself, but rather the fruit of a long fight for control over a channel of information. Therein lies the art.

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 349

Deception In Support of OPSEC (DISO). A military deception activity that protects friendly operations, personnel, programs, equipment, and other assets from FISS [Foreign Intelligence Security Service] collection. (DoDI S-3604.01, Department of Defense Military Deception, 11 Mar 2013) Also see *deception, military deception*.

The intent of DISO is to create multiple false indicators to confuse FISS, make friendly intentions harder to interpret by FISS, or to limit the ability of FISS to collect accurate intelligence on friendly forces.

DISOs are not targeted against adversary military, paramilitary, or violent extremist organization decision-makers with the intent of eliciting a particular decision or reaction, but are targeted against a FISS or an adversary's intelligence collectors to protect friendly forces by masking, simulating, or dissimulating signatures and observables needed to ascertain friendly capabilities, intent, or vulnerabilities.

Deception Means. Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: 1) physical means -- activities and resources used to convey or deny selected information to a foreign power; 2) technical means -- military material resources and their associated operating techniques used to convey or deny selected information to a foreign power; and 3) administrative means -- resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

-- Also, the vehicles or resources for conveying the deception story or deception-related information directly or indirectly to the target. These generally consist of sources accepted by the target as reliable or believable. Deception means have been subdivided into: physical, technical, administrative, and special means. (CIA in D&D Lexicon, 1 May 2002)

Deception Target. The adversary decisionmaker with the authority to make the decision that will achieve the deception objective. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

Decipher. Convert enciphered text to plain text by means of a cryptographic system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Declared. An individual or action whose intelligence affiliation is disclosed. (HDI Lexicon, April 2008)

-- Also, an officer, asset, agent, or action whose Agency affiliation is formally identified to a foreign intelligence or security service, government or organization, or other USG entity. (National HUMINT Glossary)

Declassification. The authorized change in the status of information from classified information to unclassified information. (EO 13526, Classified National Security Information, 29 Dec 2009 and DoD IG Evaluation Guide, 22 Jan 2013)

Deconfliction. The process of sharing information regarding collection between multiple agencies to eliminate potential duplication of effort, multiple unintended use of the same source, or circular reporting. (Previously in DoDI S-5240.17, CI Collection, 12 Jan 2009)

Decoy. An imitation in any sense of a person, object, or phenomenon which is intended to deceive enemy surveillance devices or mislead enemy evaluation. (JP 1-02).

Decode. Convert encoded text to plain text by means of a code. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Decrypt. Generic term encompassing decode and decipher. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Deduction. [One of the four basic types of reasoning applied to intelligence analysis,] it is the process of reasoning from general rules to particular cases. Deduction may also involve drawing out or analyzing premises to form a conclusion. (Cited in (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *abduction; induction; scientific method.*

For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003) and *Critical Thinking and Intelligence Analysis* by David Moore, JMIC Press (2006).

Deep Cover. A cover for status designed to withstand close scrutiny by the opposition or through due diligence. (National HUMINT Glossary)

Defection. Conscious abandonment of loyalty, duty, and principle to one's country. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, conscious (mental and/or physical) abandonment of loyalty, allegiance, duty, and principle to one's country. (ICS Glossary)

Defector. A person who has consciously abandoned loyalty to his country and who possess intelligence information of value to another country or countries. (CI Community Lexicon)

-- Also, a person who, for political or other reasons, has repudiated his country and may be in possession of information of interest to the US Government. (ICS Glossary)

-- Also, a person of any nationality, usually from a country whose interests are hostile or inimical to the U.S., who has escaped from the control of his or her country, is unwilling to return to that country, and is of special value to the U.S. Government because: he or she is able to add valuable new or confirmatory information to existing U.S. intelligence knowledge; he or she is, or has been, of operational or political value to a U.S. department or agency; or the defection can be psychologically exploited to the advantage of the U.S. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

"Next to penetrations (moles), defectors are your best weapon against alien intelligence services."

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

An act of treason – a *"defector is an individual who has committed treason, a person who first accepted identification with a regime and then betrayed his allegiance to cooperate with a hostile foreign intelligence service."*

-- Wilhelm Marbes, "Psychology of Treason," in *Studies of Intelligence*, vol. 30, no. 2 (Summer 1986), pp. 1-11. Originally classified "Secret" [declassified].

Defectors *"…certainly the next best thing to penetration. But defector information was finite: it ceased the moment the defector stepped out of his office and crossed to our side."*

-- Richard Helms, *A Look Over My Shoulder: A Life in the Central Intelligence Agency*(2003)

"It's the job of intelligence agencies to distinguish between defectors who claim to have something to say and defectors who are lying and they obviously didn't do their job. The Germans didn't, and we didn't."

-- Richard Perle regarding the Iraqi defector CURVEBALL, 15 Feb 2011

"*Sometimes the bona fides of a defector remain in dispute for many years, as is the case of Yuri Nosenko, who defected from the U.S.S.R. soon after the assignation of President John F. Kennedy in 1963."*

-- Loch K. Johnson and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies* (2008), p.299

Defector in Place. See *recruitment-in-place*.

Defense Attaché. See *Senior Defense Official / Defense Attaché (SDO/DATT).*

Defense Attaché Office (DAO). An organizational element of the U.S. diplomatic mission through which the Defense Attaché System conducts its mission and to which may be attached or assigned such other military detachments or elements as the Secretary of Defense may direct. (DoDI C-5105.32, Defense Attaché System, 18 Mar 2009) Also see *Senior Defense Official / Defense Attaché (SDO/DATT).*

-- Also, a DoD organization established as part of the U.S. diplomatic mission, through which the mission of the Defense Attaché System is accomplished. (DoDI C-5105.81, Implementing Instructions for DoD Operations at U.S. Embassies, 6 Nov 2008)

Defense Central Index of Investigations (DCII). An automated DoD repository that identifies investigations conducted by DoD investigative agencies. DCII does not contain eligibility information. (IC Standard 700-1, 4 Apr 2008)

> Effective 26 July 2010, DCII is operated and maintained by the Defense Manpower Data Center (DMDC) on behalf of the DoD components and USD(I). See website at: <https://dcii.dmdc.osd.mil>
>
> Access to DCII is normally limited to DoD and other federal agencies that have adjudicative, investigative and/or counterintelligence missions. Although the DCII database is physically maintained by the DMDC the data it contains is the responsibility of the contributing agencies.

-- Also, a centralized database, organized in a searchable format, of selected unique identifying information and security clearance data utilized by security and investigative agencies in the DoD, as well as selected other Federal agencies, to determine security clearance status and the existence or physical location of criminal and personnel security investigative files. The DCII database is physically maintained by the Defense Manpower Data Center; however, the data that it contains is the responsibility of the contributing agencies. (DoDI 5505.7, Titling & Indexing Subjects of Criminal Investigations in DoD, 27 Jan 2012)

-- Also, an alphabetical index of personal names and impersonal titles that appear as subjects of incidents in investigative documents held by the criminal, counterintelligence, fraud, and personnel security investigative activities of the Defense Investigative Service (DIS), the Defense Criminal Investigative Service (DCIS), and the NSA. DCII records will be checked on all subjects of DOD investigations. (AR 380-67, Personnel Security Program, 24 Jan 2014)

Defense Clandestine Service (DCS). The primary DoD element authorized to conduct clandestine human intelligence (HUMINT) operations is response to high priority national-level intelligence requirements as identified by the USD(I). DCS shall operate worldwide, to include high CI threat and politically sensitive environments. Also see *National Clandestine Service*.

> See <http://www.defense.gov/news/newsarticle.aspx?id=116064>
>
> Also see classified SECDEF memorandum, subj: (U) Established of the Defense Clandestine Service, 20 Apr 2012

-- Also, [a DoD organization that] conducts human intelligence (HUMINT) operations to answer national-level defense objectives for the President, the Secretary of Defense, and senior policymakers. The civilian and military workforce of the DCS conducts clandestine and overt intelligence operations in concert with the Central Intelligence Agency, the Federal Bureau of Investigation, and our Military Services to accomplish their mission in defense of the Nation. (www.dia.mil/dcs/; accessed 5 Sep 2013)

Defense Combating Terrorism Center (DCTC). A functional center with the Defense Intelligence Agency focused on terrorism intelligence and related issues within DoD.

> Previously known as the Joint Intelligence Task Force for Combating Terrorism (JITF-CT). In the fall of 2012, JITF-CT, the Joint Threat Finance Intelligence Office (JTFI), selected elements from the Defense CI & HUMINT Center, and DIA elements from the Counternarcotics and Western Hemisphere Office (CNW), transitioned into a single center -- *the Defense Combating Terrorism Center (DCTC).*
>
> DCTC is the lead national-level, all-source international terrorism intelligence effort within DoD. It is DoD's all-source national-level intelligence fusion center responsible for enabling DoD counter-terrorism and force protection operations. DCTC analytical assessments address terrorist capabilities, activities and intentions, including terrorist finance activity; see DoDD 2000.12 and DoDI 2000.12.
>
> DIA's Office of Counterintelligence(OCI) focuses on the intelligence apparatus and intelligence activities of international terrorists. In instances where the two missions intersect, DCTC and OCI collaborate and coordinate to ensure that DIA presents a timely, accurate, and consistent picture of the threat to U.S. forces and interests around the world.

Defense Counterintelligence and Human Intelligence Center (DCHC). Previously a center within the Defense Intelligence Agency (DIA) for counterintelligence and human intelligence that was established on 3 August 2008. DCHC was disestablished 28 Jan 2013 by Dir DIA (DIA Vision2020).

Defense Counterintelligence Anomalies Team (DCAT). [DoD CI element that] provides analysis and deconfliction of anomalies and identifies and shares CI insider threat trends with the DoD Components. The DCAT develops, promotes, expands, and improves upon insider threat detection efforts by reaching across organization boundaries and cultivating awareness of anomalies. (DoD Manual 5240.26, CI Insider Threat Program, *draft* 20 Nov 2013) See *anomalies*.

> DoD Components report and handle "anomalies" in accordance with DoDD O-5240.02 (Counterintelligence) and DoDI 5240.26 (Countering Espionage, International Terrorism, and the CI Insider Threat).

Defense Counterintelligence Components. DoD organizations that perform national and DoD counterintelligence and counterintelligence-related functions, including the DoD Counterintelligence Field Activity and the counterintelligence elements of the Military Departments, the Defense Agencies with organic counterintelligence, the Joint Staff, the Office of the Secretary of Defense, and the Combatant Commands. (DoDD 5143.01, USD/I, 23 Nov 2005)

Defense Counterintelligence Enterprise. The collective of DoD organizations authorized to conduct counterintelligence and related activities. See *Defense Counterintelligence Components,*

Defense Counterintelligence Knowledge Base (DCIKB). Serves the Defense CI enterprise as the web-enabled system for collecting observations of CI best practices and lessons learned, disseminating these across DoD CI, conducting triage for further action and facilitating change.

> *DCIKB collects, analyzes, manages, and disseminates knowledge gained through operational experience, exercises, and supporting activities in order to achieve higher levels of performance and to provide information and analysis on emerging issues and trends.*
>
> -- NIPRNet website at: <https//sss.mccll.usmc/dcikb>
>
> -- SIPRNet website at: <www.mccll.usmc.smil.mil/dcikb>

Defense Counterintelligence Manager. The official responsible who provides the centralized management of Defense CI Enterprise-wide activities. (DoDD O-5240.02, CI, 20 Dec 2007 with change 1 dated 30 Dec 2010)

> Director DIA serves as the *Defense CI Manager*, with responsibility to provided for central management of Defense CI Enterprise-wide activities (see O-DoDD 5240.02, para 5.3.1).
> This role is a corollary to the Director DIA's role as the Defense HUMINT Manager; see *Defense HUMINT Manager*.

Defense Courier Service (DCS). A global courier network for the expeditious, cost-effective, and secure distribution of highly classified and sensitive material.

> For DoD policy see DoDI 5200.33, *Defense Courier Operations (DCO),* 30 Jun 2011.
>
> DCS is under the United States Transportation Command (USTRANSCOM). On 15 November 2005, the Defense Courier Division (TCJ3-C) assumed operational control of worldwide defense courier stations and continues to synchronize the defense courier related activities of the USTRANSCOM staff. See web site at: <http://www.transcom.mil/dcd/> Note: DCS was previously known as the Armed Forces Courier Service (ARFCOS).

Defense Criminal Investigative Service (DCIS). The criminal investigative arm of the Inspector General (IG) of the Department of Defense responsible for investigating: terrorism; technology/munitions theft & diversion; cyber crime; substandard/defective products; and fraud, bribery & corruption. (DCIS – see website at <http://www.dodig.mil/INV/DCIS/index.html>)

Defense Criminal Investigative Organizations (DCIOs). The Defense Criminal Investigative Service, the U.S. Army Criminal Investigation Command, the Naval Criminal Investigation Service, and the Air Force Office of Special Investigations. (DoDI 5505.7, Titling & Indexing Subjects of Criminal Investigations in DoD, 27 Jan 2012)

Defense Critical Asset (DCA). An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *defense critical infrastructure program (DCIP); task critical asset (TCA)*.

Defense Critical Infrastructure (DCI). The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. DCI is a combination of task critical assets and defense critical assets. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *defense critical infrastructure program (DCIP).*

-- Also, Department of Defense and non-Department of Defense networked assets and facilities essential to project, support, and sustain military forces and operations worldwide. (JP 3-27, Homeland Defense, 29 Jul 2013)

-- Also, DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide. (DoD Strategy for Homeland Defense & Civil Support)

Defense Critical Infrastructure Program (DCIP). A DoD risk management program that seeks to ensure the availability of DCI [Defense Critical Infrastructure]. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *defense critical asset*, *defense critical infrastructure*, *task critical asset*.

> DCIP is an integrated risk management program designed to support DoD mission assurance. The purpose of the DCIP is to ensure the availability of Defense Critical Infrastructure in an all-threat and all-hazard environment.

> Key DCIP references include:
> -- DoD, *Strategy for Defense Critical Infrastructure*, March 2008
> -- DoDD 3020.40, *DoD Policy & Responsibilities for Critical Infrastructure*, 14 Jan 2010 with Chg 2
> -- DoDI 3020.45, *DCIP Management*, 21 Apr 2008
> -- DoDI 3020. 51, *Intelligence Support to DCIP*, 23 Jun 2011
> -- DoDI 5240.19, *CI Support to DCIP*, 31 Jan 2014
> -- DoD Manual 3020.45-M, Vol 3, *DCIP Security Classification Manual*, 15 Feb 2011
> -- CJCSI 3209.01, Defense Critical Infrastructure Program, 9 Jan 2012
> -- USSTRATCOM, *Strategic Mission Assurance Data System (SMADS) User Manual*, Apr 2013
>
> DCIP is a evolving program, see web site at: <http://dcip.dtic.mil/>

Defense Cyber Crime Center (DC3). The Defense Computer Forensics Laboratory and the Defense Computer Investigations Training Program comprise the Defense Cyber Crime Center. The forensics laboratory provides counterintelligence, criminal, and fraud computer-evidence processing, analysis, and diagnosis to DoD investigations. The investigations training program provides training in computer investigations and computer forensics to DoD investigators and examiners. AFOSI is the DoD executive agent for the Center. (DC3 web site)

> *DC3 sets standards for digital evidence processing, analysis, and diagnostics for any DoD investigation that requires computer forensic support to detect, enhance, or recover digital media, including audio and video. The Center assists in criminal, counterintelligence, counterterrorism, and fraud investigations of the Defense Criminal Investigative Organizations (DCIOs) and DoD counterintelligence activities. It also supports safety investigations and Inspector General and commander-directed inquiries.*

DC3 aids in meeting intelligence community document exploitation objectives from a criminal law enforcement forensics and counterintelligence perspective. DC3 provides computer investigation training to forensic examiners, investigators, system administrators, and any other DoD members who must ensure Defense information systems are secure from unauthorized use, criminal and fraudulent activities, and foreign intelligence service exploitation. DC3 remains on the leading edge of computer technologies and techniques through research, development, testing, and evaluation applied to digital evidence processing and computer forensic analysis; and by partnering with governmental, academic, and private industry computer security officials.

-- DC3 web site at <http://www.dc3.mil/dc3/dc3About.php>

Also see DoDD 5505.13E, *DoD Executive Agent for DC3*, 1 Mar 2010

Defense HUMINT Enterprise (DHE). The collective of DoD organizations authorized to conduct HUMINT and related activities under the centralized management of the DHM [Defense HUMINT Manager]. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013 w/ chg 1 dated 13 Jun 2013) Also see *Defense Clandestine Service*.

-- Also, the collective of DoD organizations authorized to conduct HUMINT and related activities. (DoDD S-5200.37, Management & Execution of Defense HUMINT (U), 9 Feb 2009)

Defense HUMINT Executor. The senior DoD intelligence official as designated by the head of each of the DoD components who are authorized to conduct human intelligence and related intelligence activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Defense HUMINT Manager (DHM). The Director DIA, as designated by the USD(I), is the official responsible for the centralized management of the DoD-wide HUMINT Enterprise. (DoDD S-5200.37, Management and Execution of Defense HUMINT (U), 9 Feb 2009)

-- Also, [Dir DIA] serve as the Defense HUMINT Manager (DHM) responsible for centralized management of the DoD-wide HUMINT enterprise, which is based on decentralized execution of HUMINT operations and related activities. (DoDD 5105.21, DIA, 18 Mar 2008)

Defense Industrial Base (DIB). The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. (JP 1-02 and JP 3-27, Homeland Defense, 29 Jul 2013)

DoD is responsible for critical infrastructure protection within the defense industrial base per PDD-21.

-- PDD-21, *Critical Infrastructure Security and Resilience*, 12 Feb 2013

The DIB Sector consists of government and private sector organizations that can support military operations directly; perform R&D; design, manufacture, and integrate systems; and maintain depots and service military weapon systems, subsystems, components, subcomponents, or parts—all of which are intended to satisfy U.S. military national defense requirements.

The government component of the DIB consists of certain laboratories, special-purpose manufacturing facilities, capabilities for production of uniquely military material such as arsenals and ammunition plats, and other services.

The private sector of the DIB consists of hundreds of thousands of independent, competing domestic and foreign companies and supply chains, delivering a vast array of products and services to DoD. DIB defense-related products and services equip, inform, mobilize, deploy, and sustain U.S. military and allied military forces worldwide. The DIB companies also deliver national security products and services to other federal agencies.

-- *Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010, p. 15

Defense Infrastructure Sector (DIS), A virtual association within the DCIP that traverses normal organizational boundaries and encompasses defense networks, assets, and associated dependencies that perform similar functions within the Department of Defense and are essential to the execution of the National Defense Strategy. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

IAW the DoDD 3020.40, the ten (10) *defense infrastructure sectors* are:

DIB Sector. The DoD, U.S. Government (USG), and private sector worldwide industrial complex with capabilities to perform research, development, and design and to produce and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

Financial Services Sector. The DoD, USG, and private sector worldwide network and its supporting infrastructure that meet the financial services needs of the Department of Defense across the range of military operations.

GIG Sector. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. It includes all owned and leased communications (commercial telecommunication infrastructure) and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 11103 of title 40, U.S.C. (Reference (n)).

Health Affairs Sector. The DoD, USG, and private sector worldwide healthcare network and its supporting infrastructure that meet the healthcare needs of DoD personnel across the range of military operations.

Intelligence Sector. Those DoD, USG, and private sector facilities, networks, and systems (assets) located worldwide or extra-terrestrially that conduct and support the collection, production, and dissemination of intelligence, surveillance, and reconnaissance information essential to the execution of the National Military Strategy. These assets encompass human intelligence, geospatial intelligence, measurement and signature intelligence, signals intelligence, open-source intelligence, and technical intelligence; counterintelligence collection, processing, and exploitation means; and all-source analysis and production, including the networks and means over which intelligence information is shared, communicated, and/or disseminated.

Logistics Sector. The DoD, USG, and private sector worldwide facilities, networks, and systems that support the provision of supplies and services to U.S. forces.

Personnel Sector. The DoD, USG, and private sector worldwide network that coordinates and supports personnel and human resource functions of DoD personnel.

Public Works Sector. The DoD, USG, and private sector worldwide network, including the real property inventories (environment, land, buildings, and utilities), that manages the support, generation, production, and transport of commodities (e.g., electric power, oil and natural gas, water and sewer, and emergency services) for and to the Department of Defense.

Space Sector. The DoD, USG, and private sector worldwide network, including both space- and ground-based systems and facilities, that supports launch, operation, maintenance, specialized logistics, and control systems for the space assets relied upon by the Department of Defense.

Transportation Sector. The DoD, USG, and private sector worldwide network that provides military lift support (surface, sea, and air) for U.S. military operations.

Defense Infrastructure Sector Lead Agents (DISLAs). Designated DoD officials and their respective defense sector organizations that perform defense infrastructure sector responsibilities. In coordination with their respective PSAs [Principal Staff Assistants], the DISLAs characterize their defense infrastructure sectors to identify functions, systems, interdependencies, and, ultimately, sector task critical assets that support Combatant Command, Military Department, and Defense Agency missions and sector functions. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Defense Intelligence. Integrated departmental intelligence that covers the broad aspects of national policy and national security and that intelligence relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, including any foreign military or military-related situation or activity which is significant to Defense policy-making or the planning and conduct of military operations and activities. Defense intelligence includes Active and Reserve military, strategic, operational, and tactical intelligence. (DoDD 5143.01, USD/I, 23 Nov 2005)

Defense Intelligence Agency (DIA). A Department of Defense combat support agency and a member of the United States Intelligence Community responsible for providing timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers. DIA is a major producer and manager of foreign military intelligence.

DIA is the nation's premier all-source military intelligence organization, providing the most authoritative assessments of foreign military intentions and capabilities to U.S. military commanders and civilian policymakers.

DIA's core mission resides in four intelligence competencies: all-source analysis, counterintelligence (CI), human intelligence (HUMINT), and measurement and signature intelligence (MASINT).

-- 2012-2017 Defense Intelligence Agency Strategy
Copy available at: <http://www.dia.mil/about/strategic-plan/2012-2017-DIA-Strategic-Plan.pdf>

Director DIA serves as the Defense HUMINT Manager responsible for centralized management of the DoD-wide HUMINT enterprise.

-- DoDI 5105.21, DIA, 18 Par 2008, para 6.2.1, p.5

DIA VISION2020
(IOC 28 Jan 2013)

VISION2020 [is] a transformational effort within DIA that redesigns and will fundamentally reposition the Agency to better address our nation's challenges. […]

VISION2020 aims to build a strong intelligence capability that will integrate and operationalize intelligence to ensure the security of the United States well into the 21st Century.

DIA's new center of gravity will be compromise of four Regional Centers (Asia/Pacific, Europe/Eurasia, Middle East/Africa, and the Americas) and one Functional Center (Defense Combating Terrorism Center DCTC))…

-- LTG Michael T. Flynn (USA), Director DIA

Defense Intelligence Analysis Program (DIAP). The DoD intelligence analysis community's resource allocation and prioritization program. The DIAP establishes the policies, procedures, responsibilities, and levels of analytic effort required to provide timely, objective, and cogent intelligence to warfighters, defense planners, and policymakers. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

-- Also, a DIA developed intelligence analysis production plan to enhance the ability of defense intelligence to focus on critical areas of national security interest, while maintaining a perspective on potential emerging threats. (DIA)

GDIP Directive No. 006, Subject: *Defense Intelligence Analysis Program*, 31 Oct 2005, establishes the policies, procedures, responsibilities, and levels of analytical effort required for Defense intelligence to provide timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers. Program guidance and roles and responsibilities posted on INTELINK at: <http://www.dia.ic.gov/admin/diap/index.htm>.

DIAP organizations are responsible for proactively producing intelligence on topics for which they are assigned responsibility IAW *Defense Intelligence Analysis Program Management Guidance*, 24 Feb 2010. DIA's Office of Counterintelligence is responsible for analyzing foreign intelligence activities and threats to US Defense and Service interests.

Defense Intelligence Components. All DoD organizations that perform national intelligence, Defense Intelligence, and intelligence-related functions, including: the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; the National Security Agency/ Central Security Service; and the intelligence elements of the Active and Reserve component of the Military Departments, including the United States Coast Guard when operating as a service in the United States Navy. (DoDD 5143.01, USD/I, 23 Nov 2005)

Defense Intelligence Enterprise. The Enterprise is comprised of intelligence, CI, and security components of the Joint Staff, Combatant Commands, Military Departments, and other Department elements, as well as those organizations under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD(I)). (DIA, 2012-2017 Defense Intelligence Agency Strategy)

Defense Intelligence Operations Coordination Center (DIOCC). [Defense-level entity that] integrates and synchronizes military and National Intelligence capabilities. The DIOCC plans, prepares, integrates, directs, manages and synchronizes continuous full-spectrum Defense intelligence operations in support of Combatant Commands. (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007) Also see *Joint Intelligence Operations Center (JIOC).*

> To be disestablished per SECDEF memo, subj: Track Four Efficient Initiatives Decision, 14 Mar 2011 (p.43) which directs the disestablishment the DIOCC and the transfer of its functions to the Joint Staff.

Defense Personnel Security Research Center (PERSEREC). A Department of Defense entity dedicated to improving the effectiveness, efficiency and fairness of the DoD personnel security system.

> PERSEREC was established in response to a recommendation by the DoD Security Review Commission (known as the Stilwell Commission), set up in the wake of the very damaging Walker espionage case, to improve DoD's personnel security system. In its 1985 report, the commission called for a personnel security research center to provide policymakers with an objective basis for policies and processes related to the security clearance system.
>
> PERSEREC report entitled, *Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008* (11 Aug 2009), provides summaries of 141 publicly reported espionage related cases. These cases demonstrate that loyal and conscientious employees continue to be the target of attempts by agents of foreign intelligence services to recruit them as sources of sensitive defense and intelligence information.
>
> Also see *Changes in Espionage by American: 1947- 2007*, PERSEREC Technical Report 08-5 (March 2008). PERSEREC reports available at: <http://www.dhra.mil/perserec/index.html>

Defense Security Enterprise (DSE). The organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard DoD personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences. This system of systems comprises personnel, physical, industrial, information, and operations security, as well as SAP security policy, critical program information protection policy, and security training. It addresses, as part of information security, classified information, including sensitive compartmented information, and controlled unclassified information. It aligns with counterintelligence, information assurance, foreign disclosure, security cooperation, technology transfer, export control, cyber security, nuclear physical security, chemical and biological agent security, antiterrorism, force protection, and mission assurance policy and is informed by other security related efforts. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012, w/ chg 1 dated 24 Apr 2013)

Defense Security Service (DSS). An agency of the Department of Defense (DoD) located in Quantico, Virginia with field offices throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction and control over DSS. DSS provides the military services, Defense Agencies, 24 federal agencies and approximately 13,000 cleared contractor facilities with security support services. (DSS Glossary) Also see *industrial security; National Industrial Security Program (NISP).*

DSS is the DoD Cognizant Security Office for industrial security, responsible for the DoD portion of the National Industrial Security Program (NISP) and, by mutual agreement, other U.S. Government departments and agencies; provides security education & training products and services; administers the industrial portion of the DoD Personnel Security Program (PSP); provides authorized counterintelligence services; and also supports DoD efforts to improve security programs and processes.

– DoDD 5105.42, *Defense Security Service*, 3 Aug 2010 (w/ chg 1 dated 31 Mar 2011)

On behalf of the Department of Defense and other U.S. Government Departments and Agencies, the DSS supports national security and the warfighter through our security oversight and education missions. DSS oversees the protection of U.S. and foreign classified information and technologies in the hands of industry under the National Industrial Security Program (NISP).
The NISP applies to all Executive Branch Departments and Agencies and to all cleared contractor facilities located within the United States (Para 1-102, NISPOM).

DSS elements include:

The Center for Development of Security Excellence (CDSE) is located in Linthicum, Md., and provides security education and training to DoD security professionals through formal classroom and distributed learning methodologies (i.e., computer-based, web-based and tele-training).

The Defense Industrial Security Clearance Office (DISCO), located in Fort Meade, Md., processes requests for industrial personnel security investigations and provides eligibility or clearance determinations for cleared industry personnel under the NISP.

See DSS web site at: <http://www.dss.mil/ > (SIPRNet at <https://www.dss.smil.mil>)

DSS has organic counterintelligence support. The DSS CI Directorate's mission is to identify unlawful penetrators of cleared U.S. defense industry and articulate the threat for industry and U.S. government leaders.

The CI Directorate's premier publication, *Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry*, analyzes suspicious contact reports (SCRs) from across the DIB describing suspicious foreign activity targeting U.S. personnel, technologies, and export-controlled products. This publication is available in both an unclassified and classified version. See DSS CI web page at: <http://www.dss.mil/isp/count_intell/index.html>

Timelines –

Jan 1972 – the Defense Investigative Service (DIS)—predecessor to DSS—established to consolidate DoD personnel security investigations (PSIs)
May 1993 – DIS established a counterintelligence office
Nov 1997 – DIS redesignated as the Defense Security Service (DSS) to reflect the agency's broader mission and functions, including industrial security, personnel security, security education and training missions.
Feb 2005 – DSS's personnel security investigations functions transferred to the Office of Personnel Management (OPM)
Dec 2007 – Director DSS named the functional manger for DoD security training

Defense Technology Base. All aspects of basic research plus those portions of applied research and technology development devoted to military systems in the generic sense. Prototyping and test and evaluation of specific technology enabled capabilities to prove the feasibility of a concept are also included. Development and engineering for specific military systems are NOT part of the defense technology base. (DoDI 3100.08, The Technical Cooperation Program (TTCP), 7 Aug 2012)

Defense Unknown Subject Team (DUST). DoD's Enterprise-level focal point and action center to resolve CI leads in which the subject's identity and/or specific affiliation with the DoD is not evident. (DoD FCIP Strategy FY 2013-2017) Also see *Unknown Subject; Unknown Subject Lead*.

-- Also, [DoD element that] serves as the DoD focal point to resolve CI leads in which the subject's identity and specific affiliation with DoD is not evident.

> DoD Components will report unknown subject leads to the DUST in accordance with DoD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence Insider Threat* (Enclosure 3, paragraph 1)

Defensive Counterintelligence Activities. Those counterintelligence activities designed to protect… personnel, operations, technology, and information against collection or exploitation by a foreign intelligence service, as contrasted with offensive counterintelligence activities, which are designed to attack the intelligence services of foreign adversaries by penetrating, collaborating, or conspiring with them to achieve that purpose. (AR 381-20, Army CI Program, 25 May 2010)

Defensive Cyberspace Operations (DCO). Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (JP 1-02 and JP 3-12, Cyberspace Operations, 5 Fen 2013)

Defensive Travel Security Briefing. Formal advisories that alert traveling personnel of the potential for harassment, exploitation, provocation, capture, entrapment, or criminal activity. These briefings, based upon actual experience when available, include recommended courses of action to mitigate adverse security and personal consequences. The briefings also suggest passive and active measures that personnel should take to avoid becoming targets or inadvertent victims in hazardous areas. (DSS Glossary)

Deliberate Compromise. The act, attempt, or contemplation of intentionally conveying classified documents, information, or material to any unauthorized person, including public disclosure, or the intentional misuse or mishandling of classified information, (AR 381-20, Army CI Program, 25 May 2010)

Delimitations Agreement. Common term for the DoD/Department of Justice Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation. (AR 381-20, Army CI Program, 25 May 2010)

Demarche. An official protest delivered through diplomatic channels from one government to another. (Words of Intelligence, 2nd Edition, 20110

Denial. Measures taken to block, prevent, or impair US intelligence collection. (Foreign Denial & Deception Committee, 30 Mar 2006)

-- Also, the attempt to block information that could be used by an opponent to learn some truth. (Roy Godson and James J. Wirtz, "Strategic Denial and Deception," in *Strategic Denial and Deception: The 21st Century Challenge*, eds. Roy Godson and James J. Wirtz, 2002) Also see *deception*.

-- Also, methods used to conceal state and military secrets particularly from foreign intelligence collections. (Joseph W. Caddell; *Deception 101 – A Primer on Deception*, Strategic Studies Institute, US Army War College, 2004)

-- Also, activities and programs designed to eliminate, impair, degrade, or neutralize the effectiveness of intelligence collection within and across any or all collection disciplines, human and technical. (Dr. James B. Bruce, "Denial and Deception in the 21st Century: Adaptation Implications for Western Intelligence," in *Defense Intelligence Journal*, Vol 15, No 2, 2006; pp 13-27)

Denial and Deception – equal parts art and science

Keeping secrets and negating access conceals the truth from an opponent's acquisition. *Denial* hides the real and *deception* portrays the fake.

For additional information see Joint Pub 3-13.4, *Military Deception*, 13 Jul 2006

Denial of intelligence collection is a significant impediment to successful analysis

Denied Area. An area under enemy or unfriendly control in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities. (JP 1-02 and JP 3-05, Special Operations, 18 Apr 2011)

-- Also, a country with which the US has no official or formal diplomatic relations, or a country in which the capabilities and focus of the local CI services create an operating environment so hostile as to require non-traditional tradecraft of the highest order. (National HUMINT Glossary)

Denied Area Tradecraft. The specialized clandestine methodology used in handling agents in particularly difficult and hostile environments. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Departmental Intelligence. Intelligence that any department or agency of the Federal Government requires to execute its own mission. (JP 1-02)

Department of Defense Components. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense agencies, Department of Defense field activities, and all other organizational entities in the Department of Defense. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Department of Defense Intelligence Information System (DoDIIS). The combination of Department of Defense personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and information to military commanders and national-level decision makers. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, a DIA-led enterprise that manages the intelligence information technology activities of and provides intelligence technology to the Department of Defense, the combatant commands, and other national security entities. (National Intelligence: A Consumer's Guide - 2009)

Department of State / Bureau of Diplomatic Security (DS). The security and law enforcement arm of the U.S. Department of State. DS is responsible for providing a safe and secure environment for the conduct of U.S. foreign policy; it is involved in international investigations, threat analysis, cyber security, counterterrorism, security technology, and protection of people, property, and information. (www.state.gov) Also see *Regional Security Officer*.

Every diplomatic mission in the world operates under a security program designed and maintained by DS. In the United States, diplomatic security personnel protect the Secretary of State and high-ranking foreign dignitaries and officials visiting the United States, investigates passport and visa fraud, and conducts personnel security investigations. Operating from a global platform in 25 U.S. cities and 159 foreign countries, diplomatic security ensures that America can conduct diplomacy safely and securely. DS plays a vital role in protecting U.S. embassies and personnel overseas, securing critical information systems, investigating passport and visa fraud, and fighting the war on terror.

-- Department of State website: <http://state.gov/m/ds/index.htm>

Department of State / Bureau of Intelligence and Research (INR). State's intelligence component that provides analysis of global developments to the State Department and contributes its unique perspectives to the community's National Intelligence Estimates. (WMD Report, 31 Mar 2005)

For additional information: <http://www.state.gov/s/inr/ >

Department of Homeland Security (DHS) / Directorate of Information Analysis and Infrastructure Protection. Monitors, assesses, and integrates terrorist-related information; and assesses and addresses the vulnerabilities of the nation's critical infrastructure. (WMD Report, 31 Mar 2005)

Department of Treasury / Office of Terrorism and Financial Intelligence. Treasury's intelligence component that collects and processes information that bears on U.S. fiscal and monetary policy and threats to U.S. financial intuitions. (WMD Report, 31 Mar 2005)

Dependency. [In critical infrastructure protection usage] a relationship or connection in which one entity is influenced or controlled by another entity. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Derogatory Information. Issue information that adversely reflects on a person's loyalty, reliability and trustworthiness. (IC Standard 700-1, 4 Apr 2008)

Desired Perception. In military deception, what the deception target must believe for it to make the decision that will achieve the deception objective. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

Detainee. A term used for any person captured or otherwise detained by an armed force. (JP 1-02)

Within DoD, detainee includes any person captured, detained, or otherwise under the control of DoD personnel (military, civilian, or contract employee). It does not include persons being held primarily for law enforcement purposes except where the United States is the occupying power. As a matter of policy, all detainees will be treated as EPWs until some other legal status is determined by competent authority.

For additional information see JP 3-63, *Detainee Operations*, 30 May 2008.

Detection. 1) In tactical operations, the perception of an object of possible military interest but unconfirmed by recognition; 2) In surveillance, the determination and transmission by a surveillance system that an event has occurred; 3) In arms control, the first step in the process of ascertaining the occurrence of a violation of an arms control agreement; and 4) In chemical, biological, radiological, and nuclear environments, the act of locating chemical, biological, radiological, and nuclear hazards by use of chemical, biological, radiological, and nuclear detectors or monitoring and/or survey teams. (JP 1-02)

Deterrence. The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. (JP 1-02)

Devil's Advocacy. Challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

Devil's Advocacy is most effective when used to challenge an analytical consensus or key assumption regarding a critically important intelligence question.

DIAP. Also see *Defense Intelligence Analysis Program (DIAP)*.

Digital and Multimedia (D/MM) Forensics. The application of computer science and investigative procedures involving the examination of D/MM material. D/MM forensics is derived from a combination of definitions as it applies across the spectrum of computer forensics, audio forensics, image analysis, and video analysis. Also see *digital evidence, digital forensics*, and *forensic science*.

D/MM forensic sub-disciplines include:

Computer and Electronic Device Forensics. The scientific examination, analysis, and/or evaluation of digital and electronic materials.

Audio Forensics. The scientific examination, analysis, comparison, and/or evaluation of audio.

Image Analysis. The application of image science and domain expertise to examine and interpret the content of an image and/or the image itself.

Video Analysis. The scientific examination, comparison, and/or evaluation of video.

Digital Evidence. Information of probative value stored or transmitted in binary form. (DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center, 1 Mar 2010)

-- Also, information stored or transmitted in binary form that may be introduced and relied upon in court. (DoJ, *Electronic Crime Scene Investigation, 2nd Edition: A Guide for First Responders*, Apr 2008)

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination. Digital evidence:

- Is latent, like fingerprints or DNA evidence.
- Crosses jurisdictional borders quickly and easily.
- Is easily altered, damaged, or destroyed.
- Can be time sensitive.

-- *Electronic Crime Scene Investigation, 2nd Edition,* April 2008. Available online at: www.ncjrs.gov/pdffiles1/nij/219941.pdf

Also see United States Secret Service, *Best Practices for Seizing Electronic Evidence v.3, A Pocket Guide for First Responders*

Digital Forensics. In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony. Beyond traditional legal purposes, the same techniques, scientific rigor, and procedural precision now support the range of military operations and courses of action, e.g., computer network operations as well as CI objectives. (DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center, 1 Mar 2010) Also see *digital & multimedia forensics, digital evidence*, and *forensic science*.

-- Also, the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. (NIST, Glossary of Key Information Security Terms, May 2013)

Digital Tradecraft. The conduct, topics, or techniques of modern espionage or CI that employ digital or cyber means. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010 with change 1 dated 16 Oct 2013)

-- Also, digital or cyber tactics, techniques, and procedures designed to obscure or frustrate observation by hostile or unfriendly entities. (DoDI S-3325.10, [FOUO title], 6 Jun 2013)

Digraph and/or Trigraph. A two and/or three-letter acronym for the assigned Codeword or nickname. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Diplomatic and/or Consular Facility. Any Foreign Service establishment maintained by the US Department of State abroad. It may be designated a "mission" or "consular office," or given a special designation for particular purposes, such as "United States Liaison Office." A "mission" is designated as an embassy and is maintained in order to conduct normal continuing diplomatic relations between the US Government and other governments. A "consular office" is any consulate general or consulate that may participate in most foreign affairs activities, and varies in size and scope. (JP 1-02)

Diplomatic Establishment. A mission, consulate, embassy, residential compound, or other premises owned or leased and used by a government for official purposes. (Words of Intelligence, 2nd Edition, 2011)

Diplomatic Immunity. A status wherein diplomatic officers accredited to a foreign government as ambassadors, or other public ministers, are immune from the jurisdiction of all courts and tribunals of the receiving states whether criminal or civil. The status of diplomatic immunity protects the bearer from prosecution, civil suit, punishment, or compelled testimony in the country to which he or she is accredited. (Words of Intelligence, 2nd Edition, 2011)

Diplomatic Security. The set of measures enacted to ensure that the diplomatic representatives of a nation-state, kingdom, or other political entity are able to conduct that entity's foreign affairs in a confidential, safe manner. (US State Department) See *Department of State / Bureau of Diplomatic Security*.

> *Security is a basic function of diplomacy, and specific components of diplomatic security include preserving the confidentiality of diplomatic documents and communications, protecting diplomatic personnel, ensuring the integrity of diplomatic personnel through background investigations, and safeguarding diplomatic posts overseas and diplomatic facilities at home.*
>
> -- History of the Bureau of Diplomatic Security of the United States Department of State (October 2011) Copy at <http://www.state.gov/m/ds/rls/rpt/c47602.htm>

Direct Access. Descriptor used for sources with firsthand access to the information provided. (DoDI S-5200.42, Defense HUMINT and Related Intelligence Activities (U), 8 Dec 2009) Also see *indirect access*.

Direct Liaison Authorized (DIRLAUTH). That authority granted by a commander (any level) to a subordinate to directly consult or coordinate an action with a command or agency within or outside of the granting command. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Direct Support (DS). A mission requiring a force to support another specific force and authorizing it to answer directly to the supported force's request for assistance. (JP 1-02)

Direction Finding (DF). A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. (JP 1-02)

Director Defense Intelligence Agency (Dir DIA). Advises the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Combatant Commanders on all matters concerning all-source Defense Intelligence.

> Director DIA serves as the **Defense Counterintelligence Manager** [emphasis added], the Defense HUMINT Manager, the Defense Collection Manager…, and the Commander of the Joint Functional Component Command-Intelligence, Surveillance, and Reconnaissance (JFCC-ISR). See DoDD 5105.21, *DIA*, 18 Mar 2002.

Director of National Intelligence (DNI). Serves as the principal adviser to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security; oversees the 16 federal organizations that make up the intelligence community (IC); and manages the implementation of the National Intelligence Program (NIP). (IRTPA 2004)

> Office of the Director of National Intelligence (ODNI) is charged with: 1) integrating the domestic and foreign dimensions of US intelligence so that there are no gaps in our understanding of threats to our national security; 2) bringing more depth and accuracy to intelligence analysis; and 3) ensuring that US intelligence resources generate future capabilities as well as present results.
>
> DNI created by Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) in December 2004. The Office of the Director of National Intelligence (ODNI) began operations in April 2005. It was created to drive strategic integration, ensure better coordination, and provide oversight & governance of the Intelligence Community (IC).
>
> -- See ODNI Fact Sheet (Oct 2011): <http://www.dni.gov/files/documents/ODNI%20Fact%20Sheet_2011.pdf>

Dirty Bomb. An explosive-driven radiological dispersal device.

> See NRC fact sheet, "Dirty Bombs," May 2007(accessed 27 June 2011); available on line at: <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs-bg.pdf>
>
> Also see Congressional Research Service (CRS) report R41890, "Dirty Bombs": Technical Background, Attack Prevention and Response, Issues for Congress," 24 June 2011.

Disaffected Person. A person who is alienated or estranged from those in authority or lacks loyalty to the government; a state of mind. (JP 1-02)

Discards. [S]pies supposedly deliberately sacrificed to distract a counterintelligence investigation away from a better target. This is a controversial strategy about which there remains much debate within the intelligence community… (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Discovery. Part of the pre-trial litigation process during which each party requests relevant information and documents from the other side in an attempt to "discover" pertinent facts. Generally discovery devices include depositions, interrogatories, requests for admissions, document production requests and requests for inspection. (<http://www.lectlaw.com/def/d058.htm>; accessed 18 Sep 2012)

Discoverability. Discoverability means users can "discover" selected values (e.g., who, what, where, when), but cannot gain access to the underlying information until the user requesting access is authorized and authenticated. (Markle Task Force, 1 Sep 2009)

> Discoverability is the first step in an effective system for information sharing, offering users the ability to "discover" data that exists elsewhere. Discoverability means users can "discover" selected values (e.g., who, what, where, when), but cannot gain access to the underlying information until the user requesting access is authorized and authenticated. In many ways, knowing where relevant information can be found or who has the information is the essential first step towards information sharing as this makes collaboration and analysis possible. A system of discoverability also avoids the bulk transfers of data required in large centralized databases, improving security and minimizing privacy risks.
>
> See: <http://www.markle.org/sites/default/files/MTFBrief_Discoverability.pdf>

Disguise. Concealment or misrepresentation of the physical characteristics or true nature or identity of a person or object. (CIA in D&D Lexicon, 1 May 2002)

Disinformation. Carefully contrived misinformation prepared by an intelligence or CI service for the purpose of misleading, deluding, disrupting, or undermining confidence in individuals, organizations, or governments. (CI Community Lexicon)

Dissemination. The timely distribution of intelligence products (oral, written, or graphic form) to departmental and agency intelligence Consumer's is a suitable format. (CI Community Glossary)

-- Also, the timely conveyance of intelligence in suitable form to customers. (ICS Glossary)

Dissemination and Integration. In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. Also see *intelligence process*. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Divided Loyalties. Broadly defined, individuals with intellectual or emotional commitments to another country through cultural affinity. (PERSEREC Technical Report 02-5, Espionage Against the United States by American Citizens 1947-2001, July 2002) Also see *ideology, MICE*.

DNA. The abbreviation for deoxyribonucleic acid, which is the genetic material present in the cells of all living organisms. DNA is the fundamental building block for an individual's entire genetic makeup. (www.ojp.usdoj.gov; accessed 29 Apr 2013)

> A person's DNA is the same in every cell (with a nucleus). DNA is contained in blood, semen, skin cells, tissue, organs, muscle, brain cells, bone, teeth, hair, saliva, mucus, perspiration, fingernails, urine, feces, etc.

Document and Media Exploitation (DOMEX). The processing, translation, analysis, and dissemination of collected hard copy documents and electronic media, which are under U.S. Government's physical control and are not publicly available; excludes: handling of documents and media during collection, initial review, and inventory process; and documents and media withheld from the IC DOMEX dissemination system in accordance with DNI-sanctioned agreements and policies to protect sources and methods. (ICD 302, Document and Media Exploitation, 6 Jul 2007) Also see *Document Exploitation* (*DOCEX), Harmony,* and *National Media Exploitation Center (NMEC)*.

-- Also, the processing, translation, analysis, and dissemination of collected hard-copy documents and electronic media that are under U.S. Government physical control and are not publicly available. In the Department of Defense this includes the handling of documents and media during their collection, initial review, inventory, and input to a database. (DoDD 3300.03, DoD DOMEX, 11 Jan 2011)

-- Also, the handling and exploitation of documents and/or media for intelligence purposes. (HDI Lexicon, April 2008)

> The National Media Exploitation Center (NMEC) is responsible for ensuring the rapid collection, processing, exploitation, dissemination and sharing of all acquired and seized media throughout the intelligence, counterintelligence, military and law enforcement communities. See ICD 302, copy available online at <http://www.fas.org/irp/dni/icd/icd-302.pdf>
>
> Director DIA is the IC Executive Agent for NMEC (DoDD 3300.03, *DoD DOMEX*, 11 Jan 2011)

Document Exploitation (DOCEX). The systematic extraction of information from all media formats is response to collection requirements. (Term previously defined in Army FM 2-0, Intelligence, May 2004) Also see *Document and Media Exploitation (DOMEX); Harmony;* and *NMEC.*

Doctrine. Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (JP 1-02)

> *"Doctrine evolves from theory and concepts based on values, beliefs, historical perspective, experience, and research."*
>
> -- AR 600-100, *Army Leadership*, 8 Mar 2007

-- Also, *Joint Doctrine*: fundamental principles that guide the employment of US military forces in coordinated action toward a common objective. Joint doctrine contained in joint publications also includes terms, tactics, techniques, and procedures. It is authoritative but requires judgment in application. (JP 1-02)

DoD CI Campaign (previously referred to as "*DoD CI Strategic Campaign).* See the FOUO definition in O-DoDD 5240.02, Counterintelligence, 20 Dec 2007, with change 1 dated 30 Dec 2010; available on SIPRNet at <http://www.dtic.smil.mil/whs/directives/corres/pdf/524002p.pdf>

> DoD CI Campaigns drive and shape Defense CI engagement against critical foreign intelligence threats globally to achieve strategic outcomes; these CI Campaigns are managed by DIA's Office of Counterintelligence (OCI-1).

DoD Criminal Investigative Organizations. The term refers collectively to the United States Army Criminal Investigation Command, Naval Criminal Investigative Service, U.S. Air Force Office of Special Investigations, and Defense Criminal Investigative Service, Office of the IG DoD. (DoDD 5525.07)

DoD Functional Manager for Security Training. Director Defense Security Service (DSS).

DoD Law Enforcement Organizations. Organizations, agencies, entities, and offices of the Military Departments and Defense Agencies and the DoD Inspector General that perform a law enforcement function for those departments and agencies and are manned by DoD LEOs [Law Enforcement Officers]. (DoDI 2000.26, Suspicious Activity Reporting, 1 Nov 2011)

DoD Personnel Travel Clearance. Travel clearance for DoD and DoD-sponsored personnel performing official temporary travel abroad. The three types of clearance are country clearance, theater clearance, and special area clearance. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

DoD Strategic CI Campaign. See FOUO definition in O-DoDD 5240.02, CI, 20 Dec 2007.

DoD Unknown Subject. The subject of a DoD CI investigation whose identity has not been determined. (DoDI 5240.04, CI Investigations, 2 February 2009 with change 1 dated 15 Oct 2013) Also see *Defense Unknown Subject Team; Unknown Subject*.

> An "unknown subject" is commonly referred to as an "UNSUB."
>
> DIA's Office of Counterintelligence (OCI-2) serves as the focal point and central repository for DoD unknown subject CI leads, reports and information.

Domestic Activities. Activities within the United States that do not involve a significant connection with a foreign power, organization, or person. (AR 381-20, Army CI Program. 25 May 2010)

Domestic Intelligence. Intelligence relating to activities or conditions within the United States that threaten internal security and that might require the employment of troops; and intelligence relating to activities of individuals or agencies potentially or actually dangerous to the security of the Department of Defense. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011)

Domestic Terrorism. Terrorism perpetrated by the citizens of one country against persons in that country. This includes acts against citizens of a second country when they are in the host country, and not the principal or intended target. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

-- Also, Americans attacking Americans based on U.S.-based extremist ideologies. (FBI)

-- Also, domestic terrorists: people who commit crimes within the homeland and draw inspiration from U.S.-based extremist ideologies and movements. (CRS Report R42536, The Domestic Terrorist Threat: Background and Issues for Congress, 15 May 2012)

One particularly insidious concern that touches all forms of domestic extremism is the lone offender—a single individual driven to hateful attacks based on a particular set of beliefs without a larger group's knowledge or support. In some cases, these lone offenders may have tried to join a group but were kicked out for being too radical or simply left the group because they felt it wasn't extreme or violent enough. We believe most domestic attacks are carried out by lone offenders to promote their own grievances and agendas.

-- FBI at <http://www.fbi.gov/news/stories/2009/september/domterror_090709> (accessed 18 Dec 2012)

The Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) do not officially list domestic terrorist organizations, but they have openly delineated domestic terrorist "threats." These include individuals who commit crimes in the name of ideologies supporting animal rights, environmental rights, anarchism, white supremacy, anti-government ideals, black separatism, and anti-abortion beliefs.

-- CRS Report R42536, *The Domestic Terrorist Threat: Background and Issues for Congress*, 15 May 2012

Dossier. A file consisting of information concerning an individual. (National HUMINT Glossary)

Double Agent. Agent in contact with two opposing intelligence services, only one of which is aware of the double contact or quasi-intelligence services. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *dangle; dangle operation; provocation*.

No term is more misused by amateurs and greenhorns than "double agent."

-- William R. Johnson, Former Army Intelligence and CIA

In its simplest form, a double agent works for two intelligence services at the same time, with only one of the services understanding this.

-- Stuart A. Herrington, *Traitors Among Us: Inside the Spy Catcher's World* (1999), p. 132

The double agent is the most characteristic tool of counterespionage operations, and he comes in many guises.

-- Allan W. Dulles, The Craft of Intelligence (2006), p. 123

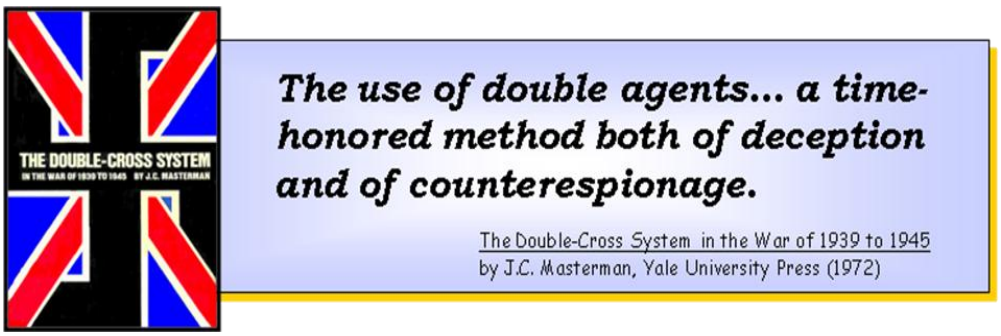
The first purpose of any double agent program is to engage the enemy. …The basic use of double agents is to keep contact with the enemy. What you use that contact for depends on the state of your CI program at any moment. But without contact, there isn't much you can do.

A double agent operation is a channel in which information moves in both directions. On each end of the channel is an intelligence or counterintelligence service. The intelligence service seeks to ensure that the flow of material through the channel is beneficial to itself. The CI service seeks to ensure that the flow of material is detrimental to its opponent.

-- William R. Johnson (Former CIA Officer)

The caviar of the intelligence business.

-- James M. Olson, Former Chief of CIA Counterintelligence



-- Also, an agent who is cooperating with an intelligence service of one government on behalf of and under the control of an intelligence or security service of another government, and is manipulated by one to the detriment of the other. (Glossary of Intelligence Terms and Definitions, IC Staff, 1978)

-- Also, a person pretending to work as a spy for one government while actually working as [an asset] for another government. (WMD Report, 31 Mar 2005)

-- Also, an agent working for two opposing agencies; he is loyal to one while betraying the other. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

-- Also, *double agents* – individuals under the control of one intelligence agency who offer their services to an opposing intelligence agency. ("Double Agent Operations," *Espionage*, Naval Investigative Service Command; nd, circa 1989)

-- Also, a clandestine operative who works for two opposing espionage organizations but who is loyal to one of the organizations and betrays the other. (*Encyclopedia of the CIA*, 2003)

-- Also, a person who engages in clandestine activity for two intelligence or security services (or more in joint operations), who provides information about one or about each to the other, and who wittingly withholds significant information from one on the instructions of the other or is unwittingly manipulated by one so that significant facts are withheld from the adversary. (John P. Dimmer - 1962; see below)

A World of Stratagems

"To tackle enemy espionage (whoever the enemy may turn out to be) it is therefore of paramount importance to keep a firm hold on the enemy's own system of agents and informers. Knowledge of his methods, knowledge of his intentions, and knowledge of the personnel of his organization are all vitally necessary. Surely all these objects are the best attained by the maintenance of double agents! The confession of faith is consequently a simple one. It amounts to this: that ***in peace as well as in war a carefully cultivated double agent system is the safest and surest weapon of counterespionage*** *[emphasis added], and the one most easily adaptable to changing conditions, changing problems, and even changing enemies."*

-- J.C. Masterman, *The Double-Cross System* (1972)

The term "double agents" as used during OSS operations in WWII: *"…captured agents who would be persuaded to continue their activities for the enemy, ostensibly in good faith but acting at the direction of X-2 [OSS Counterintelligence]…."* Also *"the case of an agent recruited by X-2 [OSS CI] and infiltrated into enemy territory to induce the enemy to employ him as an agent and return him to Allied territory."*

-- Kermit Roosevelt, *War Report of the OSS* (1976)

"The fact that doubles have an agent relationship with both sides distinguishes them from penetrations, who normally are placed with the target service in a staff or officer capacity…. The double agent is one of the most demanding and complex counterintelligence activities in which an intelligence service can engage. Directing even one double agent is a time-consuming and tricky undertaking that should be attempted only by a service having both competence and sophistication."

-- John P. Dimmer, CIA (1962)

"One side has a agent whom it deliberately tries to work in as an agent on the other side, of course without the other knowing anything about it… the most advanced and dangerous kind of work an agent can do, both for the agent himself and for the two parties."

-- Colonel Stig Erik Constans Wennerström, Swedish Air Force
Spy for the GRU -- convicted of treason in 1964

Note: For a full account of the Wennerström affair see *An Agent in Place* by Thomas Whiteside (1966), republished in 1983 in Ballantine Intelligence Library

---

Double Agents *"can serve as excellent channels through which misleading information can flow to the enemy. So double agents serve both as collectors of positive intelligence and channels for deception."*

-- Church Committee (Senate Report 94-755 , 26 April 1976)

A condoned channel of communication with the enemy

For additional open source information regarding double agents see:

William R. Johnson, *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer,* Georgetown University Press *(*2009); pp. 91-153.

Federal Government Security Clearance Programs, Report # 99-166, Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, US Senate, April 1985, specifically testimony on pp. 63-103 regarding two Army CI controlled double agent operations: 1) Chief Warrant Officer Jamos Szmolka against the Hungarian Intelligence Service in 1977-1981; and 2) Sergeant "Smith" against the KGB for over 10 years starting in the early 1970's.

"Double Agent Operations,*" Espionage*, Naval Investigative Service Command (nd, circa 1989); pp. 24-33.

John P. Dimmer (aka F.M. Begum), "Observations on the Double Agent," *Studies in Intelligence*, V6: 11, pp 57-72 (1962); declassified, originally classified Secret. Available online at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no1/html/v06i1a05p_0001.htm>

J.C. Masterman, *The Double-Cross System* (1972). Double agent operations against the Germans in World War II. Nazi agents in Britain were captured or turned themselves in and were then used by the British to broadcast mainly disinformation to their Nazi controllers.

John Barron, *Operation Solo: The FBI's Man in the Kremlin* (1996). Operation Solo tells the remarkable and true story of FBI run double agent Morris Childs, code named "Agent 58", who, for twenty-seven years, provided the FBI with the Kremlin's innermost secrets during fifty-two clandestine missions to the Soviet Union, China, and Eastern Europe.

David Wise, *Cassidy's Run* (2000). True-life story of US Army Sgt. Joseph Cassidy who successfully pretended to be a traitor to his country. In the eyes of his Soviet handlers, he was a mole planted deep inside DoD. This US Army/FBI double agent operation – code named Operation SHOCKER -- flushed out 10 Soviet spies including a Russian sleeper agent in the Bronx and revealed the lengths to which Soviet intelligence would go to penetrate DoD.

Andrew Tully, *Inside the FBI* (1980). Chapter 5 "Spies for Sale" (pp. 70-81) tells the story of a joint Naval Investigative Service and FBI double agent operation [Operation LEMONAID] targeting the Russian Intelligence Service resulting in the arrest of three Russians working out of the United Nations for espionage on 20 May 1978. Also see Jeremy J. Leggatt, "Art Lindberg's Walk in the Cold," *Reader's Digest*, June 1980.

Downgrade. To determine that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a lower degree. (JP 1-02)

Doxing. [Cyber usage] Publicly releasing a person's identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Dry Clean. [Tradecraft jargon] Actions taken to determine if one is under surveillance. (Spy Book)

Dry Cleaning. [Tradecraft jargon] Any technique used to elude surveillance. A usual precaution used by intelligence personnel when actively engaged in an operation. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, any technique used to detect surveillance; a usual precaution engaged in by intelligence personnel when actively engaged in an operation. (FBI FCI Terms)

Dynamic Threat Assessment (DTA). An intelligence assessment developed by the Defense Intelligence Agency that details the threat, capabilities, and intentions of adversaries in each of the priority plans in the Joint Strategic Capabilities Plan. (JP 2-0, Joint Intelligence, 22 Oct 2013)

> The DTA is used by the Combatant Commanders and COCOM planning staffs to conduct Mission Analysis for Step 1 - Strategic Guidance under Adaptive Planning and Execution (APEX).

Dual Agent. *Within DoD, term rescinded by JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011.*

> Previously defined in JP 1-02 as "one who is simultaneously and independently employed by two or more intelligence agencies, covering targets for both."

Dual Citizen. Any person who is simultaneously a citizen of more than one country. (DSS Glossary)

Dual-use. Technology and articles that are potentially used either for commercial/civilian purposes or for military, defense, or defense-related purposes. (DoDI 2040.02, International Transfers of Technology, Articles, and Services, 10 Jul 2008) See *critical technology*.

DUST. See *Defense Unknown Subject Team*.

E ==========

Economic Espionage. The knowing misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent. Misappropriation includes, but is not limited to, stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to obtain trade secrets without authorization. (Economic Espionage Act of 1996, PL 104-294)

Economic Espionage… is a fact of life

I think you have to separate very clearly what are the fields which are covered by the alliance and the fields which are not covered by an alliance. It's clear that when you are allies, you have certain sectors, I'm speaking of the armaments. I'm thinking of diplomatic matters where normally you should not try to gather intelligence. But in all of the other fields, being allied does not prevent the states from being competitors. Even during the Cold War, the economic competition existed. Now the competition between the states is moving from the political-military level to the economic and technological level. ***In economics, we are competitors, not allies.*** *I think that even during the Cold War getting intelligence on economic, technological, and industrial matters from a country with which you are allies is not incompatible with the fact that you are allies.*

-- Pierre Marion, Former Director of French Intelligence (DGSE)
as quoted in *Friendly Spies* by Peter Schweizer (1993)

Section 101(a) of the Economic Espionage Act of 1996 criminalizes economic espionage.
See <http://www.gpo.gov/fdsys/pkg/PLAW-104publ294/content-detail.html>
Also see <http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage>

The **Economic Espionage Act (EEA) of 1996** (18 USC §§ 1831-1839) is concerned in particular with economic espionage and foreign activities to acquire US trade secrets. In this context, trade secrets are all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether stored or unstored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing, if the owner (the person or entity in whom or in which rightful legal or equitable title to, or license in, is reposed) has taken reasonable measures to keep such information secret and the information derives independent economic value, actual, or potential from not being generally known to, and not being readily ascertainable through, proper means by the public. Activities to acquire these secrets include the criminal offenses: economic espionage and industrial espionage.

The Office of the National Counterintelligence Executive submits an annual report to Congress on the threat to the United States from foreign economic collection and industrial espionage; see annual reports at: <http://www.ncix.gov/publications/reports/fecie_all/index.html>

"US intelligence officials put the cost of lost sales due to illicit appropriation of technology and business ideas at between $US100 billion and $US250 billion a year."

-- *Financial Times*, January 2011

Educing Information (EI). The full range of approaches to obtain useful information from sources. EI includes elicitation, debriefing, and interrogation. (*Educing Information – Interrogation: Science and Art*, Dec 2006) Also see *debriefing; elicitation; interrogation; interview*.

The 2006 Intelligence Science Board report *Educing Information – Interrogation: Science and Art* is available online at <http://www.ndic.edu/press/3866.htm>

Effect. 1) The physical or behavioral state of a system that results from an action, a set of actions, or another effect; 2) The result, outcome, or consequence of an action; 3) A change to a condition, behavior, or degree of freedom. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Effects-Based Operations (EBO). [Non-doctrinal term] A process for obtaining a **desired strategic outcome** [emphasis added] or *effect* on the enemy. (JFCOM Glossary at www.jfcom.mil/about/glossary.htm)

> Effects Bases Operations: *Coordinated sets of actions directed at shaping the behavior of friends, foes, and neutrals in peace, crisis, and war.*
>
> *The concept of EBO focuses "coordinated sets of actions" on objectives defined in terms of human behaviors in multiple dimensions and on multiple levels, and measures their success in terms of the behavior produced…. Effects cannot be isolated. All effects, at each level and in each arena, are interrelated and are cumulative over time. And lastly, effects are both physical and psychological in nature.*
>
> -- Edward A. Smith, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War* (2002)

eGuardian. The FBI's unclassified, law enforcement-centric threat reporting system. It provides a means to disseminate SARs dealing with information regarding a potential threat or suspicious activity rapidly throughout the national law enforcement community. (DoDI 2000.26, Suspicious Activity Reporting, 1 Nov 2011) See *suspicious activity report*.

> All reports in the eGuardian system Shared Data Repository are viewable through Guardian, the FBI's classified threat reporting system. DoD personnel assigned to Joint Terrorism Task Forces (JTTFs) and the National Joint Terrorism Task Force (NJTTF) have access to Guardian.
>
> For additional information see: <http://foia.fbi.gov/eguardian_threat.htm>

Electronic Intelligence (ELINT). Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 1-02 and JP 3-13.1, Electronic Warfare, 25 Jan 2007) Also see *electronic warfare; foreign instrumentation signals intelligence; signals intelligence.*

> ELINT is a sub-category of signals intelligence (SIGINT) that engages in dealing with information derived primarily from electronic signals that do not contain speech or text (which are considered Communications Intelligence aka COMINT). Two major branches of ELINT are Technical ELINT (TechELINT) and Operational ELINT (OpELINT) described as follows:
>
> -- TechELINT describes the signal structure, emission characteristics, modes of operation, emitter functions, and weapons systems associations of such emitters as radars, beacons, jammers, and navigational signals. A main purpose of TechELINT is to obtain signal parameters which can define the capabilities and the role that the emitter plays in the larger system, such as a ground radar locating aircraft, and thus lead to the design of radar detection, countermeasure, or counterweapons equipment.
>
> -- OpELINT concentrates on locating specific ELINT targets and determining the operational patterns of the systems; these results are commonly called Electronic Order of Battle (EOB).
>
> For additional information see: Richard L. Bernard, *Electronic Intelligence (ELINT) at NSA*, 2009. On line at: <http://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/elint.pdf>
>
> Also see additional background information at: <www.fas.org/irp/nsa/almanac-elint.pdf>

Electronic Surveillance. The acquisition of a nonpublic communication by electronic means without the consent of a person who is party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication. (DoD 5240.1-R, Dec 1982) Also see *surveillance; foreign intelligence surveillance act (FISA).*

> Governed by the Foreign Intelligence Surveillance Act (FISA) of 1978 (50 USC §1805).
>
> For DoD CI see Chap 5. Proc 5 – Electronic Surveillance, DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 7 Dec 1982

The Electronic Communications Privacy Act of 1986 (ECPA) prohibits unauthorized electronic eavesdropping. ECPA consists of three parts. The first, often referred to as Title III, outlaws wiretapping and electronic eavesdropping, except as otherwise provided. The second, the Stored Communications Act, governs the privacy of, and government access to, the content of electronic communications and to related records. The third outlaws the use and installation of pen registers and of trap and trace devices, unless judicially approved for law enforcement or intelligence gathering purposes.

-- Also, the use of electronic devices to monitor or record conversations, activities, sound, or electronic impulses. (Army FM 2-22.2, Counterintelligence, Oct 2009)

-- Also, (ELSUR) under Title III and FISA is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Electronic Tracking Device. Direction finder including electronic tracking devices, such as, radio frequency beacons and transmitters, vehicle locator units, and the various devices that use a Global Positioning System [GPS] or other satellite system for monitoring non-communication activity. (FBI Domestic Investigations and Operations Guide, 16 Dec 2008)

Electronic Warfare (EW). Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support. (JP 1-02 and JP 3-13.1, Electronic Warfare, 25 Jan 2007)

Electronics Security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar. (JP 1-02 and JP 3-13.1, Electronic Warfare, 25 Jan 2007)

Elements of Espionage. The fundamentals components in which an intelligence service conducts espionage… some or all of the following elements are present in every espionage operation: 1) contact & communication; 2) collection; 3) motive / reward; 4 travel; and 5) tradecraft. (*Espionage 101: Elements of Espionage*, US Army AFCITC Course Handout, 3 Dec 1996, authored by CW4 Constance Y. Huff, USA) Also see *Espionage; Espionage Act; Espionage Against the United States.*

Espionage *investigative elements* are different than the *prosecutorial elements* (which are addressed in Title 18 USC, §§ 792-798 and Article 106, UCMJ).

Elicitation. In intelligence usage, the acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *educing information; debriefing; interrogation; interview.*

-- Also, engaging with a source in such a manner that he or she reveals information without being aware of giving away anything of value. (Educing Information – Interrogation: Science and Art, Dec 2006)

-- Also, the strategic use of conversation to extract information from people without giving them the feeling they are being interrogated. (FBI)

-- Also, the use of generalized questions to ascertain someone's knowledge on a particular topic. (Army FM 2-22.2, Counterintelligence, Oct 2009

A casual conversation with a hidden agenda

The subtle extraction of information during an apparently "normal" and "innocent" conversation. A supplemental technique used during interviews, debriefings and interrogations.

Elicitation is the practice of obtaining information about a topic from conversations, preferably without the source knowing what is happening.

-- Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (2004), p. 72

Elicitation, that is to say, like a lot of other tradecraft techniques, has its Scylla and Charybdis. On one hand, the cautious seeker risks concealing his purpose in such general questions or remarks that he evokes nothing of value. On the other hand, if the questions are excessively direct, the contact may quickly suspect he is being interrogated for intelligence purposes and bring the interview to an abrupt and unpleasant end.

-- George G. Bull, "The Elicitation Interview," *Studies in Intelligence*, vol. 14 no. 2 (Fall 1970), pp. 115-22. Originally classified "Secret" [declassified].

Elicitation is a technique used to discreetly gather information. It is a conversation with a specific purpose: collect information that is not readily available and do so without raising suspicion that specific facts are being sought. It is usually non-threatening, easy to disguise, deniable, and effective. The conversation can be in person, over the phone, or in writing. Conducted by a skilled collector, elicitation will appear to be normal social or professional conversation. A person may never realize she was the target of elicitation or that she provided meaningful information.

-- *Elicitation Techniques*, FBI (accessed 20 Aug 2012)
See pdf available at: <http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-brochure>

Emanation Security. Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information systems. Synonymous with Transient Electromagnetic Pulse Emanation Standard (TEMPEST). (DSS Glossary) Also see *TEMPEST.*

Emerging Warning Concerns. Newly identified issues relevant to national security of sufficient significance to warrant temporary attention by the Defense Intelligence Enterprise. An emerging warning issue may be redefined as an enduring warning issue based on national security priorities and operational plans. (DoDD 3115.16, The Defense Warning Network,5 Dec 2013)

Émigré. A person who lawfully departed his or her country with the intention of resettlement elsewhere. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a person who departs from his country for any lawful reason with the intention of permanently resettling elsewhere. (ICS Glossary)

Emission Security. The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptoequipment and telecommunications systems. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010). Also see also *communications security*.

Equipment Exploitation Operations. Intelligence exploitation operations of all types foreign and non-foreign material which may have military application or answer a collection requirement. This material includes material found on a detainee or on the battlefield (Captured Enemy Equipment (CEE)), or purchased through either open or clandestine means (Foreign Military Acquisition). (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Enabling Activities. [In CI and HUMINT usage] Any activity that supports Defense CI and HUMINT operations, functions, and missions, including source validation, collection management, collection requirements management, cover, cover support, information systems, production management, source communications, targeting, and training. (DoDI O-5100.93, Defense CI & HUMINT Center, 13 Aug 2010)

Encipher. To convert plain text into unintelligible form by means of a cipher system. (JP 1-02)

-- Also, convert plain text to cipher text by means of a cryptographic system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Encode. Convert plain text to cipher text by means of a code. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Encrypt. Generic term encompassing encipher and encode. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Encryption. The process of changing plaintext into ciphertext for the purpose of security or privacy. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

End State. Set of required conditions that defines achievement of the commander's objectives. (JP 1-02)

Enduring Warning Issue. A significant national security issue, usually linked to an operation plan or concept plan, that is well defined and are longstanding potential threats to the interests of the U.S. and its allies. (DoDD 3115.16, The Defense Warning Network,5 Dec 2013)

Enemy Combatant (EC). A person engaged in hostilities against the United States or its coalition partners during an armed conflict. (DoDD 2310.01E and JP 3-56, Detainee Operations, 6 Feb 2008)

Esoteric Communications. Public statements whose surface meaning (manifest content) does not reveal the real purpose, meaning, or significance (latent content) of the author. (Army Techniques Publication 2-22.9, Open-Source Intelligence, 10 Jul 2012)

Espionage. Intelligence activity directed towards the acquisition of information through clandestine means. (NSCID 5 and DCID 5/1) Also see *Elements of Espionage*; *Espionage Act*; *Espionage Against the United States*.

> ***"The object of secret intelligence activity [espionage] is to obtain by secret means information which cannot otherwise be secured and which is not elsewhere available."***
> -- Kermit Roosevelt, *War Report of the OSS* (1976)

> "*In espionage, two factors are constant. Intelligence officers recruit foreign nationals who can provide classified information on their governments' plans and intentions, and the counterintelligence services of those countries try to thwart these operations."*
> -- Brian P. Fairchild (CIA Case Officer for 20 years), *"Human Intelligence, Operational Security and the CIA's Directorate of Operations."* Statement before the Joint Economic Committee, United States Congress 20 May 1998

-- Also, 1) Intelligence activity directed toward the acquisition [of] information through clandestine means and proscribed by the laws of the country against which it is committed; 2) Overt, cover, or clandestine activity designed to obtain information relating to the national defense with an intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation. (CI Community Lexicon)

-- Also, Clandestine intelligence activity. This term is often interchanged with "clandestine collection." (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, 1) The art of spying; 2) The act of seeking information for one government that the other government wishes to keep secret. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

> Espionage is the clandestine collection of information by people either in a position of trust for the targeted entity, or with access to people with such access. The process of recruiting such individuals and supporting their operations is the HUMINT discipline of *agent handling*.

"Espionage—the use of spies or secret agents to steal information from enemies, adversaries, or competitors—is one of the oldest forms of intelligence gathering."

-- Arthur S. Hulnick, "Espionage: Does It Have a Future in the 21st Century?" *The Brown Journal of World Affairs;* XI: 1 (2004)

"Espionage is distinguished from other forms of intelligence gathering by its clandestinity and its 'illegal means' of acquisition."

-- Frederick P. Hitz, Former Inspector General of the CIA (1990-1998)

"Espionage is the theft of information in contravention of another nation's laws by a person known as an 'agent.' This act of theft may be direct, as in the secret copying of a classified document, or the indirect, as in hiding of an eavesdropping device, or merely oral, but is done by an agent and it breaks either a foreign law or the internal regulation of an alien organization. Espionage is not the confidential purchase of information where mere embarrassment, rather than illegality, is risked. It is not the flattery, bribery, or coercion of a person to influence his actions within legal limits. It is not 'a scuttling, violence-prone business. . . incompatible with democracy.' But rather a silent, surreptitious, violence-shunning business serving the nation."

-- William R. Johnson, "Clandestinity and Current Intelligence," *Studies in Intelligence*, vol. 20, no. 3 (Fall 1976), pp. 15-69. Originally classified "Secret / No Foreign Dissem" [declassified].

Espionage, since it is based on human vulnerability, can penetrate even the most heavily guarded repositories of national secrets.

-- Also, [*Crime of Espionage*] the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Espionage is a national security crime, specifically a violation of Title 18 USC, §§ 792-798 and Article 106, Uniform Code of Military Justice (UCMJ).

See article *"Espionage: The American Judicial Response. An in Depth Analysis of the Espionage Laws and Related Statues"* by Harold W. Bank (45 pages).
Copy at <http://www.wcl.american.edu/journal/lawrev/21/bank.pdf.> (accessed 31 Oct 2012)

"The man engaged in espionage on behalf of his own country is committing a patriotic act. The man who gives away or sells his own country's secrets is committing treason."

-- Allen W. Dulles, *The Craft of Intelligence* (2006), p. 179

"Espionage is a crime almost devoid of evidence…"

-- Peter Wright (Former Asst Director MI5), *Spycatcher* (1987)

"*The act of espionage is unlike any other criminal act in that it leaves no traces. Indeed, unless the agent is caught, the government office that has been penetrated is usually unaware that any crime has taken place. The actual detection of espionage is a very specialized task…."*

-- Miles Copeland, *Without Cloak or Dagger* (1974), p. 160

"*...[E]spionage in it's own way is a very unique crime: There are no smoking guns, no battered victims, rarely do we have any forensic evidence, no bait money, no exploding dye packs, no bank surveillance films. Espionage, in many cases, leaves no footprints."*

-- William H. Webster, Director FBI (12/10/85)

"Because it leaves no footprints, espionage is one of the more difficult crimes to uncover. Yet the business of catching spies affects profoundly the American way of life. If done well, it protects our freedoms by keeping us strong. If done poorly, it can impinge on our liberties just as surely as a takeover by a foreign power."

-- Ronald Kessler, *Spy vs. Spy* (1988), p. 8

"... the essence of espionage, even the most innocuous sort, is betrayal of trust. One might almost say that is the defining element, because without it, there is no espionage."

-- Aldrich Ames, CIA Traitor & Convicted Spy
as quoted in as quoted in *Confessions of a Spy* by Pete Earley

---

"Espionage is a crime of double-edged secrecy. Spies, well experienced in clandestine procedures and operating not as individuals but as agents of a nation, are hard to detect by traditional police work. And the loot that they seek is not the kind of evidence that can be labeled Exhibit A in the courtroom. …And there is still another kind of secret that a trail reveals: the failings of the secret-holder's own security safeguards"

-- Thomas B. Allen and Norman Polmar, *Merchants of Treason: America's Secret for Sale* (1988), p. 163

"No matter how overwhelming the evidence can be, prosecuting espionage cases is never easy."

-- John L. Martin, Retired Chief Counterespionage Section, US Department of Justice

Espionage Act. The Espionage Act of 1917 (18 USC § 792 et seq.) is a U.S. federal law passed in June 1917, shortly after the U.S. entry into World War I. It prohibited any attempt to interfere with military operations, to support U.S. enemies during wartime, to promote insubordination in the military, or to interfere with military recruitment. The law was further strengthen by the *Espionage and Sabotage Act of 1954*, which authorized the death penalty or life imprisonment for espionage or sabotage in peacetime as well as during wartime. The Act requires agents of foreign governments to register with the U.S. Government. It also suspended the statue of limitations for treason. In 1958, the scope of the act was broaden to cover Americans engaged in espionage against the U.S. while overseas. Also see *espionage.*

Statues now governing espionage date from the first effort to protect the governments' secrets in the Defense Secrets Act of 1911. The Espionage Act of 1917 adopted the approach take in 1911, incorporating many of its key phrases. Most of the 1917 act in turn has been incorporated without many revisions into 18 U.S. Code 793, the core statute for dealing with espionage. The last revisions in wording made to section 793 were in 1950 with the Internal Security Act; also in that act 18 U.S. Code 794 was added.

-- PERSEREC Technical Report 08-05, *Changes in Espionage by Americans: 1947-2007*, March 2008.

The Federal Espionage Laws codified in Title 18 Section 793 and 794 US Code along with other related crimes date back to the terrorist attack of 1916 on Black Tom Island carried out by the German IIIb intelligence service. This event had such an impact on the nation that proposals were made to court martial civilians since there were no viable laws to deal with espionage at the time.

The result was the 1917 Espionage Law of which codified a very restricted definition of the crime of Espionage. As you know espionage has four elements:

- *Unauthorized transmittal*
- *of national defense information*
- *to a foreign power or agent*
- *with the intent to harm the US or aid that foreign power.*

As a result of a German espionage case in the early 1940s, that was appealed, and precedence was established that the national defense security information transmitted in an espionage case had to be protected information. Accordingly, it is essential to prove in an espionage prosecution that the information affected the military defense of the United States and was protected information not in the public domain at the time it was transmitted.

-- Prepared Statement of David G. Major, President CI Centre, before the US House of Representatives, Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security "Enforcement of Federal Espionage Laws" Hearing, 29 January 2008

> *Prominent among the statutory offenses enacted by Congress and relating to matters of national security are the espionage laws found in title 18, sections 791 through 798.' The activities covered therein by these sections go far beyond those limited to any dictionary definition or popular concept of the term "espionage."*
>
> *The obtaining of national defense information for the benefit or use of foreign nations or its subsequent transmittal is the primary target of the espionage laws. However, equally as criminal is the conspiracy and attempt to do any of the above as well as the receiving or obtaining of national defense information with reason to believe that such information was to be used in violation of the espionage laws. In addition, the willful refusal to turn over national defense information upon proper demand by lawful authority and the loss or compromise of national defense information through gross negligence is also included in the statutory proscription. The penalties prescribed for violation of the espionage laws are severe.*
>
> -- Commission on Government Security – 1957, p. 617

Espionage Indicators. Warning signs that an insider may be working for or is susceptible to control by a Foreign Intelligence Entity (FIE). These warning signs are the result of an insider's actions, activities, and behaviors that may be indicative of potential espionage-related activity. Also see *indicator*.

-- Also, Potential Espionage Indicators: Activities, behavior or circumstances that may, unless satisfactorily explained, be indicative of potential espionage activity by an individual who may be acting as a witting espionage agent or spy. (DSS CI Report, Potential Espionage Indicators in Personnel Security Investigations, undated, circa early 2000)

> Mere exhibition of an espionage indicator does not necessarily indicate spying or a Foreign Intelligence Entity (FIE) connection; individuals may exhibit PEI for a variety of legitimate reasons. Presence of PEI, especially multiple PEI, warrants further CI action.
>
> In CI usage, ***Indicators are different from anomalies.*** Espionage indicators are manifested in an insider's actions, activities, and behaviors whereas anomalies surface as a result of FIE actions and activities [see *anomalies, anomalous activity, anomaly*].
> -- Indicator: an individual's action, activity or behavior
> -- Anomaly: foreign power activity or knowledge
>
> Potential Espionage Indicators alone do not presuppose that an individual is necessarily working on behalf of a FIE… additional CI follow-up is required.
>
> DoD Directive 5240.06, *Counterintelligence Awareness and Reporting*, 17 May 2011, lists reportable contacts , activities, indicators, and behaviors associated with foreign intelligence activities (FIEs), a term that includes international terrorists; for specifics see Tables 1-3 at Enclosure 4.

Essential Elements of Information (EEI). The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Essential Elements of Friendly Information (EEFI). Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. (Previously in JP 2-01, Joint and National Intelligence Support to Military Operations)

Essential Task. A specified or implied task that an organization must perform to accomplish the mission that is typically included in the mission statement. (JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *implied task; specified task*.

Estimative Intelligence. Intelligence that identifies, describes, and forecasts adversary capabilities and the implications for planning and executing military operations. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Evaluation. In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. (JP 1-02)

Evaluation and Feedback. In intelligence usage, continuous assessment of intelligence operations throughout the intelligence process to ensure that the commander's intelligence requirements are being met. (JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Evidence. Testimony, writings, material object, or other things presented to the senses that are offered to prove the existence or nonexistence of a fact.

> "***No matter how overwhelming the evidence can be, prosecuting espionage cases is never easy."***
> -- John L. Martin, Retired Chief of Internal Security at the Department of Justice

In legal proceedings there are several different types: 1) in terms of their relationship to the crime, they are known as "direct" or "circumstantial," and 2) in terms of their relationship to the world at large, they are known as "testimonial" or "physical."

TESTIMONIAL: statements or the spoken word from the victim(s) or witness(es).

PHYSICAL: includes such things as hairs, fibers, latent fingerprints, and biological material. Physical evidence is objective and when documented, collected, and preserved properly may be the only definitive way to reliably place or link someone to a crime scene. This is why Physical evidence is known as the "silent witness."

Physical evidence has the potential to play a critical role in the overall investigation and resolution of a suspected criminal act.

-- US Department of Justice,
Crime Scene Investigation: A Guide for Law Enforcement, January 2000

-- Also, anything that helps to ascertain the truth of a matter, or gives proof of a fact. Evidence may be physical or testimonial. (AR 195-5, Evidence Procedures, 25 Jun 2007)

-- Also, the legal data that conclusions or judgments may be based on. It is the documentary or verbal statements and material objects admissible as testimony in a court of law. Evidence is the means by which any alleged matter of fact is proven or disproved. Evidence includes all matters, except comment or argument, legally submitted to a court. Evidence is the source from which a court-martial or jury must form its conclusions as to the guilt or innocence of an accused. *Testimonial evidence*, e.g., sworn statements of eyewitness accounts and admissions of guilt, is obtained through communication with people. *Physical evidence*, e.g., identified weapons and fingerprints, is obtained by searching crime scenes, tracing leads, and developing technical data. Investigators must always be evidence conscious. Both physical and testimonial evidence are vital to the successful prosecution of an investigation. (Army FM 3-19.13, Law Enforcement Investigations, Jan 2005)

Evidence is the source from which a court-martial or jury must form its conclusions as to the guilt or innocence of an accused. Evidence is the means by which any alleged matter of fact is proven or disproved. Evidence includes all matters, except comment or argument, legally submitted to a court.
-- Army FM 3-19.13, *Law Enforcement Investigations*, Jan 2005, p. 1-8

-- Also, evidence in its broadest sense, refers to anything that is used to determine or demonstrate the truth of an assertion; the term has specialized meanings when used with respect to specific fields, such as criminal investigations and legal discourse. …Legal evidence concerns the tight rules governing the presentation of facts that tend to prove or disprove the point at issue. …Testimony (which tells) and exhibits (which show) are the two main categories of evidence presented at a trial or hearing. (Wikipedia; accessed 1 Aug 2007)

The law of evidence governs the use of testimony (e.g., oral or written statements, such as an affidavit) and exhibits (e.g., physical objects) or other documentary material which is admissible (i.e., allowed to be considered by the trier of fact, such as a jury) in a judicial or administrative proceeding (e.g., a court of law). Evidence must be acquired/received, processed, safeguarded and disposed of properly.

Military Rules of Evidence are Part III of the *Manual for Courts-Martial*; Appendix 22 of the MCM is Analysis of the Military Rules of Evidence.

Also see "Evidence" in Chapter 8 of Army FM 2-22.2, *Counterintelligence*, October 2009, pp. 8-5 through 8-8.

---

*"Espionage is a crime **almost** devoid of evidence…"*
-- Peter Wright, *Spycatcher* (1987)

"*While espionage may be **ALMOST** devoid of evidence, it is **NOT VOID** of evidence."*
-- *ESPIONAGE 101: Elements of Espionage* by CW4 Connie Huff (USA), 3 Dec 1996

Evidence Identifiers. Tape, labels, containers, and string tags used to identify the evidence, the person collecting the evidence, the date the evidence was gathered, basic criminal offense information, and a brief description of the pertinent evidence. (Crime Scene Investigation: A Guide for Law Enforcement, Sep 2013)

Execute Order (EXORD). 1) An order issued by the Chairman of the Joint Chiefs of Staff, by the authority and at the direction of the Secretary of the Defense, to implement a decision by the President or SECDEF to initiate military operations; 2) An order to initiate military operations as directed. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Execution Planning. The Adaptive Planning and Execution System translation of an approved course of action into an executable plan of action through the preparation of a complete operation plan or operation order. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Executive Agent (EA) [within DoD]. A term used to indicate a delegation of authority by the Secretary of Defense or Deputy Secretary of Defense to a subordinate to act on behalf of the Secretary of Defense. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Exfiltration. The removal of personnel or units from areas under enemy control by stealth, deception, surprise, or clandestine means. (JP 1-02)

-- Also, a clandestine rescue operation designed to get a defector, refugee, or operative and his or her family out of harm's way. (CI Centre Glossary)

-- Also, a clandestine operation undertaken to remove an individual from a denied area. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

-- Also, the surreptitious extraction of operatives in the field. (*Encyclopedia of the CIA*, 2003)

-- Also, an operation to get an individual secretly and illegally [in violation of a foreign country's law] out of a hostile area. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

> Examples include the escapes of KGB officer Oleg Gordievsky from the Soviet Union in 1985, orchestrated by MI6, and KGB officer Victor Sheymov, his wife, and daughter from the Soviet Union in 1980, carried out by the CIA.

Expanded-scope Screening [Polygraph]. (ESS) An examination that includes the questions from a CSP polygraph and questions related to falsification of security forms, involvement with illegal drugs, and criminal activity. Previously known as full-scope polygraph. (DoDI 5210.91, PCA Procedures, 12 Aug 2010 with change 1 dated 15 Oct 2013)

Exploitation. The process of obtaining information from any source and taking advantage of it. (DoDD 5205.02E, DoD OPSEC Program, 20 Jun 2012)

-- Also, the process of obtaining intelligence information from any source and taking advantage of it for intelligence purposes. (ODNI, U.S. National Intelligence – An Overview 2011)

Export Enforcement Coordination Center (E2C2). The primary forum within the federal government for executive departments and agencies to coordinate and enhance their export control enforcement efforts. The Center maximizes information sharing, consistent with national security and applicable laws. This helps partner agencies detect, prevent, disrupt, investigate and prosecute violations of U.S. export control laws. (www.ice.gov)

> Executive Order 13558 created the Export Enforcement Coordination Center. E2C2 provides a venue through which to deconflict technology transfer investigations,
>
> For additional information see <http://www.ice.gov/export-enforcement-coordination-center/>

Extremist Activity. As used in this regulation, an activity that involves the use of unlawful violence or the threat of unlawful violence directed against the Army, DOD, or the United States based on political, ideological, or religious tenets, principals, or beliefs. (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

Eyewash. [Tradecraft jargon] False entries made in files, usually to protect the security of a source, often indicating that a particular target has rejected a pitch, when in fact the offer was accepted. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

F ==========

Fabricator. An individual or group who, usually without genuine resources, invents or inflates information for personal or political gain or political purposes. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, an agent who furnishes false information for financial gain. (A Spy's Journey)

False Flag. Development or execution of any imitative or operation under false national sponsorship or credentials (aka "false colors"). The Russian term is foreign flag. (CIA in D&D Lexicon, 1 May 2002) Also see *false-flag approach* and *false-flag recruitment*

-- Also, occurs when an individual is recruited believing he or she is cooperating with an intelligence service of a specific country. In actuality, he or she has been deceived and is cooperating with an intelligence service of another country. (AFOSI Manual 71-119, CI Investigations, 27 Oct 2009)

-- Also, the technique for misrepresenting an individual's country of origin is a risky but well-established tactic adopted by all counterintelligence agencies in the absence of other, safer alternatives. Invariably, the strategy is one of last resort when a suspect is known to have engaged in espionage, but is thought to be currently inactive. The offer to be reengaged as a spy may be accepted and result in sufficient evidence to secure a conviction, or may prompt an incriminating action. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

-- Also, approach by a hostile intelligence officer who misrepresents himself or herself as a citizen of a friendly country or organization. The person who is approached may give up sensitive information believing that it is going to an ally, not a hostile power. (Spy Book)

-- Also, the use of a third country's nationality to effect the recruitment of an agent so they do not know an activity's true country of origin. (A Spy's Journey)

False-Flag Approach. An intelligence officer or agent who represents themselves as a person of another nationality in order to foster trust and lessen suspicion about the contact. (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010) Also see *false flag; false-flag recruitment*.

False-Flag Recruitment. A situation that occurs when an individual is recruited believing that he/she is cooperating with an intelligence eservice of a specific country, when in actually he/she has been deceived and is cooperating with an intelligence service of another country. (CI Community Lexicon) Also see *false-flag; false-flag approach*.

> *"…'false flag' recruitment—when an intelligence service recruits a target while pretending to represent another nation—a common piece of tradecraft. When you finally recruit the target, he believes he is providing information to some other nation. The Israelis have often used this technique by impersonating CIA officers when trying to recruit Arabs."*
> -- Duane R. Clarridge, *A Spy For All Seasons: My Life in the CIA* (1997), p. 97

-- Also, an individual recruited believing he/she is cooperating with an intelligence service of a specific country when, in reality, the individual has been deceived and is working on behalf of an intelligence service of another country. (ICS Glossary & AR 381-47, OFCO, 17 Mar 2006)

-- Also, recruitment of an individual under the guise of working for one entity when actually working for another entity. (HDI Lexicon, April 2008)

> Can also be used as a CI investigative technique to determine whether a suspected spy intends to or has committed espionage or other national security crimes against the United States; in this type of false flag a U.S. CI or law enforcement officer poses as an intelligence operative of a foreign power in an undercover operation. The FBI has successfully used this type of false flag operation in several espionage cases, e.g., see United States of America *v.* Stewart Davis Nozette (U.S. District Court for the District of Columbia, case number: 09-0565M)

Faraday Bag. Specialty collection bags for electronic parts with lining to protect the contents from electromagnetic forces. (Crime Scene Investigation: A Guide for Law Enforcement, Sep 2013)

FIE. See *Foreign Intelligence Entity*.

FISS. See *Foreign Intelligence and Security Service*.

Federal Bureau of Investigation (FBI). The primary investigative arm of the US Department of Justice (DoJ) with jurisdiction over violations of more than 200 categories of federal law and also a statutory member of the US Intelligence Community. The FBI's mission is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners. (www.fbi.gov)

> "*The FBI is unique in having a dual responsibility—to prevent harm to national security as a member of the U.S. Intelligence Community and to enforce federal laws as part of the Department of Justice. The Bureau reports to both the Attorney General and the Director of National Intelligence."*
>
> -- FBI, *Today's FBI – Facts and Figures 2010-2011*
>
> _____
>
> The FBI has authority to investigate threats to the national security pursuant to Presidential Executive Orders, Attorney General authorities, and various statutory sources. Per EO 12333 (US Intelligence Activities) the FBI coordinates the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States.
>
> _____
>
> "*We always thought of the FBI highly. We viewed it, this organization, as a formidable one. In the intelligence business, it's better to overestimate than underestimate, we never just thought of the FBI as incompetent or weak organization. It was an adversary, a formidable adversary, truly."*
>
> -- Oleg Kalugin, Retired KGB General (served in Washington DC and Former Chief of Line KR)

Federal Grand Jury (FGJ). An independent panel charged with determining whether there is probable cause to believe one or more persons committed a particular federal offense. If the FGJ believes probable cause exists, it will vote a "true bill" and the person will be indicted. An indictment is the most typical way a person is charged with a felony in federal court. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Federal Polygraph Examiner. Military, civilian, or contractor personnel authorized to conduct polygraph examinations on behalf of a federal agency. (DoD 5210.48, Polygraph and Credibility Assessment Program, 25 Jan 2007 with change 2 dated 15 Nov 2013)

Federally Funded Research and Development Center (FFRDC). Research and development-performing organizations that are exclusively to substantially financed by the Federal Government and are supported by the Federal Government either to meet a particular research and development objective or, in some instances, to provide major facilities at either universities or corporate or contractor locations for applied research to development purpose. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

Feed Material. Information that is usually true but unimportant given to an individual to pass to another intelligence service to maintain or enhance his value to that service. Sometimes called build-up material. (FBI FCI Terms)

Feedback. Information or intelligence provided to deception planners as to the progress of a deception operation and, ultimately, its success or failure. (CIA in D&D Lexicon, 1 May 2002)

Fifth Columnist. A subversive who acts out of secret sympathy for an enemy of his or her own country. (*Encyclopedia of the CIA*, 2003)

-- Also, people who clandestinely undermine a larger group such as a nation from within. A fifth column can be a group of secret sympathizers of an enemy that are involved in sabotage within military defense lines, or a country's borders. A key tactic of the fifth column is the secret introduction of supporters into the whole fabric of the entity under attack. (Wikipedia; accessed 9 August 2012)

> *The term was coined in 1936, during the Spanish Civil War. It was said then that the Spanish rebels had four columns of troops marching on the city of Madrid—and an additional "fifth column" of sympathizers within the city itself. Ready to take up arms at a moments' notice.*
>
> -- *Encyclopedia of the CIA* (2003)
>
> ---
>
> *In the United States at the end of the 1930s, as involvement in the European war seemed ever more likely, those who feared the possibility of betrayal from within used the newly coined term "fifth column" as a shorthand for sedition and disloyalty.*
>
> -- Wikipedia; accessed 9 August 2012
>
> ---
>
> The fifth column is *"that portion of our population which is ready to give assistance or encouragement in any form to invading or opposing ideologies."*
>
> -- Attorney General Robert H. Jackson, 1940
> (later Associate Justice of the United States Supreme Court, 1941–1954)
>
> ---
>
> ***The Communist Party of the United States is a fifth column if there ever was one.***
>
> -- J. Edgar Hoover, Director Federal Bureau of Investigation
> Testimony before Committee on Un-American Activities,
> U. S. House of Representatives, circa 1948

Financial Crimes Enforcement Network (FinCEN). An element of the Department of Treasury with the mission to safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering and other illicit activity. FinCEN administers the Bank Secrecy Act; supports law enforcement, intelligence, and regulatory agencies through sharing and analysis of financial intelligence; builds global cooperation with counterpart financial intelligence units; and networks people, ideas, and information. (website: <http://www.fincen.gov>)

> FinCEN exercises regulatory functions primarily under the Currency and Financial Transactions Reporting Act of 1970, as amended by Title III of the USA PATRIOT Act of 2001 and other legislation, which legislative framework is commonly referred to as the "Bank Secrecy Act" (BSA).

The BSA is the nation's first and most comprehensive Federal anti-money laundering and counter-terrorism financing (AML/CFT) statute. In brief, the BSA authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to take a number of precautions against financial crime, including the establishment of AML programs and the filing of reports that have been determined to have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings, and certain intelligence and counter-terrorism matters.

Financial Record. An original, its copy, or information known to have been derived from the original record held by a financial institution that pertains to a customer's relationship with the financial institution. (DoDI 5400.15, Guidance on Obtaining Information from Financial Institutions, 2 Dec 2004 w/ chg 3 Jul 2007)

Finding. A written legal determination made by the President of the United States authorizing a particular covert action important to US national security, in compliance with the Foreign Assistance Act of 1961, as amended by the 1971 Hughes-Ryan Amendment. (National HUMINT Glossary) Also see *covert action*.

The President shall approve all covert action Findings in writing. Under Section 662 of the Foreign Assistance Act of 1961, as amended, all covert actions undertaken… must be authorized by a Presidential Finding that each such operation is important to US national security.

-- National Security Decision Directive Number 159, 18 Jan 1985 (originally TS-Sensitive, declassified)

According to the Congressional Research Service, the reference to a **"presidential finding"** took on its current popular meaning when Congress adopted the Hughes-Ryan amendment to the Foreign Assistance Act in 1974. Section 662 of the statute prohibits the expenditure of appropriated funds by or on behalf of the CIA for covert actions "unless and until the President finds that each such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of such operation to the appropriate committees of Congress."

The requirements of this provision subsequently went through a series of transformations, the vestiges of which were recently codified in the Intelligence Authorization Act, FY1991, which still requires a written presidential finding satisfying certain conditions set forth in the statute for covert actions to occur. Such presidential findings, which are classified, are to be "reported to the intelligence committees as soon as possible" after being approved "and before the initiation of the covert action authorized by the finding." These findings are not published in the Federal Register or reproduced in CFR Title 3 compilations.

Firewall. A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy. . (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

FIVE EYES (FVEY). Australia, Canada, New Zealand, United Kingdom and the United States. (CAPCO and DoDI C-5240.08, CI Security Classification Guide, 28 Nov 2011)

Five Ws (also known as the Five Ws and one H). The formula for getting the "full" story on something. The maxim of the Five Ws (and one H) is that in order for a report to be considered complete it must answer a checklist of six questions, each of which comprises an interrogative word: Who, What, When, Where, Why, and How? (Wikipedia; accessed 20 Feb 2009)

Flag Officer. A term applied to an officer holding the rank of general, lieutenant general, major general, or brigadier general in the US Army, Air Force or Marine Corps or admiral, vice admiral, or rear admiral in the US Navy or Coast Guard. (JP 1-02)

Flaps and Seals. [Intelligence parlance for] the clandestine opening, reading, and resealing of either envelopes or packages without the recipient's knowledge. (Spycraft)

For or On Behalf of a Foreign Power. The determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in (a) control or policy direction; (b) financial or material support; or (c) leadership, assignments, or discipline. (AFOSI Manual 71-119, CI Investigations, 27 Oct 2009)

Force Multiplier. A capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Force Protection (FP). Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information . (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Force Protection Detachment (FPD). A CI element that provides CI support to transiting and assigned ships, personnel, and aircraft in regions of elevated threat. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 30 Dec 2010; also JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ change 1 dated 26 Aug 2011)

> The primary focus of FPDs is to provide current and actionable force protection information to the commander of "in transit" resources. FPDs were created in the aftermath of the USS Cole (DDG 67) bombing in the Port of Aden, Yemen on 12 October 2000.
>
> _____
>
> *Service counterintelligence programs are integral to force protection and must be adequately manned and funded to meet the dynamic demands of supporting in-transit forces.*
>
> -- Finding 20, *DoD USS Cole Commission Report*, 8 Jan 2001 (p. 97); p. 7 in the unclassified version.
>
> _____
>
> *The FPD primary mission is to detect and warn of threats to DoD personnel and resources in-transit at overseas locations without a permanent DoD CI presence. … FPDs shall maintain liaison contact with host nation officials to assess an operational picture of the local intelligence, terrorist, and criminal threat.*
>
> -- DoDI 5240.22, *CI Support to Force Protection,* 24 Sep 2009, pp. 7-8 (encl 3, para 5)
>
> _____
>
> *The principal responsibility of the FPD is to provide FP [force protection] services to DoD personnel, aircraft, ships and resources, as well as coordinate component FP activities. The FPD detects and warns of threats to DoD military and civilian assets in-transit at overseas locations that do not possess a permanent DoD CI presence.*
>
> -- Erika Triscari, "Force Protection Detachments, the Force Multiplier," *The Guardian*, April 2006, pp. 6-9.

Force Protection Response Group (FPRG). For specifics see DoDI S-5240.15, FPRG (U), 20 Aug 2010.

Foreign Agents Registration Act (FARA). A disclosure statute, enacted in 1938, that requires persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities. Disclosure of the required information facilitates evaluation by the government and the American people of the statements and activities of such persons in light of their function as foreign agents. (22 USC §611)

> See more on the FARA at DoJ website: <http://www.fara.gov>
>
> The FARA Registration Unit of the Counterespionage Section in the National Security Division (NSD), Department of Justice (DoJ) is responsible for the administration and enforcement of the Act. See DoJ website at <http://www.usdoj.gov/criminal/fara/index.html>

Foreign Collection Threat. Opportunity for a foreign entity or cooperating DoD personnel (an insider) to overtly, covertly or clandestinely collect information about RDA programs, technologies, system capabilities and employment methods that may enable an adversary to copy, counter, or defeat6 a capability, or inhibit, exploit, or sabotage a defense system. Within the context of [DoDI O-5240.24], the term collectively refers to threats posed by or form an insider, cyber exploitation, supply chain manipulation, an FIE [foreign intelligence entity], a foreign company, international transfers or exports of technology, and disposal of export-controlled technology. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

Foreign Computer Intrusion. The use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more U.S.-based computers. (AG Guidelines for Domestic FBI Operations, 29 Sep 2008)

Foreign Contact. Contact with any person or entity that is not a U.S. Person. (IC Standard 700-1, 4 Apr 2008)

Foreign Connection. A U.S. person has a foreign connection when a reasonable belief exists that the U.S. person is or has been in contact with, or has attempted to contact, a foreign person or representative of a foreign power for purposes harmful to U.S. national security interests; or when a reasonable belief exists that the U.S. person is acting or encouraging others to act in furtherance of the goals or objectives of a foreign person or power for purposes harmful to U.S. national security interests. (DoDD 5148.11, ATSD/IO, 24 Apr 2013)

-- Also, a foreign connection is established by a reasonable belief that a U.S. person is or has been in contact with, or has attempted to contact, a foreign person or a representative of a foreign power, or a reasonable belief that a U.S. person is acting or encouraging others to act to further the goals or objectives of a foreign person or foreign power. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

Foreign Counterintelligence Program (FCIP). Military component of the National Intelligence Program (NIP) that conducts counterintelligence activities in support of the Department of Defense. Also see *National Intelligence Program (NIP).*

> Within the National Intelligence Program (NIP) the two key national-level DoD intelligence programs are the General Defense Intelligence Program (GDIP) and the FCIP.
> -- Adapted from Dan Elkins, *Financial Management of Intelligence Resources: A Primer* (3rd Edition), May 1992

Foreign Cultural Analysis. Analysis of information on the demographics, norms, values, institutions, and artifacts of a population used to assist in anticipating the actions of that population within the operating environment. (DoDD 3600.01, Information Operations, 14 Aug 2006 with chg 1, 23 May 2011)

Foreign Denial & Deception. Foreign capabilities and techniques designed to conceal, manipulate, deny, deceive, influence, induct uncertainty, and generate gaps in U.S. intelligence capabilities and/or conceal intentions. Also see *denial; deception, military deception*.

> ***Aggressive foreign D&D efforts erode our intelligence advantage***
>
> Foreign knowledge and understanding of US intelligence capabilities are significant and growing problems across all intelligence disciplines and represent serious challenges to US national Security.
>
> ***"America's toughest adversaries know a great deal about our intelligence system and are becoming better at hiding their intentions and capabilities."***
>
> -- *The National Intelligence Strategy*, October 2005, p.9

Foreign Denial & Deception Committee (FDDC). An interagency intelligence committee that operates under the auspices of the National Intelligence Council (see ICD 204).

Foreign Instrumentation Signals Intelligence (FISINT). Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012) Also see *signals intelligence (SIGINT).*

> In the early 1980s the term TELINT (telemetry intelligence) was broadened to include other key signals that also describe missile/space events and was renamed Foreign Instrumentation Signals Intelligence (FISINT).

Foreign Intelligence (FI). Information relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence, except for information on international terrorist activities. (National Security Act §3(2), 50 USC §401a) Also see *positive intelligence*.

-- Also, information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities. (EO 12333 as amended and JP 2-0, Joint Intelligence, 22 Oct 2013)

> FI collection disciplines include: human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT), including imagery intelligence (IMINT); and measurement & signatures intelligence (MASINT).
>
> FI does not include counterintelligence. FI is one of the two components of intelligence, the other is counterintelligence (CI) per Executive Order 12333 *US Intelligence Activities* as amended and the National Security Act of 1947 as amended.

Foreign Intelligence Agent. A person other than a foreign intelligence officer, who is engaged in intelligence activities or sabotage for on the behalf of a foreign power, or international terrorist activity, or who knowingly conspires with or aids and abets such a person in these activities. (CI Community Lexicon) Also see *agent;* and *agent net.*

Foreign Intelligence and Security Service (FISS). An organization of a foreign country capable of executing all or part of the intelligence cycle. Note: sometimes referred to as FIS (Foreign Intelligence Service). Also see *foreign intelligence entity*.

-- Also, a foreign government's intelligence and security organization. (DoD FCIP Strategy FY 2013-2017)

Foreign Intelligence Collection Threat. The potential of a foreign power, organization, or person to overtly or covertly collect information about U.S. acquisition program technologies, capabilities, and methods of employment that could be used to develop a similar weapon system or countermeasures to the U.S. system or related operations. (DoD 5200.1-M, Acquisition Systems Protection Program, March 1994)

Foreign Intelligence Entity (FIE). Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service [FISS] and international terrorist organizations. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 2013; and DoDI S-5240.17, CI Collection Activities, 14 Mar 2014)

> FIE is a more encompassing term, which includes but not limited to Foreign Intelligence and Security Services (FISS), as well as Foreign Intelligence Services (FIS).

-- Also, any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, blocks or impairs U.S. intelligence collection, influences U.S. policy, or disrupts U.S. systems and programs. This term includes a foreign intelligence and security service and international terrorists. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 with change 1 dated 15 Oct 2013)

-- Also, any known or suspected foreign organization, person, or group (public, private, governmental) that conducts intelligence activities to acquire U.S. information, blocks or impairs US intelligence collection, influence US policy, or disrupts US systems and programs. This term includes foreign intelligence and security services and international terrorists. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010 with change 1 dated 16 Oct 2013) *Note: this definition is slightly different than the one above.*

-- Also, any foreign organization, person, or group (public, private, governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service as defined in Joint Publication 1-02. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

-- Also, known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and service services and international terrorists. (ICD 750, Counterintelligence Programs, 5 Jul 2013)

Foreign Intelligence Information. 1) Information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against— (a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or 2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—(a) the national defense or the security of the United States; or (b) the conduct of the foreign affairs of the United States. (Foreign Intelligence Surveillance Act of 1978; Public Law 95–511, 25 October 1978) Also see *Foreign Intelligence Surveillance Act (FISA).*

Foreign Intelligence Liaison. Activities or relationships between elements of the United States Government and elements of foreign governments or international organizations on matters involving foreign intelligence, counterintelligence, or clandestine intelligence activity.

Foreign Intelligence Officer. A member of a foreign intelligence service. (CI Community Lexicon) [Also referred to as an IO (intelligence officer)]. Also see *agent handler.*

Foreign Intelligence Service (FIS). An organization of a foreign country capable of executing all or part of the intelligence cycle. (CI Community Lexicon) Also see *Foreign Intelligence and Security Service, Foreign Intelligence Entity.*

Foreign Intelligence Entity (FIE) is a more all encompassing term which includes but is not limited to FIS.

The importance of intelligence services in the fortune of nations can't be overstated…. The existence or absence of a well-working spy network on the territory of a potential enemy may well spell the difference between victory and defeat.

-- Alexander Orlov in *Handbook of Intelligence and Guerrilla Warfare* (1963)

Foreign Intelligence Surveillance Act (FISA). [50 USC §1801 / Public Law 95-111] …the legal authority authorizing and regulating electronic surveillance within the United States for foreign intelligence or counterintelligence purposes and physicals searches within the United States for foreign intelligence purposes. The act sets out the application, order, and report process to be followed. (CI Community Lexicon) Also see *Foreign Intelligence Surveillance Court*.

Primary purpose must be collection of foreign intelligence information.

FISA prescribes procedures for the physical & electronic surveillance and collection of "foreign intelligence information" between or among "foreign powers". Subchapters of FISA provide for: electronic surveillance; physical searches; pen registers and trap & trace devices for Foreign Intelligence (FI) purposes; and access to certain business records for FI purposes. FISA does not apply to U.S. counterintelligence activities overseas.

-- FISA, codified in 50 U.S.C. §1801, et seq was amended by the FISA Amendments Act of 2008.

The Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, 92 Stat. 1783 (25 Oct 1978), 50 USC §§ 1801 et seq., provides a statutory framework for gathering **foreign intelligence information** through the use of electronic surveillance, physical searches, and pen registers or trap and trace devices, and access to business records and other tangible things, the 1978 Act dealt only with electronic surveillance.

The provisions passed almost 30 years ago became Title I of FISA. As originally enacted, the measure provided a statutory framework for collection of **foreign intelligence information** through the use of electronic surveillance of communications of foreign powers or agents of foreign powers, as those terms were defined in the act. The act has been amended repeatedly in the intervening years in an effort to address changing circumstances. Then, as now, the Congress sought to strike a balance between national security interests and civil liberties.

FISA consists of seven parts. The first authorizes electronic surveillance in foreign intelligence investigations. The second authorizes physical searches in foreign intelligence cases. The third permits the use and installation of pen registers and trap and trace devices in the context of a foreign intelligence investigation. The fourth affords intelligence officials access to business records and other tangible items. The fifth directs the Attorney General to report to Congress on the specifics of the exercise of FISA authority. The sixth, scheduled to expire on 30 December 2012, permits the acquisition of the communications of targeted overseas individuals and entities. The seventh creates a safe harbor from civil liability for those who assist or have assisted in the collection of information relating to the activities of foreign powers and their agents.

Electronic surveillance can provide vital information needed to identify those who are acting or preparing to act against U.S. interests for the benefit of foreign powers, including those engaged in espionage, sabotage, or terrorist acts or who otherwise pose a threat to the nation or its citizens, and to uncover their plans or activities. This information may not be readily uncovered by other investigative means. Thus, surveillance can provide a valuable tool for protecting the security of the nation and its citizens.

-- CRS Report RL34279: *Foreign Intelligence Surveillance Act: An Overview of Selected Issues*, 7 Jul 2008
Copy available on line at: <http://www.fas.org/sgp/crs/intel/RL34279.pdf>

Note: Under 50 USC §1801(e)(1), ***foreign intelligence information*** is information that relates to U.S. ability to protect against: 1) possible hostile acts of a foreign power or agent of a foreign power; 2) sabotage or terrorism by a foreign power or agent, and: 3) . clandestine intelligence activities by a foreign power or agent. Foreign intelligence information includes information with respect to a foreign power or foreign territory that relates to the national defense, national security, or conduct of foreign affairs of the United States.

Probable cause under FISA: *"Ordinarily, probable cause speaks to the probability of the existence of a certain fact, e.g., probable cause to believe a crime has been, is, or is about to be committed and that the search will result in the discovery of evidence or contraband. FISA authorizes issuance of a surveillance or search order predicated upon the probability of a possibility; the probability to believe that the foreign target of the order may engage in spying, or the probability to believe that the American target of the order may engage in criminal spying activities, 50 U.S.C. 1805(a)(3)(A), 1824(a)(3)(A), 1801(b)(1)(B), (b)(2)(A).3 But it is the predicate not the standard that is changed. The probable cause standard is the same in FISA as in a criminal context: would a prudent individual believe that a fact is probably true. It is the focus that is different. Would a prudent individual believe that spying may occur."*

-- CRS Memorandum (American Law Division), 30 Jan 2006

Misc. FISA References& Background

Foreign Intelligence Surveillance of 1978, 50 USC §1801 (Public Law 95-111)

Presidential Directive/NSC-19, Electronic Surveillance Abroad and Physical Searches for Foreign Intelligence Purposes, 25 Aug 1977 [declassified]; amended by POTUS via 24 Aug 1979 White House Memo [declassified]

Executive Order 12139, FISA, 23 May 1979

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (PL 110-261), 10 Jul 2008

Executive Order 12949, Foreign Intelligence Searches, 9 Feb 1995

A thorough constitutional justification of FISA can be found in *United States v. Duggan* (743 F.2d 59[2d Cir. 1984]) where both Fourth and Fifth Amendment challenges to this kind of electronic surveillance were addressed by the court.

US Senate. *The Foreign Intelligence Surveillance Act of 1978: The First Five Years*, Report 98-660, 98th Congress, 2nd Session, Washington, DC, 1984.

CRS Report R42725, *Reauthorization of the FISA Amendment s Act*, 2 Jan 2013; copy available at: <http://www.fas.org/sgp/crs/intel/R42725.pdf>

For additional FISA background see FAS website at: <http://www.fas.org/irp/agency/doj/fisa/>

Foreign Intelligence Surveillance Court (FISC) [often referred to as the "FISA Court"]. A U.S. federal court established in 1978 when Congress enacted the *Foreign Intelligence Surveillance Act* (FISA)--codified, as amended, at 50 USC §§ 1801-1885c. The Court entertains applications submitted by the U.S. Government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes.

Most of the Court's work is conducted ex parte as required by statute, and due to the need to protect classified national security information. The FISC sits in Washington D.C. and is composed of eleven federal district court judges who are designated by the Chief Justice of the United States.

Each judge serves for a maximum of seven years and their terms are staggered to ensure continuity on the Court. By statute, the judges must be drawn from at least seven of the United States judicial circuits, and three of the judges must reside within 20 miles of the District of Columbia. No judge may be appointed to this court more than once, and no judge may be appointed to both the Court of Review and the FISC. FISC Judges typically sit for one week at a time, on a rotating basis.

For additional information, see the FISC web site at: <http://www.fisc.uscourts.gov/>
-- FISC Rules of Procedures at: <http://www.fisc.uscourts.gov/rules-procedure>
-- FISC Public Findings at: <http://www.fisc.uscourts.gov/public-filings>

Foreign Intelligence Threat. The all-source intelligence threat posed by foreign intelligence entities to US interests.

Foreign Intelligence Threats

[T]he leading state intelligence threats to US interests in 2014 will continue to be Russia and China, based on their capabilities, intent, and broad operational scope. Sophisticated foreign intelligence entities will continue to employ human and cyber means to collect national security information.

-- Hon. James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, SSCI, 29 January 2014

Foreign intelligence services, along with terrorist groups, transnational criminal organizations, and other nonstate actors, are targeting and acquiring our national security information, undermining our economic and technological advantages, and seeking to influence our national policies and processes covertly. These foreign intelligence efforts employ traditional methods of espionage and, with growing frequency, innovative technical means. Among significant foreign threats, ***Russia*** *and* ***China*** *remain the most capable and persistent intelligence threats and are aggressive practitioners of economic espionage against the United States.* ***Countering such foreign intelligence threats is a top priority for the Intelligence Community for the year ahead*** *[emphasis added].*

-- Hon. James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013, p. 8

Foreign Liaison Officer (FLO). A foreign government military member or civilian employee who is authorized by his or her government to act as an official representative of that government in its dealings with the DoD and Military Services in connection with programs, projects, or agreements of mutual interest to DoD and the foreign government. (adapted from AR 380-10, 22 Jun 2005)

Three types of FLOs:

1) A *Security Assistance FLO* is a foreign government representative who is assigned to a DoD element or contractor facility pursuant to a requirement that is described in an FMS LOA;

2) An *Operational FLO* is a foreign government representative who is assigned to a DoD element pursuant to a documented requirement to coordinate operational matters, such as combined planning or training and education; and

3) A *National Representative FLO* is a foreign government representative who is assigned to his or her national embassy or legation in Washington, DC (for example, an attaché), to conduct liaison activities with DoD / Military Services.

Foreign Material. Any item of foreign origin including physical possession of, or access to, an item of foreign material or technology. (DIAM 58-4, Foreign Material Program, 22 Feb 2002)

Foreign Material Acquisition (FMA). FMP [Foreign Material Program] activities that include gaining physical possession, or access to, an item of foreign material or technology. (DoDD S-3325.01E, Foreign Material Program (U), 30 Dec 2011)

Foreign Material Exploitation (FME). FMP [Foreign Material Program] activities that include analysis, testing, evaluation, and documentation of the S&TI [Scientific & Technical Intelligence] characteristics of an item of foreign material. (DoDD S-3325.01E, Foreign Material Program (U), 30 Dec 2011)

Foreign Military Intelligence Collection Activities (FORMICA). Entails the overt debriefing, by trained HUMINT personnel, of all U.S. persons employed by the Department of Defense who have access to information of potential national security value. (DoDI C-5205.01, FORMICA (U), 22 Jan 2009; also JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Foreign National. Any person other than a US citizen, US permanent or temporary legal resident alien, or person in US custody. (JP 1-02)

-- Also, any person who is not a citizen of the U.S. (IC Standard 700-1, 4 Apr 2008)

Foreign Ownership, Control or Influence (FOCI). A U.S. company is considered under foreign ownership, control, or influence whenever a foreign interest has the power, direct or indirect, whether or not exercised and whether or not exercisable through ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information and/or special nuclear material or may affect adversely the performance of classified matters. (ISC 2008-700-1, 4 Apr 2008)

> Within DoD, see DTM 09-019, *Policy Guidance for FOCI*, 2 Sep 2009 (with chg 6 dated 9 Jan 2014)

Foreign Power. Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities. (DoD 5240.1-R, Dec 1982)

-- Also, foreign power means: (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation thereof; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments. (50 USC § 1801a). Also see *Agent of a Foreign Power.*

Foreign Service National (FSN). Foreign nationals who provide clerical, administrative, technical, fiscal, and other support at foreign service posts abroad and are not citizens of the United States. The term includes third country nationals who are individuals employed by a US mission abroad and are neither a citizen of the US nor of the country to which assigned for duty. (JP 1-02 and JP 3-68, Noncombatant Evacuation Operations, 23 Dec 2010)

Foreign Terrorist Tracking Task Force (FTTTF). A specialized task force that was created pursuant to Homeland Security Presidential Directive No. 2 and was consolidated into the FBI pursuant to the Attorney General's directive in August 2002. The FTTTF uses innovative analytical techniques and technologies that help keep foreign terrorists and their supporters out of the United States or lead to their location, detention, prosecution, or removal. The participants include DoD, Department of Homeland Security's bureaus of Immigration and Customs Enforcement (ICE) and Customs and Border Protection, State Department, Social Security Administration, Office of Personnel Management, Department of Energy, and CIA. (FBI website: <http://www.fbi.gov/congress/congress06/mueller120606.htm>)

Foreign Visits System (FVS). Automated system operated by the Office of the Under Secretary of Defense (Policy) that provides staffing and database support for processing requests for visits by foreign nationals to DoD activities and defense contractors. FVS consists of an unclassified segment that allows the online submission of visit requests from embassies in Washington, DC, and, in some cases, directly from foreign governments overseas. FVS also has a classified segment that provides staffing, decision-making support, and database capabilities to the military departments and DIA.

Forensics. [In computer / cyber usage] The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *forensic science*.

Forensic Copy. An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Forensic Science (often shortened to forensics). The application of multidisciplinary scientific processes to establish facts. (DoDD 5205.15E, DoD Forensic Enterprise, 16 Apr 2011) Also see *digital & multimedia forensics, digital evidence*, and *digital forensics*.

> The Secretary of the Army is the DoD Executive Agent (EA) for Forensics, specifically for those forensic disciplines relating to deoxyribonucleic acid (DNA), serology, firearms and tool marks, latent prints, questioned documents, drug chemistry, and trace materials, as well as forensics relating to forensic medicine disciplines such as forensic pathology, forensic anthropology, forensic toxicology, and DNA analysis to identify human remains.
>
> The Secretary of the Air Force is the DoD EA for Digital and Multimedia (D/MM) Forensics, specifically for those forensics disciplines relating to computer and electronic device forensics, audio forensics, image analysis, and video analysis.

Forensic-Enabled Intelligence (FEI). The intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest. (JP 2-0, Joint Intelligence, 22 Oct 2013.

FORMICA. See *Foreign Military Intelligence Collection Activities*.

FOUR EYES (ACGU). Australia, Canada, United Kingdom, and the United States. (CAPCO)

Front. [In intelligence usage] a legitimate operation created by an intelligence organization as a cover for its operatives. (*Encyclopedia of the CIA*, 2003)

-- Also, Front Company [in law enforcement/criminal investigation usage] a company or business entity that is established, used, or co-opted for an illicit purpose; wherein the management, control, influence or criminal activities are being directed by a hidden or disguised individual or group. (Colin A. May, M.S., CFE, U.S. Department of Commerce, Sep 2010)

> For additional information see Colin A. May, "Front Companies: Challenges and Tools in Criminal Investigations," *IALEIA Journal*, Vol. 19, No. 1, pp. 101-120, September 2010. The *IALEIA Journal* is published by the International Association of Law Enforcement Intelligence Analysts, Inc.,
>
> > According to Colin May (in his article cited above, p. 102),*"many people use the phrase 'front company' when they are really describing the front company's distant cousin—the Shell Company. The Financial Crimes Enforcement Network… defines shell companies as 'limited liability companies and other business entities with no significant assets or ongoing business activities.' The shell simply is a paper company; they have also been called "International Business Corporations (IBCs)" or 'shelf companies,' since in some off-shore jurisdictions, the incorporators already have created the companies and simply pull them off the shelf to change the beneficial owner. The difference cannot be overstated…."*
> >
> > *"Front companies conduct actual business—shells do not.* [Shells] *are simply paper companies. Front companies have tangible operations, although they may be illicit or illegitimate, they are definite business transactions. The main difference that many investigators and intelligence analysts seem to miss is the 'action' piece in a front company—and that, of course, is highly dependent on the criminal's intended purpose for the front company. A shell, used by a criminal, disguises their involvement in the business, but the shell has no actual operations, whereas the front company does."*
>
> Also see Defense Security Service (DSS) article "Front Companies: Who is the End User?" at: <http://www.dss.mil/isp/count_intell/front_comp_who_user.html>

Full Field Counterintelligence Investigation. An investigation which is conducted when there are specific and articulable facts giving reason to believe that a person over whom Army counterintelligence has jurisdiction may be involved in acts that may constitute threats to national security. (AR 381-20, Army CI Program, 25 May 2010) See *CI Investigation*.

> Within the FBI referred to as "Full Investigation" which may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or collect foreign intelligence. These cases may be opened if there is an "articulable basis" of possible criminal or national threat activity.
>
> The Investigation of threats to the national security can be investigated under FBI's criminal investigation authority or its authority to investigate threats to the national security. A Full Investigation solely for the collection of positive foreign intelligence extends the sphere of the FBI's information gathering activities beyond federal crimes and threats to the national security and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States' foreign affairs.
>
> -- FBI's Domestic Investigation and Operations Guide (redacted copy), 15 Oct 2011

Full-Spectrum Counterintelligence Activities. Full array of CI activities – both offensive & defensive – that can be applied in executing CI effects-based operations to achieve strategic outcomes in peacetime, crisis, war and post conflict activities (e.g., stabilization operations/reconstruction efforts). These activities support national security objectives, as well as defense decision-makers and the Combatant Commanders.

Functional Component Command. A command normally, but not necessarily, composed of forces of two or more Military Departments which may be established across the range of military operations to perform particular operational missions that may be of short duration or may extend over a period of time. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Functional Managers. Executive Order 12333 designates three Functional Managers: Director CIA for human intelligence (HUMINT), Director NSA for signals intelligence (SIGINT), and Director NGA for geospatial intelligence (GEOINT), (EO 12333, para 1.3 (b)(12)(A)(i-iiii)) See ICD 113, *Functional Managers*.

> Pursuant to EO 12333, Functional Managers report to the DNI concerning the extent of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; setting training and tradecraft standards; and ensuring coordination within and across intelligence disciplines and IC elements and with related non-intelligence activities.
>
> Functional Managers may also advise on resource management; policies and procedures; collection capabilities and gaps; intelligence processing and dissemination; technical architectures; and other issues or activities, as applicable.
>
> Note: The National Counterintelligence Executive (NCIX) is the Mission Manager for CI.

Functional Support [Analytical Product]. A type of CI analytical product that supports the specific needs of a Defense CI Component. A functional support product is related to the CI functions of collection, investigation, OFCO {Offensive Counterintelligence Operation], and functional services as described in DoDI 5240.16. The depth and comprehensiveness varies depending on the requestor's requirements. An investment in analytical effort may be significant. The production timeline ranges from hours to weeks, but can vary widely depending on the function the analysis supports. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013) Also see *Counterintelligence Analytical Product*.

Functional Support Plan (FSP). Annexes to the National Intelligence Support Plan (NISP) [that] describe how service intelligence centers and Combat Support Agencies support COCOM plans. (Adaptive Planning Roadmap II, 5 Mar 2008) Also see *Counterintelligence Functional Support Plan (CI FSP).*

> Director DoD Counterintelligence Field Activity (CIFA)* will *"fully integrate CI into the intelligence campaign planning process by developing and updating the CI functional support plans."*
> -- DUSD (CI&S) memo, subj: Counterintelligence Support to COCOMs, 29 Dec 2006
> * Note: CIFA's mission and functions transitioned into DIA effective 3 August 2008.

Fusion. In intelligence usage, the process of managing information to conduct all-source analysis and derive a complete assessment of activity. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, consolidating, combining, and correlating information together. (ADRP 2-0, Intelligence, Aug 2012)

Fusion Center. A State and major urban area focal point for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government, SLTT, and private sector partners. (Source: DHS in the National Infrastructure Protection Plan 2013)

G ==========

Gap. See *intelligence gap*.

GAMA (G). Unclassified term used to describe a type of sensitive compartmentalized information (SCI). (Words of Intelligence, 2nd Edition, 2011)

General Defense Intelligence Program (GDIP). An integrated Defense Intelligence capability that includes DIA, the Service technical production centers, and special collection activities. The GDIP integrates and produces National Intelligence for Defense and national Consumer's. It represents the national Defense Intelligence priorities for operational customers, national and Defense-wide collection management, All-Source Analysis, HUMINT, MASINT, IT, and Special Activities. The GDIP is an integrated capability, and the Director, DIA, serves as the Program Manager. The GDIP is part of the NIP, as defined in EO 12333. The GDIP may include other NIP activities as agreed between the Secretary of Defense and the DNI. (DoDI 5105.21, DIA, 18 Mar 2008) Also see *National Intelligence Program*.

> The GDIP is the broadest-based NIP program within the Department Of Defense and the military services. This program funds all national-level military intelligence units and activities that involve something other than cryptology, counterintelligence, and certain types of specialized reconnaissance, The GDIP funds intelligence production, collection, and infrastructure, which includes all defense intelligence production, all national-level DoD Human Source Intelligence (HUMINT), etc.
>
> -- Adapted from Dan Elkins, *Financial Management of Intelligence Resources: A Primer* (3rd Edition), May 1982, pp. 13-14

General Military Intelligence (GMI). Intelligence concerning the military capabilities of foreign countries or organizations, or topics affecting potential United States or multinational military operations. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *intelligence; military intelligence*.

General Support (GS). That support which is given to the supported force as a whole and not to any particular subdivision thereof. (JP 1-02) Also see *direct support*.

Geospatial Information. Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products. (JP 2-03, GEOINT Support to Joint Operations, 22 Mar 2007)

> See Congressional Research Report (CRS) R41825 (18 May 2011) for an unclassified primer on geospatial data & geographic information systems: <http://www.fas.org/sgp/crs/misc/R41825.pdf>

Geospatial Information and Services (GI&S). The collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the Earth's surface. Geospatial services include tools that enable users to access and manipulate data, and also include instruction, training, laboratory support, and guidance for the use of geospatial data. (DoDD 5105.60, NGA, 29 Jul 2009 and JP 2-03, GEOINT Support to Joint Operations, 22 Mar 2007)

Geospatial Intelligence (GEOINT). The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. (ICD 1, 1 May 2006; also JP 1-02 and JP 2-03, GEOINT Support to Joint Operations, 22 Mar 2007)

-- Also, intelligence derived from the exploitation of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. (ODNI, U.S. National Intelligence – An Overview 2011)

> *The Intelligence Community refers to the use and analysis of geospatial information to assess geographically referenced activities on Earth as geospatial intelligence (GEOINT). It is everything you can see or know about the earth. GEOINT consists of: Imagery - a likeness of any natural or man-made feature, as well as its location; Imagery Intelligence (IMINT) – information derived through interpreting imagery; and Geospatial Information – information that identifies a natural or constructed feature on Earth by its geographic location and other characteristics.*
>
> -- www.cia.gov (accessed 30 Nov 2010)
>
> ---
>
> *GEOINT collection encompasses all aspects of: literal, infrared (IR), and synthetic aperture radar (SAR) imagery; overhead persistent infrared capabilities; and geospatial information and services. GEOINT includes the exploitation and analysis of electro-optical, IR, and radar imagery; and of geospatial, spectral, laser, IR, radiometric, SAR phase history, polarimetric, spatial, and temporal data. It employs all ancillary data, signature information, and fused data products, as necessary. Integrated GEOINT products may also include data and information from collateral sources.*
>
> -- DoDD 5105.60, *NGA*, 29 Jul 2009
>
> ---
>
> *GEOINT is typically gathered from commercial satellites, government satellites, reconnaissance aircraft, or by other means such as maps, commercial databases, census information, GPS waypoints, utility schematics, or any discrete data that have locations on earth. This data is utilized to support our national security, which includes everything from assisting soldiers on the battlefield to assisting humanitarian and disaster relief efforts.*
>
> -- www.intelligence.gov (accessed 13 Aug 2012)

Ghost Surveillance. Extremely discreet and seemingly omnipresent surveillance, working mostly out of the view of the target. (CI Centre Glossary) Also see *surveillance*.

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010)

Global Force Management (GFM). The ability to align force apportionment, assignment, and allocation methodologies in support of the National Defense Strategy and joint force availability requirements; present comprehensive insights into global availability and operational readiness of U.S. military forces; globally source joint force requirements; and provide senior decision-makers a vehicle to quickly and accurately assess the impact and risk of proposed allocation, assignment, and apportionment changes. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Global Positioning System (GPS). A satellite-based radio navigation system operated by the Department of Defense to provide all military, civil, and commercial users with precise positioning, navigation, and timing. Also called GPS. (JP 1-02 and JP 3-14, Space Operations, 6 Jan 2009)

Goldwater-Nichols Act (GNA). The Goldwater-Nichols Department of Defense Reorganization Act of 1986 (PL 99-433), sponsored by Sen. Barry Goldwater and Rep. Bill Nichols, was a major reorganization of U.S. defense institutions and processes. Operational authority was centralized through the Chairman of the Joint Chiefs of Staff as opposed to the service chiefs. The Chairman was designated as the principal military advisor to the President, National Security Council, and Secretary of Defense. The act

established the position of vice-chairman and streamlined the operational chain of command from the President to the Secretary of Defense to the Unified Commanders.

> For additional information see <http://www.ndu.edu/library/goldnich/goldnich.html>
> Copy of PL 99-443 at <http://www.au.af.mil/au/awc/awcgate/congress/title_10.htm>

Gray Literature (aka Grey Literature). Material not well covered by conventional book trade channels. Gray literature is intrinsically more difficult to identify, acquire, process, access, and otherwise handle than conventional literature. Examples include but are not limited to conference papers, trade literature, electronic bulletin boards, and foreign government reports. The information that grey literature contains is not available in any kind of source. (Words of Intelligence, 2nd Edition, 2011)

Gray List. Contains the identities and locations of those personalities whose inclinations and attitudes toward the political and military objectives of the United States are obscure. Regardless of their political inclinations or attitudes, personalities may be listed on gray lists when they are known to possess information or particular skills required by US forces. They may be individuals whose political motivations require further exploration before they can be utilized effectively by US forces. (CI Community Lexicon) Also see *Black List; White List.*

-- Also, a list of those foreign personalities of operational interest whose inclinations and attitudes toward the political and military objectives of the United Sates are unknown. (HDI Lexicon, April 2008)

> Regardless of their leanings, personalities may be on gray lists when known to possess information or particular skills required by friendly forces. They may be individuals whose political motivations require further exploration before they can be used effectively. Examples of individuals who may be included in this category are:
> 1) Potential or actual defectors from the hostile cause whose credibility has not been established.
> 2) Individuals who have resisted, or are believed to have resisted the enemy government and who may be willing to cooperate with friendly forces, but whose credibility has not been established.
> 3) Nuclear, biological, chemical and other scientists and technicians suspected of having been engaged in enemy weapons of mass destruction and other programs against their will.
> -- USMC, MCWP 2-6 (previously 2-14), Counterintelligence, 5 Sep 2000

Graymail. Threat by a defendant in a trail to expose intelligence activities or other classified information if prosecuted. (Spy Book) Also see *Classified Information Procedures Act (CIPA).*

> "Graymail" colloquially refers to situations where a defendant may seek to introduce tangentially related classified information solely to force the prosecution to dismiss the charges against him.
>
> A criminal prosecution involving classified information may cause tension between the government's interest in protecting classified information and the criminal defendant's right to a constitutionally valid trial. In some cases, a defendant may threaten to disclose classified information in an effort to gain leverage.
>
> Concerns about this practice, referred to as "graymail," led the 96th Congress to enact the *Classified Information Procedures Act* (CIPA) to provide uniform procedures for prosecutions involving classified information.

Green Door. Slang term for the metaphorical locked door behind which intelligence personnel are said to hide their codeword secrets and important information not shared with consumers who need and should get it. (Words of Intelligence, 2nd Edition, 2001)

Groupthink. A decision-making flaw that occurs when a group does not consider alternatives and desires unanimity at the expense of quality decisions. Groupthink can lead to seeking out few alternative solutions because there is an illusion of group invulnerability ("we all can't be wrong'). Some symptoms of groupthink are the absence of critical discussion of information, a sharing of stereotypes to guide decisions, a strong moral climate, and the suppression of true feelings among the participants in the group. (Words of Intelligence, 2nd Edition, 2011)

GRU. *Glavnoye Razvedyvatel'noye Upravlenie* (Chief Intelligence Directorate of the General Staff); aka Russian Military Intelligence.

Russian military intelligence has a spy network abroad that is believed by espionage experts to be several times bigger than that of Russia's Foreign Intelligence Service.

-- Reuters, 24 Apr 2009

Also see Viktor Suvorov's (alias for GRU defector Vladimir Bogdanovich Rezun) books: *Aquarium* (Аквариум), 1985 and *Inside Soviet Military Intelligence*, 1984.

Guerrilla Force. A group of irregular, predominantly indigenous personnel organized along military lines to conduct military and paramilitary operations in enemy-held, hostile, or denied territory. (JP 1-02 and JP 3-05, Special Operations, 18 Apr 2011)

H ==========

Hacker. Unauthorized user who attempts to or gains access to an information system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a person who creates and modifies computer software and hardware, including computer programming, administration, and security-related items. This can be done for either negative or positive reasons. Criminal hackers create malware in order to commit crimes. (McAfee.com; accessed 15 Nov 2010)

> In computer security usage, a term used for a person who accesses a computer system by circumventing its security system.

Hacktivism. The nonviolent use of ambiguous digital tools in pursuit of political ends; these tools include website defacements, redirects, denial-of-service attacks, information theft, website parodies, virtual sit-ins, virtual sabotage, and software development. (<en.wikipedia.org/wiki/Hacktivists>; accessed 2 Apr 2009) Also see *hacktivists*.

> Hacktivism is the use of cyber instruments for political or ideological purposes.
>
> Hacktivism is a controversial term. Some argue it was coined to describe how electronic direct action might work toward social change by combining programming skills with critical thinking. Others use it as practically synonymous with malicious, destructive acts that undermine the security of the Internet as a technical, economic, and political platform**.**
>
> The term "hackitivism" first appeared in 1998, when members of a hacker group called the Cult of the Dead Cow used it as they chatted online about hacking and political liberation while discussing ideas to work with Chinese hackers following the Tiananmen Square protests.
>
> For additional information see McAfee White Paper, "Cybercrime and Hacktivism" (undated), available online at: <www.mcafee.com/us/resources/white-papers/wp-cybercrime-hactivism.pdf>

Hacktivists. Individuals who hack or attack Web sites and computer systems to communicate an ideological, social, or political message and further their cause. (FBI, Nov 2012) Also see *hacktivism*.

> *Hacktivists continue to target a wide range of companies and organizations in denial-of-service attacks…. Most hacktivists use short-term denial-of-service operations or expose personally identifiable information held by target companies, as forms of political protest. However, a more radical group might form to inflict more systemic impacts—such as disrupting financial networks—or accidentally trigger unintended consequences that could be misinterpreted as a state-sponsored attack.*
>
> -- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 12 March 2013

Handler. An intelligence officer or co-opted worker directly responsible for the operational activities of an agent; also agent handler or case officer. (CI Community Lexicon) Also see *agent handler; case officer.*

-- Also, an intelligence collector directly responsible for the operational activities of an agent, source, or asset. (HDI Lexicon, April 2008)

Hard Target. A person, nation, group, or technical system often hostile to the US or heavily protected, with a well-honed counterintelligence capability that presents a potential threat to the US or its interests, and provides significant difficulty for agent infiltration or penetration. (National HUMINT Glossary)

Harmony. The Intelligence Community's centralized database for foreign military, technical and open-source documents and their translations. Harmony is managed by the US Army's National Ground Intelligence Center (NGIC). Also see *DOMEX; DOCEX*.

Hawala. The word comes originally from the Arabic language and means transfer or remittance. (US Department of Treasury)

> *Hawala provides a fast and cost-effective method for worldwide remittance of money or value, particularly for persons who may be outside the reach of the traditional financial sector. In some nations hawala is illegal, in others the activity is considered a part of the "gray" economy. It is therefore difficult to accurately measure the total volume of financial activity associated with the system, however, it is estimated that the figures are in the tens of billions of dollars, at a minimum. Officials in Pakistan, for example, estimate that more than $7 billion flow into the nation through hawala channels each year. Other Alternative Remittance or Informal Value Transfer Systems include "hundi," "fei ch 'ien," "chit system," "poey kuan" and the black market peso exchange.*
>
> -- US Department of Treasury web site, accessed 19 Nov 2012 <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Hawala-and-Alternatives.aspx>

Hazard or Hazardous Condition. [In TSCM] a condition, either technical or physical, that could permit the exfiltration and exploitation of information. (DoDI 5240.05, TSCM, 3 Apr 2014)

Hazards. [In critical infrastructure protection usage] non-hostile incidents such as accidents, natural forces, and technological failure that cause loss or damage to infrastructure assets. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Hello Number. Tradecraft jargon for a cutout telephone where the speaker does not identify himself or his/her location. This procedure is used by proprietaries, devised facilities or cover offices of clandestine intelligence agencies for certain types of contacts with agents or affiliated personnel, usually in an emergency, and only information given by the caller over the phone is a codeword or danger signal to be relayed to the appropriate case officer for immediate call-back or other pre-arranged action. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Heuristics. Normal, intuitive mental shortcuts for processing information. They can be effective aids for problem-solving, but can lead to biases and thus to analytic errors.

High-Payoff Target (HPT). A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets that must be acquired and successfully attacked for the success of the friendly commander's mission. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007) Also see *high-value target; target.*

High-Risk Personnel (HRP). Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

High-Value Detainee Interrogation Group (HIG). The interagency body under the administrative control of the Federal Bureau of Investigation that was established to assemble and dispatch mobile interrogation teams to interrogate high-value detainees. (DoDD 3115.13, DoD Support to the High-Value Detainee Interrogation Group, 9 Dec 2010 w/ chg 1 dated 15 Nov 2013)

-- Also, an interagency body that collects intelligence from key terror suspects to prevent attacks against the United States and its allies. (www.fbi.gov) Also see *National Security Branch*.

> *In response to Task Force recommendations from Executive Order 13491, Ensuring Lawful Interrogations, the High-Value Detainee Interrogation Group was created in 2009 to coordinate law enforcement, military, and intelligence efforts in interrogating key terror suspects. The HIG is housed in the FBI's NSB [National Security Branch], and staffed with members from various IC [Intelligence Community] agencies.*
>
> -- FBI web site at <http://www.fbi.gov/about-us/nsb/national-security-branch-brochure>

High-Value Target (HVT). A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007) Also see *high-payoff target* and *target.*

HOCNet. HUMINT Operational Communication Network (HOCNet) provides information technology, communications, and desktop services for DoD HUMINT needs. (National Intelligence: A Consumer's Guide - 2009)

Homegrown Violent Extremist (HVE). A person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization. (FBI & DHS, cited in CRS Report R42536, 15 May 2012)

> *"HVEs are growing threat to the DoD, as evidenced by numerous disrupted plots targeting DoD facilities, installations, and personnel since 2009. The majority of HVE plots are unsophisticated, use readily available weapons, and target nearby facilities. While they are less likely to generate spectacular, mass casualty attacks than transnational terror groups, HVE attacks are considerably more difficult for law enforcement and intelligence agencies to detect and disrupt."*
>
> -- LTG Michael Flynn, Director, DIA, Annual Threat Assessment [Unclassified], Statement before the Senate Armed Services Committee, 18 April 2013, p.10

Homegrown Terrorist. As defined by the Congressional Research Service, homegrown describes terrorist activity or plots perpetrated within the United States or abroad by American citizens, legal permanent residents, or visitors radicalized largely within the United States. (CRS Report R41416, 23 Jan 2013)

> *American Jihadist Terrorism: Combating a Complex Threat*, CRS Report R41416, 23 Jan 2013 available online at: <http://www.fas.org/sgp/crs/terror/R41416.pdf>
>
> ---
>
> *The term "homegrown terrorism" means the use, planned use, or threatened use, of force or violence by a group or individual born, raised, or based and operating primarily within the United States or any possession of the United States to intimidate or coerce the United States government, the civilian population of the United States, or any segment thereof, in furtherance of political or social objectives.*
>
> -- House Bill 1955, 110th Congress, 24 Oct 2007
>
> ---
>
> *[T]he long war on terrorism is far from over. Most disturbingly, an increasing number of Islamist-inspired terrorist attacks are originating within America's borders. The rise of homegrown extremism is the next front in the fight against terrorism and should be taken seriously by the Administration.*
>
> -- The Heritage Foundation, Special Report No. 137, *60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism*, 22 July 2013

Homeland. The physical region that includes the continental United States, Alaska, Hawaii, United States territories, and surrounding territorial waters and airspace. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

Homeland Defense (HD). The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression, or other threats as directed by the President. (JP 1-02 and JP 3-27, Homeland Defense, 29 Jul 2013)

Homeland Security (HS). A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur. (JP 3-27, Homeland Defense, 29 Jul 2013)

-- Also, a concerted national effort to prevent terrorist attacks within the United Sates, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (National Strategy for Homeland Security, Oct 2007).

-- Also, describes the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border control, and immigration. (Quadrennial Homeland Security Review Report, Feb 2010)

-- Also, defensive efforts to counter terrorist threats. (National Strategy for Counterterrorism, 2011)

> In the years since 9/11, homeland security has become commonly and broadly known as both a term and as a Federal department.
>
> *Homeland security is a concerted effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive. Ultimately, homeland security is about effectively managing risks to the Nation's security.*
>
> -- Quadrennial Homeland Security Review Report, Feb 2010
>
> The *Quadrennial Homeland Security Review Report* (Feb 2010) is available online at: <http://www.dhs.gov/xabout/gc_1208534155450.shtm>
>
> ---
>
> According a Jan 2013 Congressional Research Service (CRS) report, the U.S. government does not have a single definition for "homeland security." Currently, different strategic documents and mission statements offer varying missions that are derived from different homeland security definitions. The concept of homeland security has evolved over the last decade.
>
> -- See CRS Report R42462, 8 Jan 2013 (accessed 9 Jan 2013)
> copy available at: <http://www.fas.org/sgp/crs/homesec/R42462.pdf>

Homeland Security Information. Any information possessed by a Federal, State, or local agency that: a) relates to the threat of terrorist activity; b) relates to the ability to prevent, interdict, or disrupt terrorist activity; c) would improve the identification or investigation of a suspected terrorist organization; or d) would improve the response to a terrorist act. (Homeland Security Act, § 891)

Honey Pot. A trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource of value to attackers. (JP 1-02 and JP 3-13.4, Military Deception)

-- Also, a system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, in computer terminology, a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network but which is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource that would be of value to attackers. (Wikipedia; accessed 18 Jan 2011)

Honey Trap. The term universally applied to operations undertaken to ensnare an unwary target in a compromising sexual encounter that may leave the victim vulnerable to blackmail that might result in espionage. (*Historical Dictionary of Cold War Counterintelligence*, 2007) .

-- Also, slang for use of men or women in sexual situations to intimidate or snare others. …[U]se of sex to trap or blackmail an individual…. (Spy Book)

-- Also, an often-used espionage technique wherein a person is deliberately targeted for sexual entrapment. (*Encyclopedia of the CIA*, 2003)

> *Pravda* (the Russian news organization) reported on the use of sexual blackmail by the KGB (Soviet Foreign Intelligence Service), see "KGB Sex Espionage," *Pravda*, 7 Aug 2002.
>
> ---
>
> Honey Trap -- *a strategy regularly adopted by the KGB's Second Chief Directorate which routinely attempted to entrap Western businessmen, foreign diplomats, and other visitors in Moscow, the techniques included the deployment of attractive women, known as "Swallows," and men, referred to as "Romeos," who homed in on vulnerable women, often lonely secretaries with access to classified information.*
>
> -- Nigel West, *Historical Dictionary of Cold War Counterintelligence*, 2007, p. 155
>
> ---
>
> The use of sex is *"a common practice among intelligence services all over the world. This is a tough dirty business. We have used that technique against the Soviets. They have used it against us."*
>
> -- Former Assistant FBI Director William C. Sullivan
> Testimony before the Church Committee, United States Senate, 1 November 1975

Horizontal Identification. [Proposed DoD definition] consistent determination of CPI across two or more RDA programs as a result of a former CPI identification process. (*Draft* 5200.39 CPI Identification and Protection within RDA Programs)

Horizontal Integration. Processes and capabilities to acquire, synchronize, correlate, and deliver National Security Community data with responsiveness to ensure success across all policy and operational missions. (CJCSI 3340.02, Horizontal Integration of Warfighter Intelligence, 23 Dec 2005)

Horizontal Protection. The process which ensures that critical program information (CPI) associated with two or more acquisition programs is protected to the same degree by all responsible DoD agencies. (AR 381-20, Army CI Program, 25 May 2010) Also see *critical program information*.

-- Also, [proposed DoD definition] application of a consistent level of protection to similar CPI associated with more than one RDA program, including inherited CPI. (*Draft* DoDI 5200.39, CPI Identification and Protection within RDA Programs)

Horizontal Protection Analysis. The process that determines if critical Defense technologies, to include CPI [critical program information], associated with more than one RDA [research, development & acquisition] program are protected to the same degree by all involved DoD activities. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008 with change 1 dated 28 Dec 2010)

> Horizontal protection within DoD is focused on ensuring that research, development and acquisition (RDA) information associated with more than one research and technology activity or acquisition program is protected to the same degree by all DoD activities, or is adequately protected based on the impact of an aggregation of the correlated information.

Host Country. A nation which permits, either by written agreement or official invitation, government representatives and/or agencies of another nation to operate, under specified conditions, within its borders. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 chg 1 dated 26 Aug 2011)

Host Nation (HN). A nation that receives the forces and/or supplies of allied nations, coalition partners, and/or NATO organizations to be located on, to operate in, or to transit through its territory. (JP 1-02)

Host-Nation Support (HNS). Civil and/or military assistance rendered by a nation to foreign forces within its territory during peacetime, crises or emergencies, or war based on agreements mutually concluded between nations. (JP 1-02 and JP 4-0, Joint Logistics, 18 Jul 2008)

Hostage Rescue (HR). A personnel recovery method used to recover isolated personnel who are specifically designated as hostages. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Hostile Act. An attack or other use of force against the United States, United States forces, or other designated persons or property to preclude or impede the mission and/or duties of United States forces, including the recovery of United States personnel or vital United States Government property. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

Hostile Environment. Operational environment in which hostile forces have control as well as the intent and capability to effectively oppose or react to the operations a unit intends to conduct. (JP 1-02)

Hostile Intent. The threat of imminent use of force against the United States, United States forces, or other designated persons or property. (JP 1-02 and JP 3-01, Countering Air and Missile Threats, 23 Mar 2012)

HotR. DoD acronym for HUMINT On-Line Tasking and Reporting System. HotR is a web-based software application that supports DoD HUMINT, as well as DoD Counterintelligence.

House Permanent Select Committee on Intelligence (HPSCI). A committee of the US House of Representatives, established by House Resolution 658 on July 14, 1977. It is the primary committee in the U.S. House of Representatives charged with the oversight of the US Intelligence Community and intelligence-related activities of all other government organizations. Also see *Senate Select Committee on Intelligence.*

> The 1980 Intelligence Oversight Act charged the Senate Select Committee on Intelligence and HPSCI with authorizing the programs of US intelligence agencies and overseeing their activities.
>
> *It is IC policy that IC elements shall, in a timely manner, keep the Congressional intelligence committees fully informed, in writing, of all significant anticipated intelligence activities, significant intelligence failures, significant intelligence activities, and illegal activities.*
>
> -- ICD 112, *Congressional Notification*, 16 Nov 2011

Human Derived Information (HDI). Activities related to the conduct of the collection of intelligence information by or through humans. It includes the following forms of information: FI, CI, Force Protection, Research and Technology Protection, and Law Enforcement. (SECNAVINST S3821.1, 19 Nov 2008)

Human Domain. The presence, activities, social structure or organization, networks and relationships, motivation, intent, vulnerabilities and capabilities of individuals or groups.

> *The human domain encompasses the totality of the physical, cultural, and social environments that influence human behavior. Success in the human domain will depend upon understanding the human terrain and establishing trust with those humans who occupy that space.*
>
> -- Navy Adm. William H. McRaven, Commander, US Special Operations Command, 5 June 2013
>
> ---
>
> *The Human Domain, or Human Dimension, which is a vital and integral part of ABI [Activity Based Intelligence], is defined as the presence, activities (including transactions - both physical and virtual), culture, social structure/organization, networks and relationships, motivation, intent, vulnerabilities, and capabilities of humans (single or groups) across all domains of the operational environment (Space, Air, Maritime, Ground, and Cyber).*
>
> -- Mark Phillips, "A Brief Overview of Activity Based Intelligence and Human Domain Analytics," (Sep 2012); copy at: <http://trajectorymagazine.com/images/winter2012/A_Brief_Overview_of_ABI.pdf>

Human Enabled Information (HEI). Activities designed to spot, assess and develop platforms which facilitate information collection and other assigned operations. (SECNAVINST S3821.1, 19 Nov 2008)

Human Factors. The physical, cultural, psychological, and behavioral attributes of an individual or group that influence perceptions, understanding, and interactions. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *human domain*.

Human Intelligence (HUMINT). A category of intelligence derived from information collected and provided by human sources [includes HUMINT enabling]. (ICD 1, 1 May 2006; JP 1-02; JP 2-0, Joint Intelligence, 22 Oct 2013; and DoDD S-5200.37, Management and Execution of Defense HUMINT, 9 Feb 2009)

-- Also, a category of intelligence derived from information collected by USG civilian employees or military personnel. Who are trained and certified HUMINT collectors, and assigned to an organization with the mission and authority to collect foreign intelligence from human sources in response to validated intelligence requirements. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, intelligence derived from information collected and provided by human sources. This intelligence includes overt data collected by personnel in diplomatic and consular posts, as well as otherwise unobtainable information collected via clandestine sources of information, debriefings of foreign nationals and U.S. citizens who travel abroad, official contacts with foreign governments, and direct observation. (National Intelligence: A Consumer's Guide - 2009)

-- Also, [from CIA perspective] vital information from human sources acquired by Core Collectors of the National Clandestine Service in response to national intelligence requirements. (www.cia.gov, posted 23 Mar 2009) Also see *national clandestine service*.

-- Also, the collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities. (Army FM 2-0, Intelligence 23 Mar 2010 and FM 2-22.2, CI, Oct 2009)

-- Also, consists of information obtained from individuals who know or have access to sensitive foreign information that has implications for U.S. security interests. (WMD Report, 31 Mar 2005)

-- Also, a category of intelligence, that which is reported by a government information collector, who has obtained it either directly or indirectly from a human source. (IC21, HPSCI Staff Study, 9 Apr 1996)

HUMINT collection is a science and an art.
-- Army FM 2-22.3, *Human Intelligence Collector Operations*

HUMINT – espionage – is the heart of the spy business

Core Mission: Collect foreign intelligence through human sources to fill critical intelligence gaps.

Human Intelligence (HUMINT) is intelligence derived from human beings who may act as both sources and collectors, and where the human is the primary collection instrument. It is a foreign intelligence (FI) collection discipline. HUMINT collectors focus on acquiring information from individuals with access to vital intelligence on the full range of national security issues.

There are two basic types of HUMINT: overt and clandestine. Overt HUMINT methods include, but are not limited to, debriefing, interrogation, elicitation, and observation. Clandestine HUMINT, sometimes referred to as Clan HUMINT, involves intelligence activity using human sources directed towards the acquisition of information through clandestine means, i.e., *espionage*.

> "*In overt collection, the collector meets openly with sources as a declared U.S. Government representative. …Clandestine collection is conducted in secret. …After the source is recruited, contact is usually strictly controlled in an effort to elude discovery. The recruitment of a clandestine human source can take months or years, but the leak of a source's information may immediately eliminate access to that source.*"
>
> -- U.S. National Intelligence – An Overview 2011, p, 54

The Director CIA serves as the ***National HUMINT Manager*** for the Intelligence Community (IC) with the authority to coordinate, deconflict, and evaluate HUMINT operations across the IC; authorities for clandestine HUMINT delegated to the Director of the National Clandestine Service (NCS); see ICD 300 and ICD 304.

The Director DIA serves as the ***Defense HUMINT Manager*** responsible for providing centralized management of DoD HUMINT.

U.S. FI collection priorities are driven by the National Intelligence Priorities Framework (NIPF); see NSPD 26 and ICD 204. For DoD HUMINT policy see DoDD S-5200.37, *Management and Execution of Defense Human Intelligence (HUMINT) (U)*, 9 Feb 2009 with chg 2.

Foreign intelligence entities worldwide, as well as a variety of non-state actors, commercial enterprises, and regional organizations) use clandestine human intelligence collection to "acquire information" (aka conduct espionage). Typically intelligence entities rely upon specially trained or designated employees, often referred to as "case officers" or "agent handlers" (aka operations officers within CIA) to spot, access, develop, and recruit agents who can provide information that is not publicly available.

Within CIA, Operations Officers (OOs) are certified Core Collectors who collect human intelligence of concern to the U.S. President, policymakers, and military by recruiting and handling clandestine human sources in a secure manner. OOs clandestinely spot, assess, develop, recruit and handle human sources with access to vital intelligence.

-- See <https://www.cia.gov/offices-of-cia/clandestine-service/careers/careers-operations-officer.html>

Human-Source Intelligence (HUMINT). The oldest method for collecting information, this is intelligence derived from human sources. Collection includes clandestine acquisition of photography, documents, and other material; overt collection by personnel in diplomatic and consular posts; debriefing of foreign nationals and US citizens who travel abroad; and official contacts with foreign governments. To the public, HUMINT is synonymous with espionage and clandestine activities. However, most of it is accumulated by overt collectors such as diplomats and military attaches.

The CIA, working closely with the Office of the Director of National Intelligence (ODNI) established the National Clandestine Service (NCS) to improve HUMINT throughout the IC. The NCS serves as the national authority for coordination, de-confliction, and evaluation of clandestine HUMINT operations, both abroad and inside the United States. While the ODNI establishes policy related to clandestine HUMINT, the NCS executes and implements that policy across the Intelligence Community (IC).

-- <http://www.intelligence.gov/about-the-intelligence-community/how-intelligence-works/data-gathering.html>

Human Intelligence is derived from the analysis of foreign positive information collected by a trained HUMINT Collector from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human contacts and informants as a tool, and a variety of collection methods to gather information that satisfies the commander's critical information requirements (CCIR) and cues other collection resources.

-- Colonel Jerry W. Jones (USA Retired), "CI and HUMINT or HUMINT and CI or CI/HUMINT or TAC HUMINT," *Military Intelligence Professional Bulletin*, vol. 28, no. 2 (April 2002), p 29.

HUMINT is the oldest collection discipline and a key contributor to the all-source picture of the battlefield. HUMINT is the intelligence, to include adversary intentions, derived from information collected from people and related documents. It uses human sources acquired both passively and actively to gather information to answer intelligence requirements and to cross-cue other intelligence disciplines. HUMINT is produced from the collection on a wide range of requirements with the purpose of identifying adversary capabilities and intentions.

-- U.S. Army ST 2-22.7, Tactical Human Intelligence and Counterintelligence Operations, April 2002, p. 7-4.

The U.S. will continue to need the capabilities to collect HUMINT, especially as a major insight into intentions and plans of hostile states or groups, and to carry out covert action.

-- IC 21: HPSCI Staff Study, 9 Apr 1996 (Finding, p.18)

As George Kisevalter, a CIA case officer who handled defector Col. Oleg Penkovsky, stressed, HUMINT was as much an art as a science, and that "common sense, and the ability to analyze charter quickly and decisively, were the intelligence officer's greatest assets." So too, the mastery of intelligence tradecraft is imperative for success.

-- Julie Anderson, "The HUMINT Offensive from Putin's Chekist State," *International Journal of Intelligence and Counterintelligence*, Vol 20 No 2 (Summer 2007), p. 274

Note: Mr. Kisevalter handled both Major Pyotr Popov, the first Soviet GRU officer run by the CIA, as well as Colonel Oleg Penkovsky. See Clarence Ashley. *CIA SpyMaster* (2004) for the inside story on a CIA legend. .

Counterintelligence (CI) is often mistaken as part of or a subset of HUMINT. Although HUMINT and CI are partners in the Human Domain -- both are intelligence activities that operate in the human domain -- ***they are distinctly different…different missions, different authorities, each focused on different content, as well as outcomes.*** FI collection values the information above all, whereas CI insists on acting on that information--*a totally different operational dynamic*. See *counterintelligence*.

Human Intelligence Collector. See *HUMINT Collector.*

Human Intelligence Source. People who provide intelligence directly; individuals associated with organizations (such as foreign government entities and intelligence services) who willingly share intelligence information with the United States; individuals and organizations who facilitate the placement or service of technical collection means that could not succeed without their support; and foreign citizens who are identified as of an intelligence interest to the United States with a reasonable expectation that they will provide information or services in the future. Information that may reveal the identities of people upon whom the United States relies for information, access to information, or cooperation leading to obtaining information is considered to potentially reveal human intelligence sources. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012) Also see *Human Source, Source*.

Human Source. A person who wittingly or unwittingly conveys by any means information of potential intelligence value. (ICS Glossary) Also see *Human Intelligence Source*; *Source.*

-- Also, a person from whom information can be obtained. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

"Every person—friendly, hostile, or neutral—is a potential source of information. The HUMINT information collection system uses various methods to collect information from a number of sources."

-- U.S. Army ST 2-22.7, *Tactical Human Intelligence and Counterintelligence Operations*, Apr 2002

"[H]uman sources collect the smallest volume of intelligence but generally it is the most difficult to obtain and the most useful when we do get it. It is in this area that the best information is acquired on the all-important subject of intentions."

-- General Veron Walters (Former DCI), *Silent Missions* (1978)

Human Source Contact Operations (SCO). HUMINT collection activity directed toward the establishment of human sources who have agreed to meet and cooperate with HUMINT collectors for the purpose of providing information. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

> *SCO sources include: one-time contacts, continuous contacts, and formal contacts from debriefings, liaison, and contact operations. The basic goal of all levels of contact is to collect information in response to collection tasking.*
>
> -- Army FM 2-22.3, *Human Intelligence Collector Operations* (2006)

Human-Source Intelligence. Intelligence obtained from human sources. See *Human Intelligence*.

Human Terrain Analysis. A multidisciplinary approach to describe and predict geospatial and temporal patterns of human behavior by analyzing the attributes, actions, reactions, and interactions of groups or individuals in the context of their environment. (DoDD 3600.01, Information Operations, 14 Aug 2006 with chg 1, 23 May 2011)

HUMINT. See *Human Intelligence*.

HUMINT Collection Activities. Categories include: tactical questioning; screening, interrogation; debriefing; liaison; human source contact operations (SCOs), documents exploitation (DOCEX); and captured enemy equipment (CEE) operations. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

> DoDD S-5200.37 provides overarching policy for all Defense HUMINT collection operations. Also see: DHE-M 3301.001, Vol I, *Collection Requirements, Reporting, and Evaluation Procedures* (U); DHE-M 3301.002, Vol II, *Collection Operations* (U); and Army FM 2-22.3, *Human Intelligence Collector Operations.*

HUMINT Collection Requirement (HCR). A long-term, DoD validated HUMINT collection requirement which supports DoD or IC operational planning, policy- and decision making, intelligence production, and intelligence databases. (DHE-M 3301.001, DIA HUMINT Manual, Vol I, 30 Jan 2009 w/ chg 2)

HUMINT Collection Methods. There are two HUMINT collection methods authorized for use within DoD: overt and clandestine. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

HUMINT Collection Requirement (HCR). A long-term DoD-wide HUMINT collection requirement which supports DoD operational planning, policy- and decision-making, intelligence production, and intelligence databases. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

HUMINT Collection Team (HCT). Element that collects information from human sources. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

HUMINT Collector. A person who is specifically trained and certified for, tasked with, and engages in the collection of information from HUMINT sources for the purposes of answering intelligence information requirements. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

-- Also, a person who is specifically trained and certified for, tasked with, and engages in the collection of information from individuals (HUMINT sources) for the purpose of answering intelligence information requirements. (Army FM 2-22.3, HUMINT Collector Operations, Sep 2006)

> Within DoD, appropriately trained and certified individuals are the only personnel authorized to conduct HUMINT operations beyond tactical questioning.

HUMINT Enabling. An operational support function in which non-HUMINT intelligence collection operations are facilitated by HUMINT collection platforms.

HUMINT Operations. Intelligence activities, including military source operations, the primary purpose of which is to obtain foreign intelligence information collected and provided by human sources. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013, with chg 1 dated 13 Jun 2013) Also see *human intelligence*.

> DoD HUMINT operations are conducted in response to DoD or national requirements based on the needs of the originator.

HUMINT Operations Cell (HOC). Assigned under the J/G2X to track all HUMINT activities in the area of intelligence responsibility. It provides technical support to all HUMINT collection operations and deconflicts HUMINT collection operations in the AO. (Term previously defined in Army FM 2-0, Intelligence, May 2004)

> For additional information on the HOC see: JP 2-01.2, *CI & HUMINT in Joint Operations (U)*, 16 Mar 2011 (w/ chg 1 dated 26 Aug 2011), p. II-8 (para 3c).

HUMINT Source. A person from which services or intelligence information are obtained. The source may possess either first or second-hand knowledge normally obtained through sight or hearing and may be witting or unwitting. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010) Also see *human source; source*.

-- Also, a person from whom information can be obtained. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

HUMINT Support Element (HSE). A DIA representative or staff element assigned to support a COCOM. An HSE provides liaison and assists the COCOM with HUMINT planning, coordination, collection management, training, and operations. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

HUMINT Targeting. The integration of all-source intelligence and systemic analytic methodologies to identify and develop relevant HUMINT leads in direct support of HUMINT collection operations. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

HUMINT Tasks. Include but not limited to: conducting source operations; liaising with host nation officials and allied counterparts; eliciting information from select sources; debriefing US and allied forces and civilian personnel including refugees, displaced persons, third-country nationals, and local inhabitants; interrogating enemy prisoners of war and other detainees; and initially exploiting documents, media, and material. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

HUMINT Training. Instruction and applied exercises for acquiring and retaining skills and knowledge required in the acquisition of foreign intelligence derived from the collection discipline that uses human beings as both sources and collectors. (DoDI 3305.15, DoD HUMINT Training, 25 Feb 2008)

HUMINT Training Joint Center of Excellence (HT-JCOE). An advanced joint HUMINT training activity that supports HUMINT activities within the DCHE [Defense CI and HUMINT Enterprise]. The HT-JCOE is comprised of HT-JCOE West and HT-JCOE East. The HT-JCOE West operates with the Department of the Army. The JT-JCOE East operates within the [Defense Intelligence Agency]. (DoDI O-5109.95, HT-JCOE, 18 Apr 2012)

Hybrid Threats. Hybrid threats refer to the ability of adversaries—lone attackers, criminal, transnational terrorist organizations, even nation-states—to employ combinations of tactics, technologies, and capabilities to gin an asymmetric advantage. (Quadrennial Homeland Security Review Report, Feb 2010)

-- Also, the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects. (ADRP 3-0, Unified Land Operations, May 2012)

Hyperspectral Imagery (HSI). Term used to describe the imagery derived from subdividing the electromagnetic spectrum into very narrow bandwidths. These narrow bandwidths may be combined with or subtracted from each other in various ways to form images useful in precise terrain or target analysis. (JP 1-02 and JP 2-03, Geospatial Intelligence Support to Joint Operations, 31 Oct 2012).

I ==========

i-Space (Integrated Space): a U.S. Intelligence Community (IC) social networking and collaboration service hosted on JWICS; intended to foster and facilitate collaboration between IC members. Previously known as "A-Space," the transformation to i-Space broadens membership from analyst only to virtually any intelligence professional with access and a mission need. (Intellipedia, accessed 1 Nov 2013)

ICE-mail. Email between organizations over JWICS network. Also referred to as ICE-mail or JWICS email. (National Intelligence: A Consumer's Guide - 2009)

ICON. See *Investigations, Collections and Operations Nexus*.

Identity. The distinguishing characteristics or personality of an individual or facility. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

Identity Intelligence (I2). The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Ideology. Commitment to a competing political or economic system such as Communism. (PERSEREC 1992) Also see divided *loyalties, MICE*.

IDSRS. See *Integrated Defense Source Registry System*.

Illegal. An officer, employee, or agent of an intelligence organization who is dispatched abroad and who has no overt relationship with the intelligence service with which he/she is connected or with the government operations that intelligence service. Term is derived from the fact that the individual is in the host country illegally. (CI Community Lexicon)

-- Also, an intelligence officer or a recruited agent who operates in a foreign country in the guise of a private person, and is often present under false identity. (FBI -- Affidavit: USA vs. Robert Philip Hanssen, 16 Feb 2001)

-- Also, *Illegal Intelligence Officers (IIO)* – individuals who enter a country either by circumventing border controls or by using false documentation. False documents permit the IIO to remain within the country for a long time while being able to withstand extensive background checks and leave the country with minimum official scrutiny. The very nature of the IIO's covert activity makes it extremely difficult for counterintelligence agencies to identify or accurately assess their total strength and potential impact on national security. (AFOSI Manual 71-144, Vol 5, CI Program, 15 May 2009)

"Illegals" have no "easily" detectable contacts with their parent intelligence service. They pose as legitimate residents of the target country and operate without benefits of diplomatic cover.

"In intelligence parlance, an 'illegal' is a spy operating without benefit of diplomatic cover. If caught, an illegal can be prosecuted, imprisoned, or even executed; by contrast, a diplomat can only be declared persona non grata and expelled by the host country."

-- David Wise, *Tiger Trap: America's Secret War with China* (2011), p. 208

"*The illegal is a highly trained specialist in espionage tradecraft. He may be a [foreign] national and/or a professional intelligence officer dispatched to the United States under a false identity.*"
-- FBI as cited in Senate Report # 94-755 (aka Church Committee Report), Book I, 26 April 1976, p.164

"*Illegal agents—that is, operatives for whom an alias identity has been systemically developed which enables them to live in the United States as America citizens or resident aliens without our knowledge of their true origins.*"
-- Rockefeller Committee Report, June 1975, p. 8

Illegal Net. An intelligence gathering unit operating under the control of an illegal residency. (AFOSI Manual 71-142, OFCO, 9 Jun 2000 and FBI FCI Terms)

Operation GHOST STORIES -- FBI investigation of a network of Russian sleeper agents under non-official cover in the United States. July 2010, the FBI arrest of 10 Russian "illegals" which provided a chilling reminder that espionage on U.S. soil did not disappear when the Cold War ended. The FBI case against the Russian Intelligence operatives went on for more than a decade.

The FBI released dozens of still images, surveillance video clips, and documents related to the investigation, see <http://www.fbi.gov/news/stories/2011/october/russian_103111/russian_103111>

Illegal Residency. An intelligence apparatus established in a foreign country and composed of one or more intelligence officers, which has no apparent connection with the sponsoring intelligence organization or with the government of the country operating the intelligence organization. (ICS Glossary)

Illegal Support Officer. An intelligence officer assigned to a legal residency whose primary function is to support illegal agents by supplying anything needed. A secondary function is the gathering of information and documents that will serve as guidance and models for documentation of future illegal agents. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Imagery. A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (JP 1-02 and JP 2-03, GEOINT Support to Joint Operations, 22 Mar 2007)

-- Also, representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Imagery Exploitation. The cycle of processing, using, interpreting, mensuration and/or manipulating imagery, and any assembly or consolidation of the results for dissemination. (JP 1-02.and JP 2-03, GEOINT Support to Joint Operations, 31 Oct 2012)

Imagery Intelligence (IMINT). The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. (JP 1-02 and JP 2-03, GEOINT Support to Joint Operations, 31 Oct 2012) Also see *geospatial intelligence*.

-- Also, IMINT is derived from the exploitation of imagery collected by visual photography, infrared sensors, lasers, multispectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media. (Army FM 2-0, Intelligence, 23 Mar 2010)

-- Also, intelligence that includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. (ODNI, U.S. National Intelligence – An Overview 2011)

> *Imagery Intelligence (IMINT): The National Geospatial-Intelligence Agency (NGA) manages all IMINT activities, both classified and unclassified, within the US Government . This includes requirements, collection, processing, exploitation, dissemination, archiving, and retrieval.*
>
> -- www.intelligence.gov (accessed 13 Aug 2012)
>
> _____
>
> There are two general types of imagery collection platforms:
> + Satellites—compromised of national technical means [NTM] and commercial platforms.
> + Airborne Systems—compromised of national, commercial, theater, and tactical.
>
> There are two general types of imagery sensors:
> + Electro-optical: panchromatic (visible); infrared; special (multispectral & hyperspectral); and polarmetric.
> + Radar: synthetic aperture radar systems that collect and display data either as representations of fixed targets or as moving target indicators.
>
> -- Army FM 2-0, *Intelligence,* 23 Mar 2010, pp. 9-2 & 9-3

Immigration and Customs Enforcement (ICE). The principal investigative arm of the U.S. Department Homeland Security (DHS). Created in 2003 through a merger of the investigative and interior enforcement elements of the U.S. Customs Service and the Immigration and Naturalization Service,

> ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade and immigration. ICE's two principal operating components are Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO).
>
> See ICE website at: <http://www.ice.gov/index.htm>

Impersonal Communication. Communications between a handler and asset which do not involve direct contact. (HDI Lexicon, April 2008)

-- Also, secret communication techniques used between a case officer and a human intelligence asset when no physical contact is possible or desired. (CI Centre Glossary)

> ***Impersonal Communications…***
>
> *[C]landestine techniques to avoid risky face-to-face contact that often employed methods such as dead drops and elaborate systems of signaling readiness to send and receive those caches of information. This system had been used successfully by intelligence services for centuries.*
>
> -- Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present*, 2013, p. 10

Implant. Electronic device or electronic equipment modification designed to gain unauthorized interception of information-bearing emanations. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Implied Task. In the context of joint operation planning, a task derived during mission analysis that an organization must perform or prepare to perform to accomplish a specified task or the mission, but which is not stated in the higher headquarters order. (JP 5-0, Joint Operation Planning, 11 Aug 2011) Also *see essential task; specified task*.

Improvised Explosive Device (IED). A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. (JP 1-02)

In the Gap. [Tradecraft jargon] Surveillance-free for a few seconds but not as long as a minute. (Spy Dust)

Inadvertent Disclosure. Type of incident involving accidental exposure of information to an individual not authorized access. (CNSS Instruction No. 4009)

-- Also, a set of circumstances or a security incident in which a person has had involuntary access to classified information to which the individual was or is not normally authorized. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Indication and Warning. Within DoD, term changed to "warning." See *warning.*

Indications. In intelligence usage, information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Indicator. In intelligence usage, an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *espionage indicator*.

-- Also, data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, *"Threat Indicator"* any observable action that suggests violent behavior, abnormal disgruntlement, radicalization, or an extreme religious or other ideological worldview. (US Army Tactical Reference Guide, Radicalization into Violent Extremism: *A Guide for Military Leaders*, Aug 2011) Also see *radicalization*, *terrorism*, *violent radicalization.*

Indirect Access. Descriptor used for sources who do not have firsthand access to the information provided and who have come upon it through one or more sub-sources. (DoDI S-5200.42, Defense HUMINT and Related Activities (U), 8 Dec 2009) Also see *direct access*.

Indoctrination (or read-on). An initial indoctrination and/or instruction provided each individual approved to a SAP prior to his exposure concerning the unique nature of program information and the policies, procedures, and practices for its handling. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Induced Defection. Tradecraft jargon for developing and encouraging a foreign official's defection from his country. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

> ***"Inducement" is the jargon used for persuading somebody to defect to you.***
> -- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

Induced Operation. An operation in which a source or agent is established in such a manner as to induce the opposition to recruit him as its agent. (CI Community Lexicon)

Induction. [One of the four basic types of reasoning applied to intelligence analysis, it is the process] of discovering relationships among the phenomena under study. …[it draws] generalizations on the basis of observations or other evidence. (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *abduction; deduction; scientific method.*

> For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003) and *Critical Thinking and Intelligence Analysis* by David Moore, JMIC Press (2006).

Industrial Espionage. The knowing misappropriation of trade secrets related to, or included in, a product that is made for or placed in interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret.

-- Also, the act of seeking a competitive, commercial advantage by obtaining a competitor's trade secrets and/or logistics. The acquisition of industrial information through clandestine operations. (DSS Glossary)

> Industrial espionage is criminalized under the Economic Espionage Act of 1996, PL 104-294. See <http://www.gpo.gov/fdsys/pkg/PLAW-104publ294/content-detail.html>
>
> Industrial espionage, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner by: (1) stealing, or without authorization appropriating, carrying away, concealing, or obtaining by deception or fraud information related to that secret; (2) copying, duplicating, reproducing, destroying, uploading, downloading, or otherwise transmitting that information without authorization; or (3) receiving that information knowing that that information had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1832).

Industrial Security. That portion of information security which is concerned with the protection of classified information in the custody of U.S. industry. (DoD 5220.22-M, NISPOM, 28 Feb 2006) Also see *Defense Security Service (DSS); National Industrial Security Program (NISP).*

-- Also, a mutli-disciplinary security program concerned with the protection of classified information developed by or entrusted to U.S. industry. (IC Standard 700-1, 4 Apr 2008 and DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012 w/ chg 1 dated 24 Apr 2013)

Infiltrate. Tradecraft jargon for the act of penetrating a country or organization. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Infiltration. In intelligence usage, placing an agent or other person in a target area in hostile territory. Usually involves crossing a frontier or other guarded line. Methods of infiltration are: black (clandestine); grey (through legal crossing point but under false documentation); and white (legal). (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Inform and Influence Activities. The integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decisionmaking. (Army FM 3-13, Inform and Influence Activities, Jan 2013)

Informant. A person who, wittingly or unwittingly, provides information to an agent, a clandestine service, or the police. (ICS Glossary and Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Information. Facts, data, or instructions in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 3-13.1, Electronic Warfare, 25 Jan 2007)

Information and Communications Technology (ICT). Includes but is not limited to information technology as defined in section 11101 of title 40, U.S.C.. The term reflects the convergence of information technology and communications. ICT includes all categories of ubiquitous technology used for gathering, storing, transmitting, retrieving, or processing information (e.g., computing systems, software, mobile telephony, satellite communications, and networks. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD 8500.01E, Information Assurance and CNSSI-4009) Also see *Information Operations*.

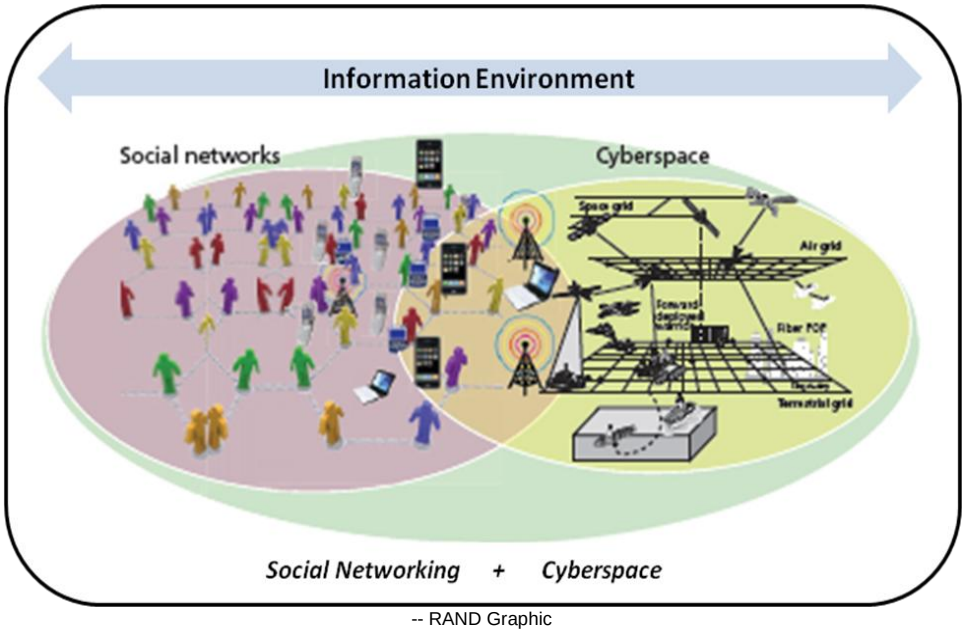
-- Also, actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. (JP 1-02 and JP 3-12, Cyberspace Operations, 5 Feb 2013)

-- Also, protecting information's confidentiality, integrity, and availability. (National Intelligence: A Consumer's Guide - 2009).

-- Also, the protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. IA is a security discipline that encompasses COMSEC, INFOSEC, and control of compromising emanations (TEMPEST). (AR 25-2, Information Assurance, 3 Aug 2007)

Information Collection. An activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations. (Army FM 3-55, Information Collection, April 2012)

Information Environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02 and JP 3-13, Information Operations, 13 Feb 2006)



-- RAND Graphic

Information Fratricide. The result of employing information-related capabilities in a way that causes effects in the information environment that impede the conduct of friendly operations or adversely affect friendly forces. (Army FM 3-13, Inform and Influence Activities, Jan 2013)

Information Protection. Active or passive measures used to safeguard and defend friendly information and information systems. (ADRP 6-0, Mission Command, May 2012)

Information Operations (IO). The integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries, while protecting our own. (JP 3-13, Information Operation, 27 Nov 2012; approved for inclusion in update to JP 1-02)

> For DoD policy see DoDD 3600.01, *Information Operations*, 2 May 2013
>
> Counterintelligence investigations, operations, collection, analysis, production, and dynamic functional CI services are employed in support of appropriate IO activities to detect and mitigate foreign intelligence, hacker, and insider threats to DoD information and information systems.
>
> ---
>
> *IO will be the principal mechanism used during military operations to integrate, synchronize, employ, and assess a wide variety of information-related capabilities (IRCs) in concert with other lines of operations to effect adversaries' or potential adversaries' decision-making while protecting our own.*
>
> – DoDD 3600.01, *Information Operations*, 2 May 2013

Information Related Capability (IRC). A capability that is a tool, technique, or activity employed within a dimension(s) of the information environment that can be used to achieve a specific end(s). (DoDD 3600.01, Information Operations, 2 May 2013) Also see *information operations*.

Information Requirements. In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *intelligence requirement; collection requirement.*

> ***The requirements process has traditionally been one of the most vexing aspects of intelligence management.***
>
> -- IC 21: HPSCI Staff Study, 6 Apr 1996

Information Security. The security discipline concerned with implementation of a system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information that is authorized protection by Executive order, statute, or regulation. Information security includes protection of classified, controlled unclassified, and sensitive compartmented information. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012, w/ chg 1 dated 24 Apr 2013)

-- Also, INFOSEC the system of policies, procedures, and requirements established in accordance with Executive Order 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to Executive Order, statute or regulation. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012) Also see *computer security; cyber security.*

-- Also, protecting information's confidentiality, integrity, and availability. (National Intelligence: A Consumer's Guide - 2009)

To be withdrawn from JP 1-02 per JP 3-13, 27 Nov 2012; previously defined as: the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. INFOSEC includes those measures necessary to detect, document, and counter such threats. INFOSEC is composed of computer security and communications security.

-- JP 3-13, *Information Operations*, 13 Feb 2006

INFOSEC plays a vital role in national security and in the Critical Infrastructure

The goal of INFOSEC is to ensure that the National Security Community has reliable and secure networks to originate, store, manipulate, and make information available to those who need it and are authorized to have it.

-- Joint Security Commission II Report, 24 Aug 1999, p. 18

Information Security Oversight Office (ISOO). US Government office that is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program.

The ISOO is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program. The ISOO is also responsible for implementing and overseeing the National Industrial Security Program (NISP) under Executive Order 12829, as amended, issued in 1993.

ISSO web site at: <http://www.archives.gov/isoo/>

Information Superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02 and JP 3-13, Information Operations, 27 Nov 2012) Also see *information operations*.

Informer. One who intentionally discloses information about other persons or activities to police or a security service (such as the FBI), usually for a financial reward. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Infrared Imagery. That imagery produced as a result of sensing electromagnetic radiations emitted or reflected from a given target surface in the infrared position of the electromagnetic spectrum (approximately 0.72 to 1,000 microns). (JP 1-02 and JP 2-03, Geospatial Intelligence Support to Joint Operations, 31 October 2012)

InfraGard. A partnership between the FBI and the private sector. InfraGard is an association of individuals, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. (FBI)

Infragard a collaboration for infrastructure protection. For more information see <http://www.infragard.net/>

Infrastructure. The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Inherited CPI. [Proposed DoD definition] CPI that is owned and generated by one RDA program, subsystem, or project that is incorporated into and used by another RDA program. (*Draft* DoDI 5200.39, CPI Identification and Protection within RDA Programs)

Initial Contact Point (ICP). A physical location where an intelligence officer makes an initial contact or brush pass with his source or asset. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Insider. [Within DoD,] anyone who has authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 with change 1 dated 15 Oct 2013) Also see *insider threat, CI insider threat.*

-- Also, any person with authorized access to any U.S. Government (USG) resource, to include personnel, facilities, information, equipment, networks, or systems. (U.S. Government Threat Detection Guide - 2011)

-- Also, anyone with access, privilege, or knowledge of information systems or services. Malicious insider is [a person] motivated to intentionally adversely impact an organization's mission (e.g., deny, damage, degrade, destroy). (Rand Study, *Understanding the Insider Threat*, March 2004)

Insider Threat (InT). A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 w/ chg 1 dated 15 Oct 2013 and DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012 w/ chg 1 dated 24 Apr 2013) Also see *insider, CI insider threat*.

-- Also, a person, known or suspected, who uses their authorized access to Department of Defense facilities, systems, equipment, information or infrastructure to damage, disrupt operations, commit espionage on behalf of a foreign intelligence entity or support international terrorist organizations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the threat that an insider will use their authorized access to harm the security of the United States. This threat can include damage to the US through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities [sabotage]. (U.S. Government Threat Detection Guide - 2011 and IC Standard 700-2, 2 June 2011)

-- Also, activities conducted by a person with placement and access that intentionally or unintentionally compromise an agency's ability to accomplish its mission, including but not limited to espionage, other criminal activity, unauthorized disclosure of information and loss or degradation of departmental resources or capabilities. (National CI Strategy Operating Plan 2008-2010, 9 Aug 2007)

-- Also, the ability of a trusted insider to bypass or defeat security safeguards or otherwise adversely affect the national security. (IC Standard 700-1, 4 Apr 2008)

-- Also, an entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a person with placement and access who intentionally or unintentionally causes loss or degradation of resources or capabilities and compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, other criminal activity, or unauthorized release or disclosure of information. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, any insider with legitimate access to government information, personnel, and facilities may intentionally or unintentionally pose a threat. (NSA CI Awareness Pamphlet on Insider Threat, undated)

-- Also, the *insider threat to critical infrastructure* is one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm. (National Infrastructure Advisory Council's Report, *The Insider Threat to Critical Infrastructures*, 8 April 2008)

Trusted insiders with means, motive, and opportunity pose a major threat

"Countering insider threats are coordinated CI, security, information assurance (IA), law enforcement (LE), and antiterrorism & force protection (AT/FP) activities…"

-- DoDI 5240.26, *Countering Espionage, International Terrorism, and the CI Insider Threats*, 4 May 2012

"Insider threats remain the top counterintelligence challenge to our community."

-- Robert "Bear" Bryant, National Counterintelligence Executive

---

"The problem of insider spies has bedeviled intelligence services from time immemorial."

-- David L. Charney. M.D., "True Psychology of the Insider Spy," in *Intelligencer: Journal of U.S. Intelligence Studies* (Fall/Winter 2010), p. 47.

"[H]istory teaches us to expect spies among us and to anticipate that some of those spies will be us…. [W]e cannot eliminate espionage… [but we must] minimize the harm that those who betray us can do to our national security and minimize the time between their defection and detection."

-- Webster Commission Report (A Review of FBI Security Programs), March 2002, pp. 17-18.

"The Insider Threat is the single-most pervasive and damaging security risk facing global organizations and governments today."

-- www.intrusic.com

"Malicious insiders may exploit their access at the behest of foreign governments, terrorists groups, criminal elements, unscrupulous associates, or on their own initiative. Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DoD, and national security, can be devastating."

-- *DoD Strategy for Operating in Cyberspace*, July 2011

"…the threat lies in the potential that a trusted employee may betray their obligations and allegiances to their employer and conduct sabotage or espionage against them. Insider betrayals cover a broad range of actions, from secretive acts of theft or subtle forms of sabotage to more aggressive and overt forms of vengeance, sabotage, and even workplace violence. The threat posed by insiders is one most owner-operators neither understand nor appreciate."

-- T. Noonan and E. Archuleta, *The Insider Threat to Critical Infrastructures* , The National Infrastructure Advisory Council, April 6, 2008, p. 32.

"WikiLeaks represents a somewhat different kind of threat. It's an insider threat, as opposed to a remote threat where someone is trying to come across the networks at you."

-- William Lynn, US Deputy Defense Secretary, Interview reported in *DefenseNews*, 18 July 2011

"In addition to threats by foreign intelligence entities, insider threats will also pose a persistent challenge. Trusted insiders with the intent to do harm can exploit their access to compromise vast amounts of sensitive and classified information as part of a personal ideology or at the direction of a foreign government. The unauthorized disclosure of this information to state adversaries, nonstate activists, or other entities will continue to pose a critical threat."

-- DNI, Worldwide Threat Assessment of the US Intelligence Community, SSCI, 29 January 2014

See ONCIX classified report, *U.S. Government Insider Threat Detection Guide – 2011* (U).

See Army Directive 2013-18, Army Insider Threat Program, 31 Jul 2013; copy available at: <http://www.fas.org/irp/doddir/army/insider.pdf>

See SECNAV Instruction 5510.37, Department of the Navy Insider Threat Program, 8 Aug 2013; copy available at: <http://www.fas.org/irp/doddir/navy/secnavinst/5510_37.pdf>

See NCIS *CI & Insider Threat Awareness and Reporting Brief* – Briefers Handbook, March 2013 with DVD (a professionally produced briefing tool for NCIS Agents)

Also see "True Psychology of the Insider Spy," in AFIO *Intelligencer: Journal of U.S. Intelligence Studies* (Fall/Winter 2010), p. 47 -- copy available at < http://www.ncix.gov/issues/ithreat/Charney-PsychologyofInsiderSpyAFIO-INTEL_Fall-Winter2010.pdf >

Additional open source information on insider threat issues at <http://www.cert.org/insider_threat/>

"A nation can survive its fools and even the ambitious.
But it cannot survive treason from within."

-- Cicero (106-43 B.C.)
Speech in the Roman Senate – circa 58 BC

Instruments of National Power. All of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational and military. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02)

Insurgency. The organized use of subversion and violence to seize, nullify, or challenge political control of a region. Insurgency can also refer to the group itself. (JP 3-24, Counterinsurgency, 22 Nov 2013)

-- Also, the organized use of subversion and violence to seize, nullify, or challenge political control of a region. (Army FM 3-24, Insurgencies and Countering Insurgencies, May 2014)

According to FM 3-24, insurgency in the most basic form is a struggle for control and influence, generally from a position of relative weakness, outside existing state institutions. Insurgencies can exist apart from or before, during, or after a conventional conflict.

Insurgent. See *insurgency.*

Integrated Defense Source Registration System (IDSRS). A DoD-level system to enable the sharing of HUMINT source information, meant to ensure Deconfliction of DoD-wide HUMINT sources. (Defense HUMINT Enterprise Manual, Vol II, 23 Nov 2010)

See USD(I) Memo, 13 August 2005 and IDSRS website on SIPRNet at: <http://dh.dia.smil/idsr/>

INTELINK. INTELINK is the classified, worldwide intranet for the U.S. Intelligence Community. At its most secure level, INTELINK utilizes the Joint Worldwide Intelligence Communications System (JWICS) as its communication vehicle. JWICS is a 24 hour a day network designed to meet the requirements for secure multi-media intelligence communications worldwide up to the Top Secret/SCI level.

INTELINK-S. INTELINK-S is similar to INTELINK except that it is accessed through the Secret Internet Protocol Router Network (SIPRNet). It is a 24 hour a day network designed to meet the requirements for secure multi-media intelligence communications worldwide at the Secret level and below.

Intelligence. 1) The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2) The activities that result in the product. 3) The organizations engaged in such activities. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *foreign intelligence; counterintelligence*.

"Intelligence deals with all things which should be known in advance of initiating a course of action"

-- Task Force on Intelligence Activities (Hoover Commission) – 1955

The term "intelligence" includes foreign intelligence and counterintelligence.

-- National Security Act of 1947 (as amended), 50 USC §401a, and EO 12333 (as amended 30 Jul 2008)

The main methods of collecting foreign intelligence (FI), collectively referred to as "intelligence collection disciplines" or the "INTs," are: human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT), including imagery intelligence (IMINT); measurement & signatures intelligence (MASINT); and open source intelligence (OSINT).

Recommended: Mark Lowenthal, PhD, *Intelligence: From Secrets to Policy* (2011, 5th edition)

-- Also, a body of evidence and the conclusions drawn there from that is acquired and furnished in response to the known or perceived requirements of Consumer's. It is often derived from information that is concealed or not intended to be available for use by the acquirer. (ODNI website www.dni.gov)

-- Also, information that has been analyzed and refined so that it is useful to policymakers in making decisions—specifically, decisions about potential threats to our national security. (FBI at <http://www.fbi.gov/about-us/intelligence/defined>)

-- Also, the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (TRADOC Pam 525-2-1, US Army Functional Concept for Intelligence, 13 Oct 10)

-- Also, secret, state activity to understand or influence foreign entities. (Michael Warner, "Wanted: A definition of Intelligence," *Studies in Intelligence,* 46: 3, 2002, pp.15-22)

A plethora of definitions for intelligence

Sherman Kent, former Chairman of CIA's Office of National Estimates asserted that intelligence can be thought of as a process, a product, as well as an organization. His point is valid, as organizations that make up the US Intelligence Community use the term "intelligence" in three different ways—*product, process, and organization*:

1) Intelligence is a ***product*** that consists of information that has been refined to meet the needs of policymakers/decision makers;
2) Intelligence is also a ***process*** through which that information is identified, collected, Analyzed, and disseminated; and
3) Intelligence refers to both the individual ***organizations*** that shape raw data into a finished intelligence product for the benefit of decision makers and the larger community of these organizations collected referred to as the Intelligence Community or IC.

A word of caution about the term "intelligence" is in order. Too often it is used synonymously or interchangeably with "information." This is inaccurate and quite misleading. Information until may be interesting, amusing, or hitherto unknown to the person receiving it, but by and in itself it is inappropriate to call it intelligence.

-- William R. Corson, *The Armies of Ignorance: The Rise of the American Intelligence Empire* (1977)

Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.

-- Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. 4th Edition (2009), p. 8

[Intelligence is] *mainly secret activities---targeting, collection, analysis, dissemination and action—intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities.*

-- P. Gill, "Theories of Intelligence: Where Are We, Where Should We Go and How Might We Proceed?" in *Intelligence Theory: Key Questions and Debates*, 2009, p. 214

[I]ntelligence in general can be thought of as the complex process of understanding meaning in available information. A typical goal of intelligence is to establish facts and then to develop precise, reliable, and valid inferences (hypotheses, estimations, conclusions, or predictions) for use in strategic decisionmaking or operational planning.

-- Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (2004), p. 13

By definition, intelligence deals with the unclear, the unknown the deliberately hidden…. In the intelligence business, you are almost never completely wrong or completely right.

-- George J. Tenet, Director CIA (5 Feb 2004)

For intelligence to have any real value, it must be acted on, sometimes quite promptly and decisively; otherwise, it can be about as useful as warm spit, regardless how romantic or dramatic it may sound.

-- LTG Samuel Wilson (Retired), Former Director DIA, April 2009

"The truth is that there is never enough good intelligence."

-- R. Jack Smith (Former DDI CIA), *The Unknown CIA* (1989)

"Timely intelligence is a critical component of preserving our national security."

-- Ambassador John D. Negroponte (12 April 2005)

Intelligence Activities. All activities that elements of the Intelligence Community are authorized to conduct pursuant to Executive Order 12333. (EO 12333, as amended 30 Jul 2008) Also see *intelligence*.

-- Also, all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333. (DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect Unites States Persons, Dec 1982)

-- Also, the collection, production and dissemination of foreign intelligence and counterintelligence pursuant to DoDD 5143.01 and EO 12333. (DoDD 5240.01, DoD Intelligence Activities, 27 Aug 2007 w/ chg 1 dated 27 Aug 2013)

Note: Executive Order 12333 (United States Intelligence Activities) specifically defines the term *intelligence* as including foreign intelligence (FI) and counterintelligence (CI).

Intelligence Analysis. The process by which collected information is evaluated and integrated with existing information to facilitate intelligence production. (ADRP 2-0, Intelligence, Aug 2012) Also see *analysis*.

Intelligence analysis is an intellectual process.

-- Mark Lowenthal, PhD

Intelligence Analyst. A professional intelligence officer who is responsible for performing, coordinating, or supervising the collection, analysis, and dissemination of intelligence. (ODNI, U.S. National Intelligence – An Overview 2011)

> *Intelligence analysts use critical and creative thinking to conduct intelligence analysis and produce timely, predictive intelligence.*
>
> -- ADRP 2-0, *Intelligence,* August 2012

Intelligence Asset. Any resource utilized by an intelligence organization for an operational support role. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *asset*.

Intelligence Collection. The acquisition of information or intelligence information and the provision of it to processing and/or production elements. (CI Community Lexicon) Also see *counterintelligence collection*; *clandestine intelligence collection; intelligence collection.*

> The main methods of collecting foreign intelligence (FI), collectively referred to as "intelligence collection disciplines" or the "INTs," are: human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT), including imagery intelligence (IMINT); measurement & signatures intelligence (MASINT); and open source intelligence (OSINT).
>
> _____
>
> *[I]ntelligence collection is an imperfect process and will rarely be able to provide analysts with everything they need to know.*
>
> -- Mark Lowenthal, PhD, "Intelligence Analysis Guide to its Study," *The Intelligencer: Journal of U.S. Intelligence Studies*, Vol 18, No. 4, Summer/Fall 2011, p. 61

Intelligence Collection Activities. The collection of foreign intelligence and counterintelligence information. (Title 10 USC §431)

Intelligence Collection Plan. A plan for gathering information from all available sources to meet an intelligence requirement. Specifically, a logical plan for transforming the essential elements of information into orders or requests to sources within a required time limit. (JP 1-02)

Intelligence Collector. A phrase sometimes used to refer to an individual, system, organization or agency that engages in the collection step of the intelligence cycle. (ICS Glossary)

Intelligence Community (IC). All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. (JP 2-0, Joint Intelligence, 22 Oct 2013 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the federal agencies and departments that have a legal mandate to collect, analyze, and disseminate intelligence. Executive Order 12333 specifically identifies members of the IC. (CI Community Lexicon)

-- Also, a federation of Executive Branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of U.S. national security. (ODNI, U.S. National Intelligence – An Overview 2011)

U.S. Intelligence Community (50 USC §401a and EO 12333)

-- Office of the Director of National Intelligence
-- Central Intelligence Agency
-- National Security Agency
-- Defense Intelligence Agency
-- National Geospatial-Intelligence Agency
-- National Reconnaissance Office
-- Intelligence & CI components of the U.S. Army, Navy, Marines, and Air Force
-- Federal Bureau of Investigation (National Security Branch)
-- Department of Energy (Office of Intelligence & Counterintelligence)
-- Drug Enforcement Administration (Office of National Security Intelligence)
-- Department of Homeland Security (Office of Intelligence & Analysis)
-- Department of State (Bureau of Intelligence & Research)
-- Department of Treasury (Office of Intelligence & Analysis)
-- Intelligence & CI components of the Coast Guard

For additional information see "An Overview of the United States Intelligence Community" at <http://www.dni.gov/who_what/061222_DNIHandbook_Final.pdf>

Also see Jeffrey T. Richelson, *The US Intelligence Community* (2012, 5th Edition)

Intelligence Community Directives (ICDs). Principal issuances through which the Director of National Intelligence (DNI) provides policy direction to the Intelligence Community (IC). (ICD 1, 1 May 2006)

ICDs are overarching policy documents of the Intelligence Community signed by the DNI and are replacing the legacy Director of Central Intelligence Directives (DCIDs).

Intelligence Contingency Funds (ICF). Appropriated funds to be used for intelligence activities when the use of other funds is not applicable or would either jeopardize or impede the mission of the intelligence unit. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dtd 26 Aug 2011)

Intelligence Cycle. The process by which information is acquired, converted into intelligence, and made available to policymakers and Consumer's. (National HUMINT Glossary) Also see *intelligence process*.

-- Also, the steps through which information is converted into intelligence and made available to users. The cycle typically includes six steps: planning and direction, collection, processing and exploitation, analysis and production, dissemination, and evaluation. (ODNI, U.S. National Intelligence – An Overview 2011) [Note: "evaluation" recently added as the sixth step in the cycle.]

INTELLIGENCE CYCLE
Source: CIA
(Note: The sixth step – *evaluation* – is not captured in the above diagram)

The *Intelligence Cycle* is customarily illustrated as a repeating process consisting of [see graphic above].

[1] ***Planning and direction*** encompasses the management of the entire effort and involves, in particular, determining collection requirements based on customer requests.

[2] ***Collection*** refers to the gathering of raw data to meet the collection requirements. These data can be derived from any number and type of open and secret sources.

[3] ***Processing*** refers to the conversion of raw data into a format analysts can use.

[4] ***Analysis and production*** describes the process of evaluating data for reliability, validity, and relevance; integrating and analyzing it; and converting the product of this effort into a meaningful whole, which includes assessments of events and implications of the information collected.

[5] [***Dissemination***] the product is disseminated to its intended audience.

-- Judith Meister Johnston and Rob Johnston., Chapter Four – "Testing the Intelligence Cycle Through Systems Modeling and Simulation," in *Analytic Culture in the U.S. Intelligence Community*, The Center for the Study of Intelligence, CIA, 2005, pp 45-46.

-- Also, the process of developing unrefined data into polished intelligence for the use of policymakers (FBI at <http://www.fbi.gov/about-us/intelligence/intelligence-cycle>)

The "Intelligence" Cycle

[The intelligence cycle is] a series of feedback loops, with analyst at the center. Initial problem definition may come from either a policymaker request or an analyst's assessment that an issue merits analytic attention. The analyst then looks at the data available and ideally may engage in a series of interactions with collectors, a series of feedback loops. While in the collection phase, the analyst should be simultaneously engaging with policymakers or the war fighters, as appropriate, to refine questions as conditions change. When a finished intelligence product is produced, it should generate further questions from the consumer, and the feedback loops continue. The process operates on a continuum, as opposed to a discrete series of events with a defined beginning and end.

-- VADM J.M. (Mike) McConnell, USN (Ret) in CISSM, *The Future of Intelligence Analysis, Volume I Final Report*, 10 March 2006
(CISSM = Center for International and Security Studies at Maryland, University of Maryland)

-- Also, an iterative process in which collection requirements based on national security threats are developed, and intelligence is collected, analyzed, and disseminated to a broad range of customers. Consumers sometimes provide feedback on finished intelligence products, which can be used to refine any part of the intelligence cycle to ensure consumers are getting the intelligence they need to make informed decisions and/or take appropriate actions. (Congressional Research Service (CRS) Report RL33616, 14 Jan 2009)

The Intelligence Cycle – *An Iterative Process*

Source: www.intelligence.gov (accessed 27 Jul 2012)

Intelligence shapes national security policies…

The successful intelligence process converts acquired information into clear, comprehensible intelligence and delivers it to the President, policymakers, and military commanders in a form they can utilize to make educated policy decisions. Generating reliable, accurate intelligence is an active, never-ending process commonly referred to as the intelligence cycle.

The process begins with identifying the issues in which policy makers are interested and defining the answers they need to make educated decisions regarding those issues. We then lay out a plan for acquiring that information and go about collecting it. Once we have the proper intelligence, we sort through it, analyze what it means, and prepare summary reports and recommendations, which we deliver to national security policy makers. The answers our reports supply often reveal other areas of concern, which lead to more questions. In this way, the end of one cycle effectively leads to the start of the next.

-- Intelligence.Gov – How Intelligence Works (accessed 28 April 2011) <http://www.intelligence.gov/about-the-intelligence-community/how-intelligence-works/>

Dynamic Process Fueling Dynamic Solutions

Intelligence Cycle… still valid????

According to Kristan J. Wheaton, Assistant Professor of Intelligence Studies at Mercyhurst University, *"Intelligence professionals have long known that the traditional way of describing the intelligence process, the so called 'intelligence cycle,' is flawed." He concludes the intelligence cycle fails on three counts: "We cannot define what it is and what it isn't, it does not match the way intelligence actually works in the 21st Century, and it does not help us explain our processes to the decision-makers we support. Efforts to fix these flaws have not worked and, furthermore, this is all widely recognized by those who have studied the role and impact of the cycle."*

-- See Kristan J. Wheaton, "Let's Kill the Intelligence Cycle," *Competitive Intelligence,* Vol 15 No 2, April/June 2012, pp. 9-24. See article at <http://mciis.org/files/Wheaton_LetsKillTheIntelligenceCycle.pdf>

Intelligence Database. The sum of holdings of intelligence data and finished intelligence products at a given organization. (JP 1-02 and 2-01, Joint and National Intelligence Support to Military Operations, 5 January 2012)

Intelligence Discipline. A well-defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *human intelligence (HUMINT); geospatial intelligence (GEOINT); measurement and signature intelligence MASINT); signals intelligence (SIGINT); open-source intelligence (OSINT); technical intelligence (TECHINT); counterintelligence (CI)*.

Intelligence Enterprise. The sum total of the intelligence efforts of the entire U.S. intelligence community. (ADRP 2-0, Intelligence, Aug 2012, p. 2-6)

Intelligence Estimate. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Intelligence Federation. A formal agreement in which a combatant command joint intelligence center receives preplanned intelligence support from other joint intelligence centers, Service intelligence organizations, Reserve organizations, and national agencies during crisis or contingency operations. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Gap. Information that is needed to inform intelligence analysis but is absent from reporting—*what we know we don't know*.

-- Also, a missing element that, if found, allows one to choose among alternatives with greater confidence. (Robert M. Clark, *Intelligence Analysis: A Target Centric Approach*, 2004)

> ***Identifying [intelligence] gaps is a continuous and iterative process…***
> -- Robert M. Clark, *Intelligence Analysis: A Target Centric Approach* (2004), p. 143

Intelligence Information Need. A need, expressed by users of intelligence, for information necessary to support their mission. (Intellipedia)

Intelligence Information Report (IIR). The primary vehicle used to provide HUMINT information to the consumer. It utilizes a message format structure that supports automated data entry into the Intelligence Community databases. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> IIRs contain *raw intelligence*—unevaluated intelligence information, generally from a single source, that has not been fully evaluated, integrated with other information, or interpreted and analyzed.

-- Also, a report used to provide information collected via HUMINT to DoD and IC customers. The IIR utilizes a message format to support automated data entry into IC databases. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

Intelligence Interrogation. The systematic process of using approved interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence requirements, consistent with applicable law. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *educing information; elicitation; debriefing; interrogation; intelligence interviewing; interview.*

-- Also, the systematic process of using interrogation approaches to question a captured or detained person to obtain reliable information to satisfy foreign intelligence collection requirements. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

> DoD Policy: No person in the custody or physical control of DoD or detained in a DoD facility shall be subject to cruel, inhuman, or degrading treatment or punishment as defined in title XIV of Public Law 109-163, also known as, "The Detainee Treatment Act of 2005." Acts of physical or mental torture are prohibited.
>
> All intelligence interrogations, debriefings, or tactical questioning to gain intelligence from captured or detained personnel shall be conducted humanely, in accordance with applicable law and policy, including Army FM 2-22.3 (*Human Intelligence Collector Operations*, 6 Sep 2006).
>
> ---
>
> Intelligence interrogations and tactical questioning will be conducted only by personnel trained and certified IAW DoDD 3115.09. All DoD interrogations will operate using US Army Field Manual 2-22.3, Human Intelligence Collector Operations.
>
> -- JP 2-01.2, *CI & HUMINT in Joint Operations (U),* 16 Mar 2011 w/ chg 1 dated 26 Aug 2013, p. IV-9
>
> ---
>
> For DoD policy see DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, 11 Oct 2012 with change 1 dated 15 Nov 2013.
>
> Also see *Interrogation: World War II, Vietnam, and Iraq* (Washington, DC: National Intelligence College, Sep 2008); available online at <http://www.ndic.edu/press/12010.htm>

Intelligence Interviewing. The [non-coercive] gathering of useful and accurate information by professionals questioning detainees. (Intelligence Science Board, *Intelligence Interviewing: Teaching Papers and Case Studies*, April 2009) Also see *educing information; elicitation; debriefing; interrogation; interview.*

> See the 2009 Intelligence Science Board report, *Intelligence Interviewing: Teaching Papers and Case Studies*, available online at <www.fas.org/irp/dni/isb/interview.pdf> -- the emphasis of this report is on non-coercive intelligence interviewing.
>
> This report may be of interest to the full range of intelligence professionals involved with interrogation and intelligence interviewing. In particular to those who focus on strategic interrogation and/or "high-value" detainees.

Intelligence Liaison. [Activity which] includes official contacts between a component of the US Intelligence Community and a foreign intelligence or security service which are directly related to espionage or counterintelligence, or other intelligence activities. (DCID 5/1P) Also see *liaison.*

Intelligence Mission Management (IMM). A systematic process by a joint intelligence staff to proactively and continuously formulate and revise command intelligence requirements, and track the resulting information through the processing, exploitation, and dissemination process to satisfy user requirements. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Officer (IO). A professionally trained member of an intelligence service. He or she may be serving in the home country or abroad as a member of a legal or illegal residency. (AFOSI Manual 71-142, 9 Jun 2000 and FBI FCI Terms)

-- Also, a professional employee of an intelligence organization engaged in intelligence activities. (ODNI, U.S. National Intelligence – An Overview 2011)

Intelligence Operations. The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. Intelligence operations include planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, the tasks undertaken by military intelligence units and Soldiers to obtain information to satisfy validated requirements. (ADRP 2-0, Intelligence, Aug 2012)

Note: Intelligence consists of two components: foreign intelligence (FI) and counterintelligence (CI). *Intelligence operations* is a broad term with broad application, whereas "CI operations" is a specific term with a precise application.

Intelligence operations are conducted to provide intelligence in support of all missions.

Intelligence operations gain and maintain contact with threat forces; collect signatures and observables to identify, locate, and provide intentions of threat forces and threat networks. Intelligence operations are not solely accomplished from airborne platforms or standoff surveillance sites. They are often executed in and amongst local populations and in close proximity to threat forces and/or groups. Intelligence operations also facilitate understanding of the terrain and civil considerations within an area of operations.

-- U.S. Army TRADOC Pam 525-2-1, US Army Concept for Intelligence 2016-2028, 13 Oct 2010, p. 9

Intelligence Oversight. The process of independently ensuring all DoD intelligence, counterintelligence, and intelligence-related activities are conducted in accordance with applicable U.S. law, E.O.s, Presidential directives, and DoD issuances designed to balance the requirement for acquisition of essential information by the IC, and the protection of Constitutional and statutory rights of U.S. persons. Intelligence Oversight also includes the identification, investigation, and reporting of questionable intelligence activities and S/HS matters involving intelligence activities. (DoDD 5148.11, ATSD/IO, 24 Apr 2013)

Intelligence Planning (IP). The intelligence component of the Adaptive Planning and Execution system, which coordinates and integrates all available Defense Intelligence Enterprise capabilities to meet combatant commander intelligence requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *Counterintelligence Functional Support Plan (CI FSP).*

-- Also, the intelligence portion of Adaptive Planning and Execution (APEX). Intelligence planning provides a process that effectively integrates, synchronizes, prioritizes and focuses Defense intelligence (both Theater and National) on achieving the supported commander's operational objectives and desired effects during all phases of the plan. Additionally, the process identifies knowledge gaps and capability shortcomings within the DoD intelligence community (IC). (CJCSM 3314.01, Intelligence Planning, 28 Feb 2008)

Note: the term "Intelligence Campaign Planning" or "ICP" is no longer in use; the process is now referred to as "Intelligence Planning."

Intelligence Planning Process. The intelligence component of Adaptive Planning. It is a process that integrates, synchronizes, prioritizes, and focuses DoD Intelligence (both theater and national) on achieving the supported commander's operational objectives and desired effects during all phases of an OPLAN or concept plan. Additionally, the process identifies knowledge gaps and capability shortfalls within DoD Intelligence. (DoDI 5105.21, DIA, 18 Mar 2008)

Intelligence Preparation of the Battlespace (IPB). The analytical methodologies employed by the Services or joint force component commands to reduce uncertainties concerning the enemy, environment, time, and terrain. Intelligence preparation of the battlespace supports the individual operations of the joint force component commands. (JP 1-02 and JP 2-01.3, Joint Intelligence Preparation of the Operational Environment) Also see *Joint Intelligence Preparation of the Operational Environment.*

Intelligence Process. The process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012) Also see *intelligence cycle*.

-- Also, the Army refers to the intelligence cycle as the "intelligence process," which it defines as: intelligence operations are conducted by performing four steps that constitute the intelligence process: Plan, Prepare, Collect, and Produce. Additionally, there are four continuing activities that occur across the four intelligence process steps: Generate intelligence knowledge, Analyze, Assess, and Disseminate. (See Chapter 4, "Intelligence Process in Full Spectrum Operations," Army FM 2-0, Intelligence, Mar 2010)

-- Also, those steps by which information is collected, converted into intelligence, and disseminated. (Senate Report 95-755, Book I – Glossary, 26 Apr 1976)

Intelligence Processing. Conversion of collected information and/or intelligence into a form more suitable for the production of intelligence. (CI Community Glossary and ICS Glossary)

Intelligence Product. An intelligence report disseminated to customers by an intelligence agency or element. The report contains information and/or analysis of potential intelligence value to meet the intelligence needs of users within and outside the Intelligence Community. It may involve current or future developments or capabilities, intentions, and activities of entities of interest. (ICD 208, 17 Dec 2008)

Intelligence Production. The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence for known or anticipated military and related national security consumer requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *production*.

-- Also, conversion of material into finished intelligence through the integration, analysis, evaluation, and/or interpretation of all available data and the preparation of intelligence products is support of known or anticipated customer requirements. (CI Community Glossary and ICS Glossary)

Intelligence Reach. The activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command. (ADRP 2-0, Intelligence, Aug 2012)*

* Note: Supersedes the definition in Army FM 2-0, *Intelligence*, 23 Mar 2010

Three important aspects of intelligence reach
are searches and queries, data mining, and collaboration.
-- ADRP 2-0, *Intelligence*, Aug 2012

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). An act to reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes. IRTPA established both the position of Director of National Intelligence (DNI) and the National Counterterrorism Center (NCTC). (PL 108-458, 17 Dec 2004)

Link to the IRTPA: <http://www.ncix.gov/publications/law/index.html>

Intelligence-Related Activities. Those activities outside the consolidated defense intelligence program that: respond to operational commanders' tasking for time-sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities. (Specifically excluded are programs that

are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.) (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Report (INTREP). A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, a product of the production step of the intelligence cycle. (ICS Glossary)

Intelligence Reporting. The preparation and conveyance of information by any means. More commonly, the term is restricted to reports as they are prepared by the collector and as they are transmitted by the collector to the latter's headquarters and by this component of the intelligence structure to one or more intelligence-producing components. Thus, even in this limited sense, reporting embraces both collection and dissemination. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Intelligence Requirement (IR). 1) Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence; 2) A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *information requirements; collection requirement*.

The articulation of the requirement is the most important part of the process, and it seldom is as simple as it might seem.
– DIA, *Intelligence Essentials for Everyone*, June 1999

-- Also, a requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations (U), 9 Jan 2013 w/ chg 1 dated 13 Jun 2013)

-- Also, [intelligence] requirement: a general or specific validated request for intelligence information made by a user. (National HUMINT Glossary)

-- Also, a type of information requirement developed by subordinate commanders and the staff (including subordinate staffs) that requires dedicated ISR collection for the elements of threat, terrain and weather, and civil considerations. (Army FM 2-0, Intelligence, 23 Mar 2010)

-- Also, the need to collect intelligence information or to produce intelligence, either general or specific, on a particular subject. (ODNI, U.S. National Intelligence – An Overview 2011)

Intelligence Sensemaking. Encompasses the processes by which specialized knowledge about ambiguous, complex, and uncertain issues is created. This knowledge is generated by professionals who in this context become known as Intelligence Sensemakers. (*Sensemaking: A Structure for an Intelligence Revolution* by David T. Moore) Also see *sensemaking*.

Copy of *Sensemaking: A Structure for an Intelligence Revolution* by David T. Moore available at <http://ni-u.edu/ni_press/pdf/Sensemaking.pdf>

Intelligence Source. The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. (JP 2-0, Joint Intelligence, 22 Oct 2013)

An "intelligence source" can be people, documents, equipment, or technical sensors.

Intelligence Sources and Methods. 1) *Sources*: Persons, images, signals, documents, data bases, and communications media capable of providing intelligence information through collection and analysis programs, e.g., HUMINT, IMINT, SIGINT, and MASINT; and 2) *Methods*: Information collection and analysis strategies, tactics, operations and technologies employed to produce intelligence products. If intelligence sources and methods are disclosed without authorization their effectiveness may be substantially negated or impaired. (IC Standard 700-1, 4 Apr 2008)

> The terms "intelligence sources and methods" are used in legislation and executive orders to denote specific protection responsibilities of the Director of National Intelligence (DNI).

Intelligence, Surveillance, and Reconnaissance (ISR). An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations; this is an integrated intelligence and operations function. (DoDD 5143.01; JP 1-02; and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Synchronization. The "art" of integrating information collection and intelligence analysis with operations to effectively and efficiently support decisionmaking. (ADRP 2-0, Intelligence, Aug 2012)

Intelligence System. Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Task List (ITL). A compilation of the specified and implied intelligence tasks required to satisfy the information needs to support the successful achievement of the Combatant Command's operational objectives. The ITL is developed by the Combatant Command J2 and Defense Intelligence Operations Coordination Center (DIOCC). Assignment of roles and responsibilities for the specific collection, analysis and production is accomplished during the development of the [COCOM's IPLAN] and the NISP. The end state is a synchronized collection, analysis and production effort, from tactical to national level that will support the successful achievement of the Combat Command's operational objectives. (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007)

Intelligence Threat. The intention and capability of any adversary to acquire and exploit critical information. The purpose of the acquisition is to gain a competitive edge or diminish the success of a particular U.S program, operations, or industrial activity. (IOSS Intelligence Threat Handbook - Jun 2004) Also see *threat; threat to national security; transnational threat; foreign intelligence collection threat.*

> *Foreign intelligence services, along with terrorist groups, transnational criminal organizations, and other nonstate actors, are targeting and acquiring our national security information, undermining our economic and technological advantages, and seeking to influence our national policies and processes covertly. These foreign intelligence efforts employ traditional methods of espionage and, with growing frequency, innovative technical means.*
>
> *Among significant foreign threats, **Russia** and **China** remain the most capable and persistent intelligence threats and are aggressive practitioners of economic espionage against the United States.*
>
> -- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 12 March 2013

Intellipedia. The Intelligence Community's version of the famous encyclopedia. It is used by analysts, working groups, and engineers throughout the IC. (CIA news release March 2008)

Interagency. United States Government agencies and departments, including the Department of Defense. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011) Also see interagency coordination.

Interagency Coordination. Within the context of DoD involvement, the coordination that occurs between elements of DoD, and engaged US Government agencies and departments for the purpose of accomplishing an objective. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Inter-dependency. [In critical infrastructure usage] relationships or connections between entities of different DoD Components and defense infrastructure sectors. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *intra-dependency*.

Interdiction. 1) An action to divert, disrupt, delay, or destroy the enemy's military surface capability before it can be used effectively against friendly forces, or to otherwise achieve objectives; and 2) In support of law enforcement, activities conducted to divert, disrupt, delay, intercept, board, detain, or destroy, as appropriate, vessels, vehicles, aircraft, people, and cargo. See also air interdiction. (JP 1-02 and JP 3-03, Joint Interdiction, 3 May 2007)

Intergovernmental Organization (IGO). An organization created by a formal agreement (e.g., a treaty) between two or more governments. It may be established on a global, regional, or functional basis for wide-ranging or narrowly defined purposes. Formed to protect and promote national interests shared by member states. Examples include the United Nations, North Atlantic Treaty Organization, and the African Union. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011)

-- Also, an organization comprised primarily of sovereign states (referred to as member states), or of other IGOs. (w/ chg 2 dated 21 Sep 2012, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010)

Internal Security. The state of law and order prevailing within a nation. (JP 1-02 and JP 3-08, Inter-organizational Coordination During Joint Operations, 24 Jun 2011)

International Terrorist Activities. Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum. (DoD 5240.1-R, 7 Dec 1982)

International Terrorism. Activities that involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state. Local, or tribal jurisdiction; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by assassination or kidnapping; and occur totally outside the United States, or transcend national borders in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. (50 USC 1810 Section 101(c) and FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

International Traffic in Arms Regulations (ITAR). A set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). (Wikipedia, accessed 10 Sep 2013)

> ITAR implements the provisions of the Arms Export Control Act (AECA), and are described in Title 22 (Foreign Relations), Chapter I (Department of State), Subchapter M of the Code of Federal Regulations. The Department of State Directorate of Defense Trade Controls (DDTC) interprets and enforces ITAR. Its goal is to safeguard U.S. national security and further U.S. foreign policy objectives.
>
> The related Export Administration Regulations are enforced and interpreted by the Commerce Department. DoD is also involved in the review and approval process. Physical enforcement of import and export laws at border crossings is performed by Customs and Border Protection, an agency of the Department of Homeland Security.
>
> See State Department web site at: http://www.pmddtc.state.gov/regulations_laws/itar_official.html

INTERPOL. The world's largest international police organization, with 188 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime. (www.interpol.int/)

> INTERPOL aims to facilitate international police co-operation even where diplomatic relations do not exist between particular countries. Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights. INTERPOL's constitution prohibits "any intervention or activities of a political, military, religious or racial character."

Interpretation. A part of the analysis and production phase in the intelligence process in which the significance of information is judged in relation to the current body of knowledge. (Previously in JP 2-0, Joint Intelligence, 22 Jun 2007)

Interrogation. Systematic effort to procure information by direct questioning of a person under the control of the questioner. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 **w/** chg 1 dated 26 Aug 2011; and Senate Report 94-755, Book I – Glossary, 26 Apr 1976) Also see *educing information; elicitation; debriefing; intelligence interrogation; intelligence interviewing; interview; strategic intelligence interrogation.*

-- Also, interaction and conversation with a source who appears initially unwilling to provide information. (Educing Information – Interrogation: Science and Art, Dec 2006)

-- Also, systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006 and FM 2-0, Intelligence, 23 Mar 2010)

-- Also [law enforcement interrogation], the systematic effort by law enforcement investigators to prove, disprove, or corroborate information relevant to a criminal investigation using direct questioning in a controlled environment. (FM 19-10 / ATTP 3-39, Law and Order Operations, June 2011)

-- Also, a methodology employed during the interview of a person to obtain information that the source would not otherwise willingly disclose. A typical purpose is not necessarily to force a confession, but rather to develop, playing on the source's character, sufficient rapport as to prompt the source to disclose information valuable to the interrogator. (Wikipedia; accessed 1 Aug 2007)

> Within DoD: Intelligence interrogation is the systematic process of using approved techniques, consistent with applicable law, to question a captured or detained person to obtain reliable information responsive to intelligence requirements. Interrogation is considered an overt HUMINT collection method but is regulated separately from other DoD HUMINT activities.
>
> ———————————
>
> For DoD policy see DoDD 3115.09, *DoD Intelligence Interrogation, Detainee Debriefings, and Tactical Questioning*, 11 Oct 2012.
>
> Per Executive Order 13491, *Ensuring Lawful Interrogations* (22 Jan 2009), only those interrogation approaches and techniques addressed in U.S. Army FM 2-22.3 are authorized.
>
> U.S. Army FM 2-22.3, *Human Intelligence Collector Operations* (Sep 2006), available online at: <http://www.fas.org/irp/doddir/army/fm2-22-3.pdf>

Interrogation Approach. [In detainee operations] an interrogation technique as identified in U.S. Army Field Manual 2-22.3 that is used by trained and certified interrogators to establish and maintain control over and rapport with a detainee in order to gain the detainee's cooperation to answer the interrogator's questions. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

Interview. [In intelligence usage,] to gather information from a person who is aware that information is being given although there is ignorance of the true connection and purposes of the interviewer. Generally overt unless the collector is other than purported to be. (JP 1-02) Also see *educing information; elicitation; debriefing; intelligence interrogation; intelligence interviewing; interrogation.*

-- Also, a nonstructured discussion, where open-ended questions are asked to determine facts about an incident or crime. (FM 19-10 / ATTP 3-39, Law and Order Operations, June 2011)

-- Also, a dynamic human interaction to collect facts to be used for decision-making and/or action-taking. Interviewing is the gathering of facts/information; it is non-accusatory and less structured than an interrogation.

-- Also, a conversation between two or more people (the interviewer and the interviewee) where questions are asked by the interviewer to obtain information from the interviewee. Interviews can be divided into two rough types, interviews of assessment and interviews for information. (Wikipedia)

> Investigative interview is the process whereby an investigator verbally obtains information from people associated with direct knowledge relevant to the investigation.

Intra-dependency. Relationships or connections between entities of a DoD Component and a defense infrastructure sector. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *inter-dependency*.

Intrusion. [In cyber usage], unauthorized access to a DoD, DIB [defense industrial base], or critical infrastructure network, information system, or application. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010 with change 1 dated 16 Oct 2013)

-- Also, unauthorized act of bypassing the security mechanisms of a system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also. movement of a unit or force within another nation's specified operational area outside of territorial seas and territorial airspace for surveillance or intelligence gathering in time of peace or tension. (JP 1-02)

Investigation. The systematic inquiry into an allegation of unfamiliar or questionable activities, wherein evidence is gathered to substantiate or refute the allegation or questionable activity. An investigation is initiated when there are articulable facts that indicate a possible violation of law or policy. Some investigations may be conducted unilaterally by an agency (depending on their authorities), jointly with an external investigate body, or referred to an external investigate body for unilateral investigation. (ONCIX Insider Threat Detection – Glossary) Also see *counterintelligence investigation.*

-- Also, the application of law enforcement and/or counterintelligence authorities and methodologies to conduct a detailed, sustained, structured, and objective inquiry to ascertain the truth about an event, situation, or individual. (SECNAVINST 5430.107, Mission & Functions of the NCIS, 28 Dec 2005)

-- Also, the act of investigating; the process of inquiring into or following up; research; study; inquiry, especially patient or thorough inquiry or examination…. (Wiktionary; accessed 28 June 2012)

> *Conducting a successful investigation is often the result of having a wide range of knowledge and using common sense in its application. There are certain actions that apply to all investigations. Investigators follow these intelligent and logical steps to ensure that an investigation is conducted systematically and impartially. There are certain actions that, over time, have proven useful for specific investigations. It is a wise investigator who understands and applies the knowledge, skills, and techniques learned for a particular investigation and uses them wherever they are most useful in any investigation.*
>
> -- FM 3-19.13, *Law Enforcement Investigations*, Jan 2005, p. 1-15

Investigations, Collections & Operations Nexus (ICON). The Air Force's central counterintelligence and counterterrorism analysis center of excellence; an element of the Air Force Office of Special Investigations (AFOSI).

> *The ICON is AFOSI's primary stop for analytical and specialist support for all criminal and counterintelligence investigations and operations. It is the home to AFOSI's 24/7 Global Watch Center and the current Intelligence Desk which produces AFOSI"S flagship publication, the "AFOSI Blue Line." Additionally, the ICON is responsible for acting as the key liaison and interface with National Intelligence and Law Enforcement organizations for AFOSI's CI, CT, criminal, economic crime, and cyber operational issues.*
>
> -- Air Force Office of Special Investigations

Investigative Jurisdiction. Term for the jurisdiction of an investigative agency over a particular crime or over the locus of where the crime was committed. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Investigative Lead. A person who possesses information about or was a witness to an incident under investigation or a record which contains information of value to the investigation. (AR 381-20, Army CI Program, 25 May 2010) Also see *lead*.

Investigative Plan (IP). A detailed plan for the conduct of a CI investigation to ensure that all investigative activity is conducted in a properly sequenced, coordinated, coherent, timely and efficient manner. The plan should outline the actions to be accomplished to resolve an allegation, a report, or information relating to matters under investigation. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, a document used to plan proposed investigative activities, including special investigative techniques, to support counterintelligence investigation. (Army FM 2-22.2, CI, Oct 2009)

> ***Blueprint for a CI Investigation – a tool to describe the purpose & objectives***
>
> *The IP is the equivalent of an operations order for the conduct of a CI investigation.*
>
> -- 902d MI Group Investigations Handbook, Jun 2012, p.94

> *CI investigations will vary is scope, objective, and resources to successfully resolve the incident under investigation. The IP is the document that provides a detailed road map on the conduct of CI investigations including all investigative participants, all investigative activities required, all resources and external support required, and all interagency or legal coordination required to successfully resolve the incident. IPs are living documents and may require revision due to information development and case direction.*
>
> – Army FM 2-22.2, *Counterintelligence*, Oct 2009 (Chapter 2 - CI Investigations, pp. 2-1 thru 2-47)

Investigative Source. See FOUO definition in AR 381-20, Army CI Program (U), 25 May 2010.

Investigative Source Operation (ISO). A controlled counterintelligence operation that may be used in counterintelligence investigations. Also see *counterintelligence investigation*.

> Three types of CI Investigative Source Operations are: role players; collaborative sources; and investigative access sources.
>
> Proposals for the use of an ISO require proper legal review and formal approval. For detailed information see classified Army Regulation 381-20, *Army Counterintelligence Program (U),* 25 May 2010, Chapter 10 - Counterintelligence Operations, paragraph 10 -2 (pp. 44-47).

Irregular Warfare (IW) A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

-- Also, a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will. (DoD 3000.07, Irregular Warfare, 1 Dec 2008)

-- Also, [as defined by Army] a violent struggle among state and nonstate actors for legitimacy and influence over a population. (FM 3-0, Operations, Feb 2008)

ITAR. See *International Traffic in Arms Regulations*.

J ==========

J-2X. The staff element of the intelligence directorate of a joint staff that combines and represents the principal authority for counterintelligence and human intelligence support. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *2X*.

-- Also, a J-2 staff element normally associated with a deployed joint force, consisting basically of the HUMINT operations cell (HOC) and the task force counterintelligence coordinating authority (TFCICA), and the Operational Support Element (OSE). The J-2X is responsible for coordination and deconfliction of all human source-related activity. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Jack-in-the-Box (JIB). A dummy—sometimes inflatable—placed in a car to deceive [surveillance] about the number of persons in the vehicle. (Spy Book)

> *"A three-dimensional human torso sitting atop a spring-activated scissor-lift mechanism fitted with a rotating head, which collapse[s] into a small portable briefcase or duffel bag. " Can be used to effectively elude surveillance by "controlling the location of the event (an empty street…), the lighting (an unlit area), the audience (the trailing surveillance car), the timing (when the cars were a sufficient distance apart), and the sight line (visible only from the rear)."*
>
> -- H. Keith Melton and Robert Wallace, *The Official CIA Manual of Trickery and Deception* (2009)
>
> ---
>
> *"It is used in an automobile to evade surveillance, by deceiving (a) surveillant(s) that a person being tailed is still in the automobile, when, in fact, the jib has replaced him or her. The FBI was allegedly thus deceived while staking out Edward Lee Howard, the former CIA case officer who escaped and subsequently defected to the former USSR."*
>
> -- Leo D. Carl, *The CIA Insider's Dictionary* (1996), p. 319
>
> ---
>
> *"A jib is an inflatable man-sized dummy first employed by the CIA in the early 1980s. It was designed to replace an operative escaping from the inside of a moving vehicle. As the escapee rolls from the passenger side of the vehicle, the jib is employed. Thus, the jib serves as a decoy for pursuers [trailing surveillance team]."*
>
> -- W. Thomas Smith, Jr., *Encyclopedia of the CIA*, 2003

Jihad. Arabic word derived from a verb that means "to struggle, strive, or exert oneself." Violent extremists understand the concept *jihad* as a "religious call to arms." Also see *jihadist*.

> Historically, key Sunni and Shia religious texts most often referred to *jihad* in terms of religious approved fighting on behalf of Islam and Muslims. Most Al Qaeda-produced ideological material reflects Al Qaeda supporters' shared view of *jihad* as an individual duty to fight on behalf of Islam and Muslims, and, in some case, to offensively attack Muslims and non-Muslims who are deemed insufficiently pious or who oppose enforcement of Islamic principles and religious law.
>
> The terms *jihadist, violent Islamist*, and *militant Islamist* refer to groups and individuals whose statements indicate that they share such an understanding of *jihad* and who advocate or use violence against the United States or in support of transnational Islamist agendas.
>
> -- Congressional Research Service (CRS) Report R41674, 8 Mar 2011
>
> ---
>
> *…[J]ihad is a complex term that can be understood in a number of different ways. Traditional Islamic jurisprudence distinguishes between two major levels of jihad. The Greater Jihad refers to the inner struggle of the individual believer to affirm his or her commitment to the requirements of Islam, and is also called jihad of the heart. It is the Lesser Jihad, or jihad of the sword (often translated "holy war," a translation the author scrupulously avoids) that is the central concern of his study.*

> *Sometimes called the "sixth pillar of Islam," there is no question that jihad is a required commitment of the Muslim. Moreover, although most Qur'anic verses define it as the collective responsibility all Muslims to defend the community against non-Muslim aggressors, there are a few verses, as well as hadith (authentic traditions ascribed to the Prophet Muhammad), that can be interpreted to justify wars of imperial conquest. It is also certainly true that at various times in Islamic history conquerors have used the concept of jihad to justify imperial expansion.*
>
> -- Max L. Gross, Dean of the School of Intelligence Studies, Joint Military Intelligence College, and Middle East scholar and intelligence analyst. (As quoted in Joint Military Intelligence College, Discussion Paper 13, entitled *Global War Terrorism: Analyzing the Strategic Threat*, Nov 2004, p. viii-ix).

Jihadist. Term describes radicalized individuals using Islam as an ideological and/or religious justification for their belief in the establishment of a global caliphate, or jurisdiction governed by a Muslim civil and religious leader known as a caliph. (CRS Report R41416, 23 Jan 2013) Also see *jihad*.

> Jihadists draw on Salafi Islam—the fundamentalist belief that society should be governed by Islamic law based on the Quran and following the model of the immediate followers and companions of the Prophet Muhammad.
>
> The CRS Report points out there is an important distinction between the terms "radicalization" and "violent extremism" as it relates to the threshold of U.S. law enforcement interest and action. This is because Americans have the right under the First Amendment to adopt, express, or disseminate ideas, even hateful and extremist ones. But when radicalized individuals mobilize their views, i.e., they move from a radicalized viewpoint to membership in a terrorist group, or to planning, materially supporting, or executing terrorist activity, then the nation's public safety and security interests are activated. Thus, the terms may be differentiated as follows:
>
> -- ***"Radicalization"*** describes the process of acquiring and holding radical, extremist, or jihadist beliefs.
>
> -- ***"Violent Extremism"*** describes violent action taken on the basis of radical or extremist beliefs. For many, this term is synonymous with "violent jihadist" and "jihadist terrorist."
>
> The term "violent jihadist" characterizes jihadists who have made the jump to illegally supporting, plotting, or directly engaging in violent terrorist activity.
>
> See CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*. For more on Salafi Islam, see CRS Report RS21695, *The Islamic Traditions of Wahhabism and Salafiyya*.
>
> For more on Al Qaeda's global network, see CRS Report R41070, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*.

Joint. Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (JP1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02)

Joint Base. For purposes of base defense operations, a joint base is a locality from which operations of two or more of the Military Departments are projected or supported and which is manned by significant elements of two or more Military Departments or in which significant elements of two or more Military Departments are located. (JP 1-02 and JP 3-10, Joint Security Operations in Theater, 03 February 2010)

Joint Captured Materiel Exploitation Center (JCMEC). A physical location for deriving intelligence information from captured enemy materiel. It is normally subordinate to the Joint Force/J-2. (JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Joint Counterintelligence Unit (JCIU). An organization composed of Service and Department of Defense agency counterintelligence personnel, formed under the authority of the Secretary of Defense and assigned to a combatant commander, which focuses on the combatant command strategic and operational counterintelligence missions. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, an organization composed of Service and Defense agency CI personnel, formed under the authority of a Secretary of Defense-approved operation order, which focuses on combatant command strategic and operational CI missions within an area of conflict. This unit is under the command authority of the Combatant Commander, or his or her duly designated subordinate joint force commander, for the duration of the operation, or as otherwise specified in the operation plan or order. (DoDI S-5240.09, OFCO, 29 Oct 2008)

For more detailed discussion of the JCIU see Appendix B, Joint Counterintelligence Unit (U), JP 2-01.2, *CI & HUMINT in Joint Operations (U),* 16 Mar 2011 w/ chg 1 dated 26 Aug 2011.

Also see the *Joint Counterintelligence Unit Handbook (U)*, published June 2010 by the Defense CI & HUMINT Center (D2X-ES-C Lessons Learned Branch).

For lessons learned see the following classified reports —
-- (U) *Strategic CI Directorate Iraq (SCID-I) Lesson Learned Report*, 5 Jun 2009
-- (U) *Strategic CI Directorate Afghanistan (SCID-A) Lesson Learned Report*, undated circa Jun 2010)

Note: The transition of Strategic CI Directorates (SCIDs) to Joint CI Units (JCIUs) was not merely a change in title—it fundamentally changed the SCID from a CI organization with no clear chain of command to a CI unit that is directed, controlled, and focused by the Combatant Commander at the operational level of war.

Joint Counterintelligence Training Academy (JCITA). Professional training and education institution for advanced joint DoD CI training. (DoDI 3305.11, DoD CI Training, 19 Mar 2007) See *counterintelligence training.*

-- Also, the primary professional training and education center for advanced and joint CI training within DoD and is known as the DoD Center of Excellence for CI training. (DoDI JCITA, 13 Nov 2013)

JCITA provides advanced counterintelligence training to the Department of Defense and other national security stakeholders agencies within the federal government.

JCITA SIPRNet website at: <https://jcita.dia.smil.mil>

JCITA …training counterintelligence today to protect our nation tomorrow.

Joint Deployable Intelligence Support System (JDISS). A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Joint Doctrine. Fundamental principles that guide the employment of US military forces in coordinated action toward a common objective. Joint doctrine contained in joint publications also includes terms, tactics, techniques, and procedures. It is authoritative but requires judgment in application. (JP 1-02)

Joint Document Exploitation Center (JDEC). A physical location for deriving intelligence information from captured adversary documents including all forms of electronic data and other forms of stored textual and graphic information. It is normally subordinate to the joint force intelligence directorate. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, a joint center established to receive, inventory, catalogue, selectively translate, and disseminate captured or acquired documents and media. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Joint Force. A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. (JP 1-02)

Joint Force Commander (JFC). A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. (JP1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02) Also see *joint force*.

Joint Intelligence. Intelligence produced by elements of more than one Service of the same nation. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Joint Intelligence Operations Center (JIOC). An interdependent, operational intelligence organization at the Department of Defense, combatant command, or joint task force (if established) level, that is integrated with national intelligence centers, and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, those centers, below the Defense-level (COCOM and specified Unified Commands) established by the Secretary of Defense on 3 April 2006, to plan, prepare, integrate, direct, synchronize, and manage continuous, full-spectrum defense intelligence operations within their respective AORs. The J2 of each command is designated as the respective JIOC Director. (DIA HUMINT Manual, Vol I, DHE-M 3301.001, 30 Jan 2009 w/ chg 2 dated 1 Feb 2012)

Joint Intelligence Preparation of the Operational Environment (JIPOE). The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the operational environment; describing the impact of the operational environment; evaluating the adversary; and determining adversary courses of action. (JP 1-02 and JP 2-01.3, Joint Intelligence Preparation of the Operational Environment)

Joint Intelligence Support Element (JISE). A subordinate joint force element whose focus is on intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Joint Intelligence Task Force-Combating Terrorism (JITF-CT). See *Defense Combating Terrorism Center (DCTC).*

In the fall of 2012 the JITF-CT transitioned to the Defense Combating Terrorism Center (DCTC).

Joint Intelligence Training (JIT). Fundamental training that guides the development and utilization of intelligence professionals and organizations designed to support two or more Services employed in coordinated action. (DoDI 3305.14, JIT, 28 Dec 2007)

Joint Inter-Agency Cyber Task Force (JIACTF). Joint inter-agency task force created by the Director of National Intelligence (DNI) to execute DNI responsibilities in monitoring and coordinating the CNCI and to report to the President on Comprehensive National Cybersecurity Initiative (CNCI) implementation, together with recommendations as deemed appropriate. (Securing Cyberspace for the 44th Presidency, Dec 2008)

Joint Interrogation and Debriefing Center (JIDC). Physical location for the exploitation of intelligence information from detainees and other sources. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> JIDCs are established under the direction of the joint force commander within the joint operations area and are normally collocated with detainee holding facilities. The mission of the JIDC is to conduct screening and interrogation of detainees, questioning of walk-in sources, and translation and exploitation of documents associated with detainees. The JIDC coordinates exploitation of captured equipment with the joint captured material exploitation center, captured documents with the joint document exploitation center, and high-value human sources with the joint strategic exploitation center.
>
> For additional information see JP 3-63, *Detainee Operations*, 30 May 2008

Joint Interrogation Operations (JIO). 1) Activities conducted by a joint or interagency organization to extract information for intelligence purposes from enemy prisoners of war, dislocated civilians, enemy combatants, or other uncategorized detainees; or 2) Activities conducted in support of law enforcement efforts to adjudicate enemy combatants who are believed to have committed crimes against US persons or property. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Joint Investigation. An investigation in which more than one investigative agency has established investigative authority over an offense and/or subject of the investigation, and the agencies involved agree to pursue the investigation in concert, with agreements reached detailing investigative responsibilities, procedures, and methods. (CI Community Lexicon)

Joint Operational Planning. Planning activities associated with joint military operations by combatant commanders and their subordinate joint force commanders in response to contingencies and crises. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Joint Operation Planning and Execution System (JOPES). An Adaptive Planning and Execution system technology. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Joint Operation Planning Process (JOPP). An orderly, analytical process that consists of a logical set of steps to analyze a mission, select the best course of action, and produce a joint operation plan or order. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Joint Operations. A general term to describe military actions conducted by joint forces and those Service forces employed in specified command relationships with each other, which of themselves, do not establish joint forces. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Joint Operations Area (JOA). An area of land, sea, and airspace, defined by a geographic combatant commander or subordinate unified commander, in which a joint force commander (normally a joint task force commander) conducts military operations to accomplish a specific mission. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Joint Personnel Adjudication System (JPAS). The centralized database of standardized personnel security processes; virtually consolidates the DoD Central Adjudication Facilities by offering real time information concerning clearances, access, and investigative statuses to authorized DoD security personnel and other interfacing organizations. (IC Standard 700-1, 4 Apr 2008)

-- Also, the centralized Department of Defense database of standardized personnel security processes; virtually consolidates the DoD Central Adjudication Facilities by offering real time information concerning clearances, access, and investigative statuses to authorized DoD security personnel and other interfacing organizations (e.g., Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management, and the Air Force personnel Center). (DSS Glossary)

Joint Personnel Recovery Center (JPRC). The primary joint force organization responsible for planning and coordinating personnel recovery for military operations within the assigned operational area. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Joint Strategic Capabilities Plan (JSCP). A plan that provides guidance to the combatant commanders and the Joint Chiefs of Staff to accomplish tasks and missions based on current military capabilities. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Joint Strategic Exploitation Center (JSEC). Theater-level physical location for an exploitation facility that functions under the direction of the joint force commander and is used to hold detainees with potential long-term strategic intelligence value, deemed to be of interest to **counterintelligence** or criminal investigators, or who may be a significant threat to the Unites States, its citizens or interest, or US allies. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> The JSEC is a theater-level exploitation facility and is normally collocated with a rear area collection and holding center for detainees. The JSEC's mission is the conduct of interrogations and debriefings to generate intelligence information responsive to theater and national requirements, and to identify detainees with potential long-term strategic intelligence value, deemed to be of interest to **counterintelligence** or criminal investigators, or who may be a significant threat to the United States, its citizens or interests, or US allies.

Joint Task Force (JTF). A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. (JP 1-02)

Joint Task Force Counterintelligence Coordinating Authority. See *Task Force Counterintelligence Coordinating Authority (TFCICA).*

Joint Terrorism Task Forces (JTTFs). Small cells of highly trained, locally based, investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. It is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. (DoJ website: <http://www.usdoj.gov/jttf/>) Also see *National Joint Terrorism Task Force*.

-- Also, a coordinated "action arm" for federal, state, and local government response to terrorist threats in specific U.S. geographic regions. The FBI is the lead agency that oversees the JTTFs. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, an FBI-led task force whose primary mission is to collect intelligence of actual, suspected, or planned acts of terrorism directed against U.S. persons and property. (DoD FCIP Strategy FY 2013-2017)

> *JTTFs were established by the FBI to conduct operations to predict and disrupt terrorist plots. JTTFs are in over 100 cities nationwide; in addition, there is at least one in each of the FBI's 56 field offices. The National Joint Terrorism Task Force (NJTTF), in Washington, D.C., coordinates all the JTTFs.*
>
> -- ODNI, *U.S. National Intelligence – An Overview 2011*, p. 30
>
> ---
>
> *Joint Terrorism Task Forces (JTTFs) are based in 103 cities nationwide, with at least one in each of the FBI's 56 field offices. They include more than 4,400 members nationwide and represent some 600 state and local agencies and 50 federal agencies.*
>
> -- FBI, *Today's FBI: Facts & Figures 2013-2014*
>
> ---
>
> *DoD CI personnel participating on JTTFs work in partnership with other JTTF members to detect and neutralize terrorists, terrorist-enabling individuals, and organizations threatening DoD interest.*
>
> -- DoDI 5240.22, *CI Support to Force Protection*, 24 Sep 2009, p. 6

Joint Worldwide Intelligence Communications System (JWICS). The sensitive compartmented information portion of the Defense Information Systems Network, which incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, the Intelligence Community's TS-SCI global network; a communications network that delivers secure information services to national and defense intelligence components around the world. All U.S. Government TS-SCI networks run off of JWICS. (National Intelligence: A Consumer's Guide - 2009)

Judgment. [As used in intelligence analysis] Judgment is what analysts use to fill gaps in their knowledge. It entails going beyond the available information and is the principal means of coping with uncertainty. It always involves an analytical leap, from the known into the uncertain. Judgment is an integral part of all intelligence analysis. (*Psychology of Analysis* by Richards J. Heuer, Jr, 1999)

K ==========

Key. A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Key Enabler. That crucial element that supplies the means, knowledge, or opportunity that allows for the success of an assigned task or mission. (USJFCOM Glossary)

Key Facilities List. A register of selected command installations and industrial facilities of primary importance to the support of military operations or military production programs. It is prepared under the policy direction of the Joint Chiefs of Staff. (JP 1-02)

Keystroke Monitoring. The process used to view or record both the keystrokes entered by a computer user and the computer's response during an inactive session. (NIST, Glossary of Key Information Security Terms, May 2013)

Khobar Towers Bombing. A terrorist [truck] bombing of the residence of U.S. military personnel at the Khobar Towers complex in Dhahran, Saudi Arabia, on 25 June 1996 killed 19 American military personnel and wounded hundreds more. (Words of Intelligence, 2nd Edition, 2011)

Knowledge. In the context of the cognitive hierarchy, information analyzed to provide meaning and value or evaluated as to implications for the operation. (FM 6-0, Mission Command, 11 Aug 2003).

Knowledge Management. The process of enabling knowledge flow to enhance shared understanding, learning, and decisionmaking. (ADRP 6-0, Mission Command, May 2012)

Knowledgeability Brief (KB). A document used to notify consumers of the availability and background of an overt source for debriefing. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

L ==========

Laundering. In counterdrug operations, the process of transforming drug money into a more manageable form while concealing its illicit origin. Foreign bank accounts and dummy corporations are used as shelters. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

-- Also, a process of hiding sources, transmittal, and people involved in financial matters and transfers of money for intelligence and today more commonly for criminal purposes, primarily associated with terrorist activity and narcotics trafficking. (Words of Intelligence, 2nd Edition, 2011)

Law Enforcement. Activities to protect people, places and things from criminal activity resulting from non-compliance with laws, includes patrols, emergency responses, undercover operations, arrests, raids, etc.

-- Also, the generic name for the activities of the agencies responsible for maintaining public order and enforcing the law, particularly the activities of prevention, detection, and investigation of crime and the apprehension of criminals. (www.ojp.usdoj.gov; accessed 29 Apr 2013)

Counterintelligence is part art, part science, a discipline aimed at identifying and exploiting or stopping foreign spies. Law enforcement is easier: You identify the bad guys and arrest them.

-- Bill Gertz, "Enemies," *The Washington Times*, 18 Sep 2006

Traditional law enforcement activities aim at apprehending and prosecuting perpetrators of criminal activity after the commission of their crimes. In most circumstances, the primary responsibility of law enforcement is to determine whether a crime has been committed, conduct an investigation to identify and apprehend the perpetrator, and gather evidence to assist prosecutors in a criminal trial.

Law Enforcement is police work waging a war against crime—*it's evidence-prosecution centric*. Whereas counterintelligence is national security work waging a war against foreign intelligence threats—*it's information-exploitation centric.*

Each operates in fundamentally dissimilar manners… *different legal authorities, oversight structures, governing paradigms, cultures, etc.* These two disciplines merge or intersect when hidden intelligence activity is also criminal, i.e., national security crimes (espionage, treason, spying, etc.).

"Effective enforcement of U.S. espionage statues and Articles 104 and 106 of the Uniform Code of Military Justice is essential to national security…. Services have different approaches to counterintelligence due to their unique missions.… NCIS and AFOSI counterintelligence doctrine holds that counterintelligence primarily is a law enforcement issue. …under Army counterintelligence doctrine, counterintelligence is, first and foremost, an intelligence mission…. Considerable intersection exists between law enforcement, counterintelligence, and intelligence in the areas of espionage, terrorism, and low-intensity conflict…. The law enforcement, counterintelligence, and intelligence collection disciplines must complement one another."

-- "Report of the Advisory Board on the Investigative Capability in the Department of Defense - Vol. I," Department of Defense, January 1995, pp. 67-75.
Copy available online at: <http://handle.dtic.mil/100.2/ADA299523>

The goals of law enforcement and intelligence collection conflict…

"Law enforcement agencies collect information solely to put criminals in prison—a onetime, short-term goal; pay the informant, make a bust, go to trial with the informer as witness. Espionage is conducted for long-term production of intelligence: recruit the agent, collect the information, hopefully for years or decades."

-- Duane R. Clarridge, *A Spy For All Seasons: My Life in the CIA* (1997), p. 409

Law Enforcement Agency (LEA). Any of a number of agencies (outside the Department of Defense) chartered and empowered to enforce US laws in the United States, a state or territory (or political subdivision) of the United States, a federally recognized Native American tribe or Alaskan Native Village, or within the borders of a host nation. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

Law Enforcement Officer. An employee, the duties of whose position are primarily the prevention, investigation, apprehension, or detention of individuals suspected or convicted of offenses against the criminal laws, including an employee engaged in this activity who is transferred to a supervisory or administrative position; or serving as a probation or pretrial services officer. (Cited as 18 USC at <http://www.lectlaw.com/def/l008.htm>)

Law of War. That part of international law that regulates the conduct of armed hostilities. Also called the law of armed conflict. (JP 1-02 and JP 1-04, Legal Support to Military Operations,17 August 2011)

Lawful Search. An examination, authorized by law, of a specific person, property, or area for specified property evidence, or a specific person, for the purpose of seizing such property, evidence or person. (AR 190-30, Military Police Investigation, 1 Nov 2005)

Lead. In intelligence usage, a person with potential for exploitation, warranting additional assessment, contact, and/or development. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Counterintelligence Operational Lead (CIOL).*

-- Also, an identified potential source. (HDI Lexicon, April 2008 and Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, [for investigative purposes,] single investigative element of a case requiring action. (IC Standard 2008-700-01, 4 Apr 2008)

-- Also, any source of information that, if exploited, may reveal information of value in the conduct of a counterintelligence investigation. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, for CI collection purposes, any person who has the potential to provide information of value to the supported command. (DoD, CI Functional Services IWG Handbook, 19 Feb 2009)

Lead Agency. The US Government agency designed to coordinate the interagency oversight of the day-to-day conduct of an ongoing operation. (JP 1-02 and JP 3-08 Interorganizational Coordination During Joint Operations, 24 June 2011)

-- Also, in CI usage concerning an investigation, the agency in a joint investigation that has primary authority concerning the offense committed or is designated as such by agreement of the investigative agencies involved. The lead agency is ultimately responsible for determination of investigative responsibilities, procedures, and methods. Also see *joint investigation.*

Lead Federal Agency (LFA). The federal agency that leads and coordinates the overall federal response to an emergency. Designation and responsibilities of a lead federal agency vary according to the type of emergency and the agency's statutory authority. (JP 1-02 and JP 3-41, CBRNE Consequence Management, 2 Oct 2006)

Leaks. See *unauthorized disclosure*.

National Security Leaks

"I am deeply disturbed by the continuing leaks of classified information to the media…, disclosures of this type endanger American lives and undermine America's national security."

-- Senator Dianne Feinstein, Chairman of the Senate Intelligence Committee, 5 June 2012

Least Intrusive Means. See *Rule of Least Intrusive Means*. The collection of information about US persons shall be accomplished by the *least intrusive means*.

Legal Attaché (LEGAT). The FBI has offices around the globe. These offices—called legal attachés or legats—are located in U.S. embassies. (fbi.gov) -- See <http://www.fbi.gov/contact-us/legat>

-- Also, the title of FBI special agents deployed abroad to liaison posts in overseas diplomatic missions… (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Legal Residency. An intelligence apparatus in a foreign country composed of intelligence officers assigned as overt representatives of their government, but not necessarily identified as intelligence officers. (ICS Glossary)

Legal Traveler. Any individual traveling with legitimate documentation to perform a specific collection or support mission. (National HUMINT Glossary)

-- Also, any individual traveling with legal documentation to perform specified intelligence collection or support missions, or any individual who may be selected for debriefing on legal travel to or through geographical areas of interest. (AR 381-20, Army CI Program, 25 May 2010)

Legend. The complete cover story developed for an operative. (CI Centre Glossary)

-- Also, a coherent and plausible account of an individual's background, living arrangements, employment, daily activities, and family given by a foreign intelligence service by an illegal or agent. Often the legend will be supported by fraudulent documents. (FBI FCI Terms)

-- Also, false identify that an agent builds up through forged documents and other means such as living under the name of the person whose identify he assumes. (Spy Book)

-- Also, a carefully constructed cover for an intelligence officer. (Spycraft)

-- Also, a spy's fictional identity and a complete cover story developed for operatives. (*Encyclopedia of Cold War Espionage, Spies, and Secret Operations*, 3rd edition, 2012)

Liaison. That contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011) Also see *intelligence liaison*.

-- Also, [activity] conducted to obtain information and assistance, to coordinate or procure material, and to develop views necessary to understand counterparts. Liaison contacts are normally members of the government, military, law enforcement, or other member of the local or coalition infrastructure. The basic tenet of liaison is *quid pro quo*. An exchange of information, services, material, or other assistance is usually a part of the transaction. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

A basic tenet of liaison is quid pro quo (something for something exchange.

-- FM 2-22.2, Counterintelligence , October 2009, p. 4-8

"A crucial but often overlooked part of U.S. intelligence efforts is liaison with foreign intelligence services…. A productive liaison relationship does not necessarily preclude spying on each other—but it does mean both sides try to be especially careful not to get caught at it."

-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

"*Liaison is not explicitly spelled out in the theoretical approaches [regarding] intelligence. If one looks to the intelligence cycle paradigm, one will even discover that liaison has no fixed location in the cycle… it is actually a mode of activity in every point in the intelligence cycle [and] shares this quality with counter-intelligence*."

-- Dutch Analysts Bob De Graaf and Cees Wiebes in Jeffreys-Jones, *External Vigilance* (1997)

"Answering questions about the costs and benefits of foreign intelligence liaison requires a thorough understanding of the subject in theory and in U.S. practice. Although sometimes equated with intelligence sharing, intelligence liaison is actually better understood as a form of subcontracted intelligence collection based on barter."

-- Dr. Jennifer E. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and Counterintelligence*, Vol 19 No 2 (Summer 2006), p. 196

"Liaison has a number of associated risks, one being the problem of false corroboration. It is not uncommon for several intelligence services to unwittingly use the same agent."

-- Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (2004), p. 72

Liaison Operations. Operations to coordinate activities and exchange information with foreign military, governmental, and non-governmental civilian agencies. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2011)

According to Army FM 2-22.3 (HUMINT Collector Operations), "liaison operations" are programs to coordinate activities and exchange information with host country and allied military and civilian agencies and NGOs. CI liaison activities are designed to ensure a cooperative operating environment for CI elements and/or to obtain information, gain assistance, develop CI leads for further exploitation, procure material, etc.

Lie. Any statement made with the intent to deceive. (Textbook of Political-Military Counterdeception: Basic Principles & Methods, August 2007)

Light Cover [aka shallow cover]. A type of cover that will not withstand close scrutiny or due diligence. (National HUMINT Glossary)

Line of Operations. 1) A logical line that connects actions on nodes and/or decisive points related in time and purpose with an objective(s). 2) A physical line that defines the interior or exterior orientation of the force in relation to the enemy or that connects actions on nodes and/or decisive points related in time and space to an objective(s). (JP 1-02)

-- Also, a line that defines the directional orientation of a force in time and space in relation to the enemy and links the force with its base of operations and objectives. (Army FM 3-0, Operations, Feb 2008)

Link. A behavioral, physical, or functional relationship between nodes. (JP 1-02)

Link Analysis. Subset of network analysis, exploring associations between objects.

Listening Post. A secure site at which signals from an audio operation are monitored and/or received. (Spycraft)

Load. Tradecraft jargon… to put something in a dead drop; to service a dead drop. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Load Signal. A visual signal to indicate the presence of an individual or object at a given location. (HDI Lexicon, April 2008)

-- Also, …a visual signal displayed in a covert manner to indicate the presence of an individual or object at a given location. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Local Agency Check (LAC). A review of the appropriate criminal history and court records in jurisdictions over areas where the Subject has resided, attended school, or been employed during a specific period of time. (IC Standard 700-1, 4 Apr 2008) Also see *Military Agency Check; National Agency Check*.

-- Also, a records or files check of official or publicly available information retained by any local office or government agency within the AO [area of operation] of the field element conducting the check. (FM 2-22.2, Counterintelligence, October 2009)

-- Also, a records or files check of official or publicly available information conducted at any local office or government agencies within the operational area of the [CI] field element conducting the check. These records may include holdings and databases maintained by local and state law agencies, local courts, and local offices of federal agencies. (902d MI Group Investigations Handbook, Jun 2012)

-- Also, an investigative check of local police departments, courts, etc., to determine whether the subject has been involved in criminal conduct. The LAC is a part of all Personnel Security Investigations (PSIs) except the Entrance National Agency Check (ENTNAC). (DSS Glossary)

Logic Bomb. A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. (NIST, Glossary of Key Information Security Terms, May 2013)

-- Also, computer jargon for programmed instructions clandestinely inserted into software, where they remain inactive and undetected until the computer reached a certain point in its operations, at which time the instructions take over. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

-- Also, [in cyber usage] also known as a "time bomb," a program that allows a Trojan to lie dormant and then attack when the conditions are just right. Triggers for logic bombs include a change in a file, a particular series of keystrokes, or a specific time or date. (McAfee Labs - Threat Glossary)

Lone Wolf. A lone wolf or lone-wolf fighter is someone who commits violent acts in support of some group, movement, or ideology, but does so alone, outside of any command structure. (Wikipedia; accessed 28 Jun 2011)

The lone wolf – one of the biggest challenges

Individuals who sympathize with or actively support al-Qa'ida may be inspired to violence and can pose an ongoing threat, even if they have little or no formal contact with al-Qa'ida.

-- National Strategy for Counterterrorism, June 2011, p. 4

Lone wolf terrorism involves terrorist attacks carried out by persons who (a) operate individually, (b) do not belong to an organized terrorist group on network, and (c) whose modi operandi are collected are conceived and directed by the individual without any direct outside hierarchy.

-- Flükiger, "The Radical," pp. 111-119.

"Inspire" magazine -- al Qaeda of the Arabian Peninsula's English-language magazine -- has a regular feature called "Open Source Jihad" …that is intended to train… lone wolves and small cells in the West to conduct attacks and to provide them with the tools necessary to do attacks. [This magazine seeks to encourage] …jihadists to conduct lone wolf attacks. Lone wolf assailants are really the most difficult type for government intelligence and security agencies to gather intelligence about. Really to find a lone wolf assailant, you need to monitor his activities closely and understand what's going on inside his head if he doesn't communicate to other people. Because of this, the lone wolf really presents a challenge to Western security and intelligence agencies.

-- Stratfor.com (4 April 2010)
<http://www.stratfor.com/analysis/20110404-dispatch-al-qaedas-inspire-magazine>

A Lone Wolf is characterized by the following operational strengths and weaknesses. First, it is difficult to anticipate who a Lone Wolf is because there is no longer any need for physical contact with extremists for radicalization to occur. As Raffaello Pantucci puts it in his article on Lone Wolves: "The increasing prevalence of the Internet and the easy availability of extremist material online have fostered the growth of the autodidactic extremist." Second, ***the Lone Wolf actor is the most difficult terrorist to detect, deter, or capture, because his planning takes place almost entirely within his own mind*** [emphasis added].

-- Thomas F. Ranieri with Spencer Barrs, "Internet and Ideology: The Military Counterintelligence Challenges of the *Net Wolf*," *American Intelligence Journal*, Vol 29, No 2, 2011, p. 82

Lookout. Stationary position from which a fixed surveillance is conducted and is ostensibly hidden from view or knowledge of the target of the surveillance. (Words of Intelligence, 2nd Edition, 2011)

Low Visibility Operations. Sensitive operations wherein the political-military restrictions inherent in covert and clandestine operations are either not necessary or not feasible; actions are taken as required to limit exposure of those involved and/or their activities. Execution of these operations is undertaken with the knowledge that the action and/or sponsorship of the operation may preclude plausible denial by the initiating power. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

M ==========

M3. Acronym for "Multimedia Message Manager" within the DoD Intelligence Information System (DoDIIS). M3 provides automated text message handling to the military and civilian intelligence community in a classified environment.

> M3 is the standard message handler for the DoDIIS community which provides: real-time dissemination of incoming message traffic based on user interest profiles; retrospective search of archive message database; and message composition, co-ordination, release and validation. M3 software automatically filters and delivers personalized information to individuals and groups, based on their content and delivery preferences. The search software also enables users to search through more than 20 years' worth of stored messages.

Mail Cover. The process by which a record is made of any data appearing on the outside cover of any class of mail matter as permitted by law, other than that necessary for the delivery of mail or administration of the Postal Service. (DoD 5240.1-R, Dec 1982)

-- A record of information on the outside (cover) of any mail piece. It is kept to locate a fugitive, protect national security, or obtain evidence of a crime punishable by a prison term exceeding 1 year. This record is one of the few ways information on mail may be disclosed outside the USPS, and its use is lawful only if authorized by postal regulations. (USPS Pub 32, *Glossary of Postal Terms*, May 1997)

-- Also, an investigative tool used to record information on the outside container, envelope, or wrapper of mail, including the name and address of the sender and the place and date of postmarking. (USPS Publication 146, *A Law Enforcement Guide to the U.S. Postal Service,* Sep 2008)

> Postal Service Regulation 39 CFR § 233.3 is the sole authority and procedure for opening a *mail cover* and for processing, using and disclosing information obtained from a *mail cover*.
>
> See USPS Pub 146, *A Law Enforcement Guide to the U.S. Postal Service* (Sep 2008)* and USPS Pub 55, *USPS Procedures: Mail Cover Requests,* available from the US Postal Service by request to authorized users.
>
> * USPS Pub 146 also available at: <www.hsdl.org/?view&doc=112575&coll=limited>

Make (aka made). Tradecraft jargon… surveillance term for the surveillant being detected by the subject of a surveillance. (Leo D. Carl, The CIA Insider's Dictionary, 1996)

Malicious Code. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. (NIST, Glossary of Key Information Security Terms, May 2013) Also see *malware, Trojan Horse.*

Malicious Cyber Activity. Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. (PPD-20, US Cyber Operation (U), 16 Oct 2012)

Malware. A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (NIST, Glossary of Key Information Security Terms, May 2013)

-- Also, a generic term used to describe malicious software such as viruses, Trojan horses, spyware, and malicious active content. (McAfee.com; accessed 15 Nov 2010)

-- Also, malicious or malevolent software, including viruses, worms, and Trojans, that is preprogrammed to attack, disrupt, and/or compromise other computers and networks. A packaged exploitation of vulnerability, there is often a "payload" of instructions detailing what the system should do after it has been compromised. (Cybersecurity and Cyberwar)

-- Also, malicious software that secretly accesses a computer system without the owner's informed consent. A general term to mean a variety of forms of hostile, intrusive, or annoying software or program code, including computer viruses, worms, trojan horses, spyware, most rootkits, and other malicious software or program. (Wikipedia)

Malware -- an acronym that stands for MALicious softWARE -- comes in many forms. Generally speaking, malware is software code or snippets of code designed with malice in mind and usually performs "undesirable actions" on a host system.

According to Kevin Coleman, *Defense Systems*, "…in 2009, there were 25 million new strains of malware. That equals a new strain of malware every 0.79 seconds." Recently he blogged that "…in the past month [Sep 2012] there were more than 2,166,000 new strains of malware introduced into our operational environment."

-- Source: <http://defensesystems.com/blogs/cyber-report/2012/09/cyber-threats.aspx?sc_lang=en > (accessed 15 Dec 2012)

According to an article in the *Journal of Homeland and National Security Perspectives*, In 2008, *"a service member in the Middle East inserted a flash drive with malware known as agent.btz into a classified government computer. The worm infected the classified intranets titled Secret Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence communication System (JWICS). The worm had been designed to execute a predetermined search once on the targeted computer system, upon finding the desired data it would transfer it covertly to the thumb drive, and once reinserted into a machine connected to the internet the data immediately transferred from the thumb drive back to the creators of the malware. The foreign intelligence agency that designed this worm, suspected of being Russian Intelligence, created a highly sophisticated worm in agent.btz that could think for itself, morphing when threatened and capable of identifying and using multiple exfiltration paths. Agent.btz is probably not the only malware that has successfully accessed classified American systems. Foreig intelligence agencies are constantly working to develop more advanced intrusion sets, at the same time the U.S. attempts to detect intrusions. It would be irresponsible to assume that U.S. networks are fully secure, and the U.S., and every other nation, will have to deal with that reality for the foreseeable future."*

-- Ashley Tanner, "Examining the Need for a Cyber Intelligence Discipline," *Journal of Homeland and National Security Perspectives* 1:1, 2014

Manipulation. The mixing of factual and fictitious or exaggerated evidence (one of the four deception means for conveying deception information to a target). (CIA, D&D Lexicon, 1 May 2002)

Maritime Domain. All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances. (NSPD-41/HSPD-13, Maritime Security Policy, 21 Dec 2004)

-- Also, the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. (JP 3-32, Command and Control for Joint Maritime Operations, 8 Aug 2006)

Marine Corps Intelligence Activity (MCIA). MCIA provides tailored intelligence and services to the Marine Corps, other services, and the IC based on expeditionary mission profiles in littoral areas. (DoD FCIP Strategy FY 2013-2017)

> For Marine Corps doctrine, tactics, techniques, and procedures on counterintelligence see Marine Corps Warfighting Publication (MCWP) 2-14, *Counterintelligence*, 5 Sep 2000.

Maskirovka. Soviet term -- a set of measures to deceive, or mislead, the enemy with respect to Soviet national security capabilities, actions, and intentions. These measures include concealment, simulation, diversionary actions and disinformation. The Soviet Union doctrine of *maskirovka* calls for the use of camouflage, concealment and deception (CC&D) in defense-related programs and in the conduct of military operations. (NSSD 108, 12 Oct 1983) Also see *deception*.

> *Maskirovka* is actually a very broad concept that encompasses many English terms. These include: camouflage, concealment, deception, imitation, disinformation, secrecy, security, feints, diversions, and simulation. While terms overlap to a great extent, a complication is that the Russian term is greater than the sum of these English terms. Thus, those in the West should attempt to grasp the entire concept rather than its components.
>
> *Maskirovka* is not a new concept in the USSR. Its roots can be traced to the Russian Imperial Army. Several Soviet authors trace it back to Dmitry Donskoy's placing a portion of his mounted forces in an adjacent forest at the Battle of Kulikovo Field in 1380. Seeing a smaller force than anticipated, the Tatars attacked, only to be suddenly overpowered by the concealed force.
>
> -- Charles Smith,"Soviet Maskirovko," *Airpower Journal*, Spring 1988
> Copy available at <http://www.airpower.au.af.mil/airchronicles/apj/apj88/spr88/smith.html>

MCC. See *Military Counterintelligence Collection*.

McCarthyism. The practice of making accusations of disloyalty, subversion, or treason without proper regard for evidence. (<http://en.wikipedia.org/wiki/McCarthyism>; accessed 29 Aug 2012)

> *The term has its origins in the period in the United States known as the Second Red Scare, lasting roughly from 1950 to 1954 and characterized by heightened fears of communist influence on American institutions and espionage by Soviet agents. Originally coined to criticize the anti-communist pursuits of Republican U.S. Senator Joseph McCarthy of Wisconsin, "McCarthyism" soon took on a broader meaning, describing the excesses of similar efforts. The term is also now used more generally to describe reckless, unsubstantiated accusations, as well as demagogic attacks on the character or patriotism of political adversaries.*
>
> -- Source: Wikipedia at <http://en.wikipedia.org/wiki/McCarthyism> (accessed 29 Aug 2012)

Meaconing. A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. (JP 1-02 and JP 3-13.1, Electronic Warfare, 25 Jan 2007)

Measurement and Signature Intelligence (MASINT). Information produced by quantitative and qualitative analysis of physical attributes of targets and events in order to characterize, and identify them. (ICD 1, Intelligence Community Leadership, 1 May 2006)

-- Also, technically derived intelligence data other than imagery and SIGINT. The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, information produced by quantitative and qualitative analysis of physical attributes of targets and events in order to characterize, locate, and identify them. MASINT exploits a variety of phenomenolgies to support signature development and analysis, to perform technical analysis, and to detect, characterize, locate, and identify targets and events. MASINT is derived from specialized, technically-derived measurements of physical phenomenon intrinsic to an object or event and it includes the use of quantitative signatures to interpret the data. (DoDI 5105.58, MASINT, 22 Apr 2009)

-- Also, information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify targets and events, and derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, describes a category of technically derived information that provides distinctive characteristics of a specific event such as a nuclear explosion, or locates, identifies, and describes distinctive characteristics of targets through such means as optical, acoustic, or seismic sensors. (WMD Report)

MASINT will become increasingly important in providing unique scientific or highly technical information contributions to the IC. It can provide specific weapon identifications, chemical compositions and material content, and a potential adversary's capability to employ weapons.

-- IC21: HPSCI Staff Study, 6 Apr 1996 (p. 40)

MASINT is scientific and technical intelligence information used to locate, identify, or describe distinctive characteristics of specific targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. For example, MASINT can identify distinctive radar signatures created by specific aircraft systems or the chemical composition of air and water samples.

The Central MASINT Organization, a component of the Defense Intelligence Agency, is the focus for all national and Department of Defense MASINT matters.

-- www.intelligence.gov (accessed 13 Aug 2012)

An excellent open source book on MASINT see: Robert M. Clark, *The Technical Collection of Intelligence*. Washington, DC: CQ Press, 2011.

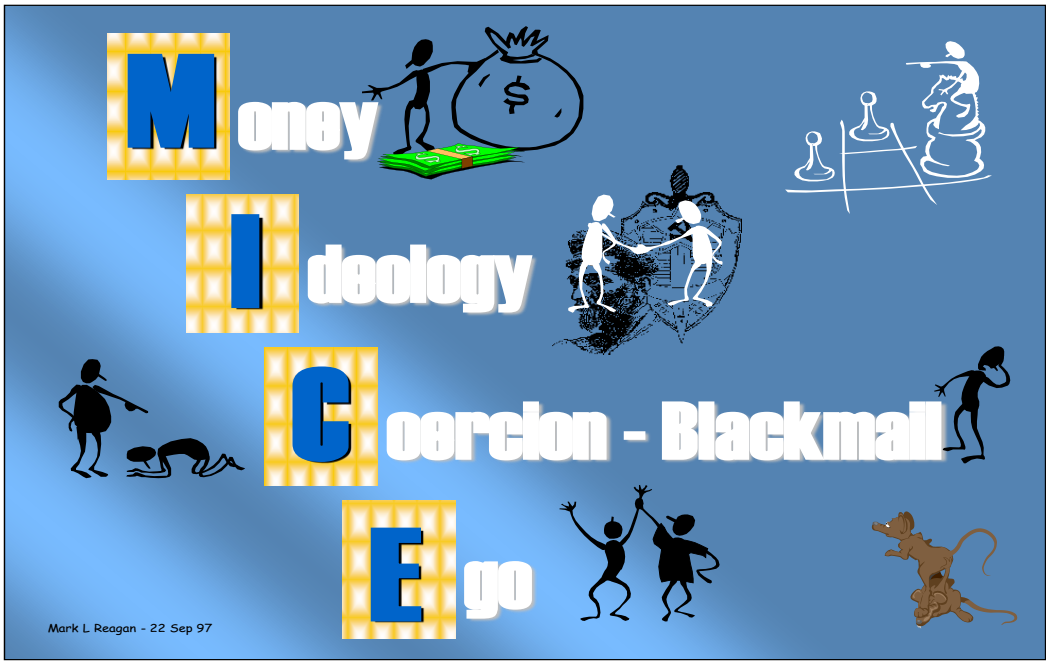
Measures of Effectiveness (MOE). A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Media Exploitation. The receipt, cataloging, duplication, screening/prioritizing, gisting, initial evaluation, translating key pieces of media, uploading data into appropriate data bases, identifying the need for further detailed exploitation of pieces of media, tracking the requested detailed exploitation efforts, and disseminating selected media for further use/analysis by the Intelligence Community. (National Media Exploitation Center CONOPS, Jan 2004)

MI5. British Security Service is responsible for "protecting the UK against threats to national security from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means." (www.mi5.gov.uk/)

MI6. British Secret Intelligence Service (SIS) is responsible for foreign intelligence. MI6 collects secret intelligence and mounts covert operations overseas in support of British Government objectives IAW the UK's Intelligence Services Act of 1994. (www.sis.gov.uk/)

MICE. The commonly used acronym to explain the motivation of traitors. MICE stands for "money, ideology, coercion, and ego," a combination of which may prompt an individual to betray his/her country. (*Historical Dictionary of Cold War Counterintelligence*, 2007) Also see *motivation.*



Motivations for espionage vary

If you add "revenge" to the list above, then the acronym is "CRIME"

"MALICE" is another acronym for **M**oney, **A**nger, **L**ust, **I**deology, **C**ompromise, and **E**go.

"*Spies, being human, often invent a better-sounding motive if their sole reason for betraying their country is money."*

-- General Frantisek Moravec, Former head of Czech Military Intelligence

Microdot. Photographic reduction of documents to three by six millimeters. (FBI FCI Terms) See *Mikrat.*

-- Also, the photographic reduction of writing or other material to facilitate transfer from one location to another without detection. (Spy Book)

-- Also, an optical reduction of a photographic negative to a size that is illegible without magnification, usually 1mm or smaller in area. (Spycraft)

Microdots are another method of surreptitious communication between an agent in the field and his controller. Photographs are reduced down to microscopic size, so that they are practically invisible to the naked eye. Microdots are generally concealed under stamps, on top of punctuation marks in typewritten letters, or under the lips of envelopes.

– Peter Wright, *Spycatcher* (1987), p. 119

Mikrat. Smaller than a microdot. (FBI FCI Terms) See *microdot.*

-- Also, the product of microphotography, as used in microdots. (Spy Book)

Military Agency Check (MAC). A records or files check conducted at any military agency with the AO [area of operations] of the field element conducting the check. (FM2.22-2, Counterintelligence, Oct 2009). Also see *local agency check; national agency check.*

Military Assistance Advisory Group (MAAG). A joint Service group, normally under the military command of a commander of a unified command and representing the Secretary of Defense, which primarily administers the US military assistance planning and programming in the host country. (JP 1-02 and JP 3-22, Foreign Internal Defense, 12 Jul 2010)

Militarily Critical Technology. See *critical technology; militarily critical technologies list; technology.*

Militarily Critical Technologies List (MCTL). A technical reference for the development and implementation of DoD technology security policies on international transfers of defense related goods, services, and technologies as administered by the Director, Defense Technology Security Administration (DTSA). (DoDI 3020.46, MCTL, 24 Oct 2008)

-- MCTL website at <http://www.dtic.mil/mctl/>
-- Also see <http://www.acq.osd.mil/rd/tech_security/mctp/mctl.html>
-- Also see <http://www.dhra.mil/perserec/csg/t1threat/mctl.htm>

Military Counterintelligence Collection (MCC). An CI collection activity using recruited or non-recruited sources to collect information responsive to operational, tactical, and strategic CI requirements, to include those of the Military Departments. (DoDI S-5240.17, CI Collection Activities, 14 Mar 2014) Also see *collection; counterintelligence collection*; *counterintelligence collection activities*.

Military Deception (MILDEC). Deception that is conducted to deliberately mislead adversary and potential adversary decision makers and commanders in order to cause the adversary to take specific actions or inactions that will contribute to the accomplishment of the friendly mission. [This definition is proposed for inclusion in the next edition of JP 1-02]. (DoDI S-3604.01, Department of Defense Military Deception, 11 Mar 2013) Also see *deception, deception in support of OPSEC*.

-- Also, actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

-- Also, those actions executed to deliberately mislead adversary decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (Army FM 3-0, Operations, with Chg 1, 2011)

In war-time, truth is so precious that she should always be attended by a bodyguard of lies
-- Winston Churchill (November 1943)
as cited in Anthony Cave Brown, *Bodyguard of Lies: The Extraordinary True Story Behind D-Day* (1975)

MILDEC is conducted to deliberately mislead adversary and potential adversary decision makers and commanders in order to cause the adversary to take specific actions or inactions that will contribute to accomplishment of the friendly mission.

MILDEC can mask, protect, reinforce, exaggerate, minimize, distort, or otherwise misrepresent U.S. technical and operational capabilities, intentions, operations, and associated activities.

According to JP 3-13.4, Counterintelligence provides the following for MILDEC planners:

1) Identification and analysis of adversary intelligence systems to determine the best deception conduits;
2) Establishment and control of deception conduits within the adversary intelligence system, also known as offensive CI operations;
3) Participation in counterdeception operations;
4) Identification and analysis of the adversary's intelligence system and its susceptibility to deception and surprise; and
5) Feedback regarding adversary intelligence system responses to deception operations.

For additional information see Joint Pub 3-13.4, *Military Deception*, 13 Jul 2006

It was Desert Storm that I became convinced of the power of deception in warfare, it truly is a force multiplier.

-- Tommy Franks (General, USA Ret), *American Solider* (2004)

Military Department (MILDEP). One of the departments within the Department of Defense created by the National Security Act of 1947, which are the Department of the Army, the Department of the Navy, and the Department of the Air Force. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Military Department Counterintelligence Organization (MDCO). Elements of the Military Departments authorized to conduct CI investigations, i.e., Army CI, Naval Criminal Investigative Service [NCIS], and the Air Force Office of Special Investigations [AFOSI]. (DoDD 5240.06, CIAR, 17 May 2011 w/ chg 1 and DoDI 5240.10, CI in the Combatant Commands and Other DoD Components, 5 Oct 2011 w/ chg 1)

MDCO, formerly known as "CI Lead Agencies," approved for inclusion in next edition of JP 1-02.

Military Information Support Operations (MISO). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 1-02 and JP 3-13.2, Psychological Operations, 7 Jan 2010)

Previously known as Psychological Operations or PSYOP; this change directed by SECDEF Memo, subject: Changing the Term Psychological Operations (PSYOP) to Military Information Support Operations (MISO), dated 3 Dec 2010. Also FY2012 National Defense Authorization Act (P.L.112-81) Section 1086, re-designates "psychological operations" as "military information support operations" in Title 10, United States Code, to conform to DoD usage.

Military Intelligence (MI). The collection, analysis, production, and dissemination of information relating to any foreign military or military-related situation or activity that is significant to military policy-making or the planning and conduct of military operations and activities. (DoDD 5143.01, USD/I, 23 Nov 2005)

Military intelligence appears in three basic forms: strategic, operational, and tactical.

-- **Strategic Intelligence**: intelligence that is required for the formulation of strategy, policy, and military plans and operations at the national and theater levels.

-- **Operational Intelligence**: intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. It focuses on narrower, but significant theater-oriented military responsibilities.

-- **Tactical Intelligence**: intelligence that is required for planning and conducting tactical military operations at the local level. It concerns information about the enemy that is designed to help locate the enemy and decide which tactics, units, and weapons will most likely contribute to victory in an assigned area, and when properly applied, it can be a significant force multiplier.

Military Intelligence Board (MIB). A decision-making forum which formulates Department of Defense intelligence policy and programming priorities. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Military Intelligence Program (MIP). The MIP consists of programs, projects, or activities that support the Secretary of Defense's intelligence, counterintelligence, and related intelligence responsibilities. This includes those intelligence and counterintelligence programs, projects, or activities that provide capabilities to meet warfighters' operational and tactical requirements more effectively. The term excludes capabilities associated with a weapons system whose primary mission is not intelligence. The term "MIP" replaces the terms "Joint Military Intelligence Program (JMIP)" and "Tactical Intelligence and Related Activities (TIARA)." (DoDD 5205.12, MIP, 14 Nov 2008)

> The Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Activities (TIARA) were combined in 2005 to form the MIP.
>
> *"The MIP was established to improve management of Defense Intelligence capabilities and resources. USD/I is the Program Executive for the MIP."*
>
> -- USD/I Memo, subj: Establishment of the MIP, 1 Sep 2005

Military Service. A branch of the Armed Forces of the United States, established by act of Congress, in which persons are appointed, enlisted, or inducted for military service, and which operates and is administered within a military or executive department. The Military Services are: the United States Army, the United States Navy, the United States Air Force, the United States Marine Corps, and the United States Coast Guard. (JP 1-02)

Military Source Operations. The collection, from, by and/or via humans, of foreign, military and military-related intelligence. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, DoD HUMINT collection and operations focused on foreign military and military-related intelligence conducted under the authorities of the Secretary of Defense. Military source operations are conducted by appropriately trained and certified personnel under the control of a Defense HUMINT Executor. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013, with chg 1 dated 13 Jun 2013)

-- Also, the collection from, by, and/or via humans, of foreign military and military-related intelligence conducted under SecDef authorities to satisfy DoD needs. (HDI Lexicon, April 2008)

-- Also, DoD HUMINT activity or operation which is conducted to specifically respond to, and satisfy, DoD intelligence collection requirements. These operations directly support the execution of the Secretary's responsibilities, commanders in the field, military operational planners, and the specialized requirements of the military departments (e.g., research and development process, the acquisition of military equipment, and training and doctrine) and span the entire HUMINT operational continuum, utilizing varying degrees of tradecraft to ensure the safety and security of the operation. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

> Military Source Operations are conducted by trained personnel under the control of Defense HUMINT Executors. See DoDD S-5200.37, *Management and Execution of Defense HUMINT (U),* 9 Feb 2009 for specifics.

Misdirection. A classic conjurer's trick, misdirection is the term applied in the counterintelligence community for the tactic of supplying an ostensibly plausible explanation for an event actually caused by something quite different, probably by an individual or an operation, deemed sufficiently valuable to require protection. Invariably a human asset may produce some information which requires action that could compromise him or her, so misdirection is intended to divert attention elsewhere. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Misperception. The formation of an incomplete or inaccurate image or perception of some aspect of reality. The faulty image may be formed due to a lack of information or intentionally erroneous information provided to the perceiver. (CIA, D&D Lexicon, 1 May 2002)

Mission. 1) The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore; 2) in common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Mission Assurance. A process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the execution of DoD mission-essential functions in any operating environment or condition. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the process or state of ensuring the survival of an organization's essential missions and operating capability when confronted by natural or man-made emergencies and disasters. (DoD Strategy for Operating in Cyberspace, May 2011)

Mission Critical Functions. Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed. (DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012)

Mission Manager. A position with the [Intelligence] Community for an individual, operating with the Director's [DNI] authorities, who coordinates all intelligence activities against a specific country or topic [e.g., counterterrorism counterproliferation, counterintelligence]. (HPSCI Report 27 Jul 2006)

-- Also, *Mission Managers* are the principal Intelligence Community officials overseeing all aspects of national intelligence related to their respective mission areas. Mission Managers are designated for counterintelligence, counterterrorism, Counterproliferation, Iran, North Korea, and Cuba & Venezuela. (ICD 900, Mission Management, 21 Dec 2006)

> The NCIX serves as the Mission Manger for Counterintelligence.
> The Director NCTC serves as the Mission Manager for Counterterrorism.

Mission Need. A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Mission needs are determined by the mission and functions of an IC element or the roles and responsibilities of particular IC personnel in the course of their official duties. (ICD 501, 21 Jan 2009)

Mission Statement. A short sentence or paragraph that describes the organization's essential task(s), purpose, and action containing the elements of who, what, when, where, and why. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *mission*.

Mission Tasking Authority (MTA). See *Counterintelligence Mission Tasking Authority*.

Mitigation. Actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. Includes solutions that contain or resolve risks through analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems. (DSS Glossary)

-- Also, capabilities necessary to reduce loss of life and property by lessening the impact of disasters. (PPD-8, 2011)

Modus Operandi (MO). A distinct pattern or method of procedure thought to be characteristic of or habitually followed by an individual or an organization involved in criminal or intelligence activity. (AR 381-20, Army CI Program, 25 May 2010)

> *Modus Operandi*--a Latin phrase--approximately translated as "method of operating." The term is used to describe someone's habits or manner of working, their method of operating or functioning. In English, it is frequently shortened to M.O.

Mole. A member of an organization who is spying and reporting on his/her own organization on behalf of a foreign country; also called a penetration. (National HUMINT Glossary) Also see *mole hunt*; *penetration.*

-- Also, a human penetration into an intelligence service or other highly sensitive organization. Quite often a mole is a defector who agrees to work in place. (CI Centre Glossary)

-- Also, literary and media term for penetration agent infiltrated into an opposition government agency. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

-- Also, the opposing faction's insert, or penetration, into an intelligence apparatus. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

> In 1622, Sir Francis Bacon used the term "mole" in the *History of the Reign of King Henry VII:*
>
> > *He was careful and liberal to obtain good Intelligence from all parts abroad…. As for his secret spials, which he did employ both at home and abroad, by them to discover what practices and conspiracies were against him, surely his care required it; he had such* ***moles*** [emphasis added] *perpetually working and casting to undermine him.* (p. 216)
>
> In modern times, the term was popularized by John le Carré (penname for David Cornwell, a British author of espionage novels) who used the term "mole" to mean a "penetration" of a adversary intelligence service. In le Carré's 1974 novel, *Tinker, Tailor, Soldier, Spy*, Smiley is recalled to hunt down a Soviet "mole" in the Circus (British Secret Intelligence Service, aka MI6).
>
> Also a title of a book by William Hood, *Mole: The True Story of the First Russian Spy to Become an American Counterspy* about Pyotr Semyonovich Popov, a Major in Soviet Military Intelligence (the GRU); see <http://en.wikipedia.org/wiki/Pyotr_Semyonovich_Popov>.
>
> Hood's book, *Mole*, is one of the best publicly available descriptions of a penetration of an intelligence service and provides a detailed and highly personal account of how intelligence tradecraft is practiced, the mental and psychological toll this takes, and the risks involved (for both agent and case officer).

Mole Hunt. The term popularized by John le Carré for a counterintelligence investigation conducted into hostile penetration. (*Historical Dictionary of Cold War Counterintelligence*, 2007) Also see *mole*.

-- Also, the search for moles in one's own service. (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd edition, 2012)

> Also the title of a book by David Wise, *Molehunt: The Secret Search for Traitors That Shattered the CIA* (1992).

Money Laundering. Generally refers to financial transactions in which criminals, including terrorist organizations, attempt to disguise the proceeds, sources or nature of their illicit activities. (US Department of Treasury)

Moscow Rules. The ultimate tradecraft methods for use in the most hostile of the operational environments. During the Cold War, Moscow was considered the most difficult of operating environments. (Spy Dust)

Once, an accident. Twice, a coincidence. Three times, an enemy action.

-- Ian Fleming, *Goldfinger* (1959)

Auric Goldfinger mentions this rule to James Bond in Goldfinger's warehouse in Geneva.

"Moscow rules" …the precepts we all understand for conducting our operations in the most difficult of operating environments: the Soviet capital. …They were dead simple, and all full of common sense:

-- Never make surveillance mad or embarrassed—they will shut you down.
-- Never look over your shoulder or steal free looks in store windows when on the street.
-- Make them think it was their fault that they had lost you, not vice versa, because KGB officers knew better than to report their own mistakes.

… a mantra that could guide them in determining whether they were the subject of hostile surveillance: Once, an accident. Twice, a coincidence. Three times, an enemy action.

-- Antonio and Jonna Mendez, *Spy Dust: Two Masters of Disguise Reveal the Tools and Operations that Helped Win the Cold War* (2002), p. 36

Motivation. The complex of reasoning and emotional or other drives that induces a person to accept employment or cooperate with an agency for a particular assignment. (AFOSI Instruction 71-101, 6 Jun 2000) Also see *"MICE."*

-- Also, broadly defined, is a feeling or state of mind that influences one's choices and actions. (PERSEREC Technical Report 05-10, May 2005)

-- Also, tradecraft jargon for bases for agent recruitment that are usually (1) ideological; (2) financial; (3) coercion or blackmail; (4) sexual; (5) ego satisfaction; (6) familial; (7) love of adventure or excitement; (8) a combination of two or more of the preceding. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Motivation for espionage results from a complex interaction between personality characteristics and situational factors

-- PERSEREC Technical Report 05-10, May 2005 (p.1)

Psychological portraits of the major spies show complex motivations, which often include dissatisfaction with the job. …The profile of a traitor may not be significantly different from that of many sociopaths or felons. …Spies also usually have two other characteristics: They relish the secret world of intrigue and they enjoy the chance to show others as fools. …The typical spy enjoys deception and may have a personality bordering on, or well into, the psychotic.

-- Thomas B. Allen and Norman Polmar, *Merchants of Treason: America's Secrets for Sale* (1988), pp.51-52

Espionage Motivations

Motives by which spies are driven are highly individualized—simple motives often conceal deeper and more complicated motivations. Motivation for espionage is often elusive and frequently involves multiple reasons. According to a 2008 PERSEREC study, assigning the motivation for committing espionage is often most accurate when motivation is inferred from evidence available while the crime was being committed, rather than from the self justifications after the fact. Like most criminals, once caught, spies see their own past intentions and the pressures that may have affected their behavior in a changed light. Motives for espionage can also change over the course of espionage activities.

MONEY: Historically a leading motivation -- the primacy of money as a motive is a common observation in studies of espionage. Money (financial gain) also appears frequently in combination with other motives. Americans most consistently have cited money as the dominant motive for espionage, especially in the 1980s—*the decade of the spy*. This motivation reflects a person's need for money (e.g., indebtedness, financial pressures), or simple greed, or some combination thereof. Often seen in people who see themselves as underpaid (whether real or perceived). Many

cases involved indebtedness. Being in debt or having a history of insolvency, bankruptcy, or late payments is a major component of the financial considerations scrutinized in a personnel security investigation for a security clearance. Among the typical financial motives of debt or greed, debt continues to motivate espionage more than just greed. Although no recent cases, several past spies were frequent gamblers. Money remains one of multiple motives in many recent cases.

> *"Spies, being human, often invent a better-sounding motive if their sole reason for betraying their country is money."*
> -- General Frantisel Moravec, Former Head of Czech Military Intelligence

IDEOLOGY/DIVIDED LOYALTIES: This motivation encompasses both ideological driven motives (commitment to a competing political or economic system, e.g. Communism or Jihadism) and/or those with competing allegiances (i.e., intellectual or emotional commitments to another country through birth, family ties or cultural affinity). Ideology was the dominant motive in the 1940s, whereas divided loyalties has increased over time of all motives for espionage. Divided loyalties—holding and acting on an allegiance to a foreign country or cause in addition to or in preference to allegiance to the United States—has dramatically increased since 1990. PERSEREC studies indicate that spying prompted by divided loyalties has become the most common motive for American espionage, replacing spying for money as the primary motive. Additionally this trend has been accelerating since 2000.

COMPROMISE/COERCION: Being forced to commit espionage through blackmail or threat to relatives in a foreign country. Used to recruit spies most often in the early period before 1980, when foreign intelligence services engaged in occasional blackmail using relatives overseas, or entrapped Americans in sexual blackmail scams. Has not been seen in recent cases.

EGO/THRILLS: Some spies commit espionage for thrills or to make themselves feel important—ego-boosting. Some have a fascination with spying and find espionage a thrilling enterprise that allows them to enact fantasies of secret lives and heroic deeds they have read about in popular spy novels. Includes the related ego-boost of getting away with it, as well as the thrill of successfully maintaining a secret life parallel to the spy's professional career, and thereby cleverly demonstrating that his competence surpasses his colleagues. Although rarely the primary motive, there have been several cases involving individuals who spied for the thrill of getting away with espionage, or from their need to stroke their egos.

DISGRUNTLEMENT/REVENGE: In recent cases, disgruntlement was the second most common cause. This motive takes many different forms: disenhancement, extreme unhappiness with people and employment, disaffection, bitterness, frustration, anger, disillusionment, and alienation. Usually directly related to employment/work-related issues caused by the person's relationships or treatment in the workplace, and associated desire to take revenge. Disappointment, anger, frustration, or alienation can arise from interactions among coworkers or between employees and supervisors. Feelings of disgruntlement often lead to efforts to get revenge and espionage is one way to get bak at the offending individual, organization, or at the whole government they represent. A common motivation among those who volunteer.

INGRATIATION: The desire to help or please someone else motive some to commit espionage. Most often through an emotional, personal relationship or attachment. This motivation can also manifest when trying to impress a potential future employer. Most spies who committed espionage to please others tended to be successful.

RECOGITION: Usually a secondary motive of spies seeking recognition, approval and/or attention from those to whom they provided information. Individuals often feel overworked and underappreciated and espionage allows them to connect or bond with an agent handler and seek the approval and attention of the handler.

For more information, see following Defense Personnel Security Research Center (PERSEREC) Reports:

-- *Americans Who Spied Against Their Country Since World War II*, Rpt PERS-TR-92-005, May 1992
-- *Espionage Against the United States by American Citizens 1947-2001*, Rpt 02-5, Jul 2002
-- *Changes in Espionage by Americans: 1947-2007*, Tech Rpt 08-05, Mar 2008
-- *Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008*, 2 Nov 2009

MTAC. See *Multiple Threat Alert Center.*

Multiple Threat Alert Center (MTAC). Department of Navy's fusion, analysis and dissemination center for terrorist, criminal, counterintelligence and security information; operated by the Naval Criminal Investigative Service (NCIS).

> *The terrorist attack on the World Trade Center in New York and the Pentagon in Washington, DC on September 11, 2001 led NCIS to transform the Antiterrorist Alert Center (ATAC) into the MTAC in 2002.*
>
> -- NCIS <http://www.ncis.navy.mil/AboutNCIS/History/Pages/default.aspx>

Multilateral Collection. A collection activity conducted with two or more cooperating foreign intelligence services against a mutually targeted foreign intelligence, security service, or international terrorist entity. (Previously in DoDI S-5240.17, CI Collection, 12 Jan 2009) Also see *bilateral.*

> Multilateral: activities conducted with more than one nation.

Multilateral OFCO. An OFCO [Offensive Counterintelligence Operation] conducted by a U.S. CI agency with two or more cooperating foreign intelligence services against a mutually targeted FISS, foreign entity, or terrorist element. (DoDI S-5240.09, 29 Oct 2008)

Multilevel Security (MLS). Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Multinational. Between two or more forces or agencies of two or more nations or coalition partners. Also see also *alliance; coalition*. (JP 1-02)

Multinational Force (MNF). A force composed of military elements of nations who have formed an alliance or coalition for some specific purpose. (JP 1-02) Also see multinational operations.

Multinational Operations. A collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance. (JP 1-02 and JP 3-16, Multinational Operations, 7 Mar 2007) Also see *alliance; coalition; coalition action.*

Multispectral Imagery (MSI). The image of an object obtained simultaneously in a number of discrete spectral bands.(JP 1-02 and JP 3-14, Space Operations, 6 Jan 2009)

N ==========

Narcoterrorism. Terrorism that is linked to illicit drug trafficking. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

Name Trace. A search of available recorded data to find information about a person, normally conducted to determine the presence or absence of derogatory information about the person, as a first step in judging his suitability or intelligence value. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a search of data for information about an individual, organization, or subject. (National HUMINT Glossary)

National Agency Check (NAC). An in-depth name trace consisting of Federal Bureau of Investigation Name and Criminal History Fingerprint Checks, Defense Clearance Investigation Index (DCII) search, and can include checks on military personnel records, citizenship, selective service, Central Intelligence Agency records, State Department records, and other US Government agencies. Also see *local agency check; military agency check.*

-- Also, [part of a] personnel security investigation consisting of a review of: investigative and criminal history files of the Federal Bureau of Investigation, including a technical fingerprint check; Office of Personnel Management Security/Suitability Investigations Index; DoD Central Index of Investigations (DCII) and Joint Personnel Adjudication System (JPAS); and such other national agencies (e.g., CIA, DNI) as appropriate to the individual's background. (IC Standard 700-1, 4 Apr 2008)

-- Also, formal request to federal agencies for searches of their records and supporting databases and files for information of investigative [/CI] interest. (FM 2-22.2, Counterintelligence, Oct 2009 and 902d MI Group Investigations Handbook, Jun 2012)

-- Also, an integral part of all background investigations, the NAC consists of searches of OPM's Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the FBI Identification Division's name and fingerprint files, and other files or indices when necessary. (Army – see below)

> National Agency Check and Inquiries (NACI) - This is the basic and minimum investigation required on all new Federal employees. It consists of a NAC with written inquiries and searches of records covering specific areas of a person's background during the past five years. Those inquiries are sent to current and past employers, schools attended, references, and local law enforcement authorities.
>
> Access NACI (ANACI) - This is a new investigation designed as the required initial investigation for Federal employees who will need access to classified national security information at the Confidential or Secret level. The ANACI includes NACI and Credit coverage with additional local law enforcement agency checks.
>
> NAC with Local Agency Check and Credit (NACLC) - This is a new investigation which is the same as the ANACI without the written inquiries to past employers, schools attended, etc. It is designed as the initial investigation for contractors at the Confidential and Secret national security access levels. The NACLC also is to be used to meet the reinvestigation requirement for all individuals (including contractors) who have Confidential or Secret clearances.
>
> -- US Army at: <http://www.dami.army.pentagon.mil/site/PerSec/InvTypes.aspx> (accesses 24 Sep 2013)

National Capital Region (NCR). A geographic area encompassing the District of Columbia and eleven local jurisdictions in the State of Maryland and the Commonwealth of Virginia. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

National Center for Credibility Assessment (NCCA). A federally funded institution providing graduate and continuing education courses in psychophysiological detection of deception (PDD). (www.ncca.mil/mission.htm)

-- Also, an interagency training institute that provides polygraph education and training, conducts credibility assessment research and development, and manages the Polygraph Quality Assurance Program. (DoD FCIP Strategy FY 2013-2017)

For DoD policy see DoDD 5210.48, Polygraph and Credibility Assessment Program. NCCA is under the operational control of the Defense Counterintelligence and Human Intelligence Center (DCHC), DIA. It was previous known as the Defense Academy for Credibility Assessment (DACA) and before that as the DoD Polygraph Institute (DoDPI).

National Clandestine Service (NCS). The NCS operates as the clandestine arm of the CIA, and serves as the national authority for the coordination, deconfliction, and evaluation of clandestine human intelligence operations across the Intelligence Community. The NCS supports our country's security and foreign policy interests by conducting clandestine activities to collect information that is not obtainable through other means. The NCS also conducts counterintelligence and special activities as authorized by the President. (CIA at <https://www.cia.gov/offices-of-cia/clandestine-service/index.html>)

-- Also, the NCS serves as the national authority for the integration, coordination, deconfliction, and evaluation of human intelligence operations across the entire Intelligence Community, under authorities delegated to the Director of the CIA who serves as the National HUMINT Manager. The Director of the NCS reports directly to the Director of the CIA and will work with the Office of the Director of National Intelligence to implement all of the DNI's statutory authorities. (ODNI News release 3-05, 13 Oct 2005) Also see *Defense Clandestine Service*.

Formerly known as CIA Directorate of Operations or DO (in 2005, the DO transitioned to the NCS). The NCS was established in response to recommendations made in March 2005 by the President's Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

Collecting foreign intelligence — finding someone who has protected information and convincing that person to share it — is the "bread and butter" of what the clandestine service does, although "if we succeed, we'd rather not talk about it."

-- Thomas Twetten, Former Chief of CIA Clandestine Operations, 27 Jan 2011

Clandestine Service…

A clandestine service does much more than simply collect "HUMINT" clandestinely, that is secretly exploit agents for the purpose of collecting intelligence. A clandestine service also works in liaison with other spy services to run all types of operations; it taps telephones and installs listening devices; it breaks into or otherwise gains access to the contents of secured facilities, safes, and computers; it steals, compromises, and influences foreign cryptographic capabilities so as to make them exploitable by US SIGINT; it protects its operations and defends the government from other intelligence services by engaging in a variety of counterespionage activities, including the aggressive use of double agents and penetrations of foreign services; and it clandestinely emplaces and services secret SIGINT and MASINT sensors. It also has the capability of using its techniques and access to run programs at the President's direction to influence foreign governments and developments, that is, "covert action." The unifying aspect of these activities is not some connection to HUMINT; rather, they are highly diverse but interdependent activities that are best conducted by a clandestine service.

-- *IC 21: Intelligence Community in the 21st Century*, Chap. IX – Clandestine Service; available on line at: <http://www.gpo.gov/fdsys/pkg/GPO-IC21/html/GPO-IC21-9.html>

National Counterintelligence Executive (NCIX). Performs duties provided in the CI Enhancement Act of 2002 and such other duties as may be prescribed by the Director of National Intelligence or specified by law. NCIX serves as Mission Manager of Counterintelligence and the Chairperson of the National CI Policy Board. Resides within the Office of the Director of National Intelligence (ODNI). (CI Enhancement Act of 2002) Also see *Office of the National Counterintelligence Executive*.

-- Also, the NCIX serves as the head of national counterintelligence for the U.S. Government, per the CI Enhancement Act of 2002. (National Intelligence: A Consumer's Guide - 2009)

Additional information on NCIX at <http://www.ncix.gov/about/index.html>

National Counterintelligence Policy Board (NACIPB). Special board established by statue within the executive branch of Government; reports to the President through the National Security Council. The Board serves as the principal mechanism for developing policies and procedures for the approval of the President to govern the conduct of counterintelligence activities; and upon the direction of the President, resolving conflicts that arise between elements of the Government conducting such activities. The Board also acts as an interagency working group to ensure the discussion and review of matters relating to the implementation of the Counterintelligence Enhancement Act of 2002 and provides advice to the National Counterintelligence Executive on priorities in the implementation of the *National Counterintelligence Strategy*. (Extracted from 50 U.S.C. §402a)

NACIPB is chaired by the National Counterintelligence Executive and consists of senior USG personnel appointed by the head of the department or element concerned, as follows: Department of Justice, including the Federal Bureau of Investigation (FBI); Department of Defense, including the Joint Chiefs of Staff; Central Intelligence Agency (CIA); Department of State; Department of Energy; and any other department, agency, or element of the US Government specified by the President.

National Counterproliferation Center (NCPC). Coordinates strategic planning within the Intelligence Community (IC) to enhance intelligence support to United States efforts to stem the proliferation of weapons of mass destruction and related delivery systems. It works with the IC to identify critical intelligence gaps or shortfalls in collection, analysis or exploitation, and develop solutions to ameliorate or close these gaps. It also works with the IC to identify long-term proliferation threats and requirements and develop strategies to ensure the IC is positioned to address these threats and issues. NCPC will reach out to elements both inside the IC and outside the IC and the U.S. Government to identify new methods or technologies that can enhance the capabilities of the IC to detect and defeat future proliferation threats. (ODNI News release 9-05, 21 Dec 2005)

-- Also, the NCPC, which resides in the ODNI, is the bridge from the IC to the policy community for activities within the U.S. Government associated with countering the proliferation of weapons of mass destruction (WMD). (National Intelligence: A Consumer's Guide - 2009)

National Counterterrorism Center (NCTC). The primary center for US government analysis of terrorism. It falls under the Office of the Director of National Intelligence (ODNI). One of its primary missions is "to serve as the central and shared knowledge bank on known and suspected terrorists and international terrorist groups, as well as their goals, strategies, capabilities, and networks of contacts and support." (EO 13354, National Counterterrorism Center, 27 Aug 2004)

In August 2004, the President established the NCTC to serve as the primary USG organization for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism and to conduct strategic operational planning by integrating all instruments of national power. In December 2004, Congress codified the NCTC in the Intelligence Reform and Terrorism Prevention Act (IRTPA) and placed the NCTC in the Office of the Director of National Intelligence (ODNI). NCTC is a multi-agency organization dedicated to eliminating the terrorist threat to US interests at home and abroad.

-- NCTC website: <http://www.nctc.gov/about_us/about_nctc.html >

NCTC was established in 2004 to ensure that information from any source about potential terrorist acts against the U.S. could be made available to analysts and that appropriate responses could be planned. Investigations of the 9/11 attacks had demonstrated that information possessed by different agencies had not been shared and thus that disparate indications of the looming threat had not been connected and warning had not been provided.

NCTC prepares studies ranging from strategic assessments of potential terrorist threats to daily briefings and situation reports. It is also responsible, directly to the President, for planning (but not directing) counterterrorism efforts. The NCTC received a statutory charter in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458); it currently operates with a staff of more than 500 personnel from its headquarters in northern Virginia.

-- Congressional Research Service (CRS) Report R41022, 19 Dec 2011

National Crime Information Center (NCIC). A computerized system of crime records and data, maintained by the Federal Bureau of Investigation, that can be tapped into by virtually every criminal justice agency nationwide. (Cyber Threats to National Security, Symposium Five, 2011)

See <http://www.fbi.gov/about-us/cjis/ncic/ncic >

National Critical Infrastructure and Key Assets (NCI & KA). *Within DoD: None – term removed from JP 1-02.*

Previously defined in JP 3-28, Civil Support (14 Sep 2007) as: The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. They include telecommunications, electrical power systems, gas and oil distribution and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations.

National Critical Systems and Technology Joint Task Force (NCST-JTF). A collaborative forum to lead USIC and federal agency counterintelligence efforts for the protection of critical technologies. (NCST-JTF tri-fold, undated, circa 2012)

NCST-JTF Mission

Leverage the collective CI resources of the Task Force member agencies to prevent, preempt, deter, and investigate attempts to acquire, proliferate and transfer critical US technologies to foreign powers.

Apprehend and prosecute individuals who may commit or plan such acts negatively affecting U.S. National Security interest.

National Cyber Investigate Joint Task Force (NCIJTF). The focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations. The FBI is responsible for developing and supporting the joint task force, which includes 19 intelligence agencies and law enforcement, working side by side to identify key players and schemes. Its goal is to predict and prevent what's on the horizon and to pursue the enterprises behind cyber attacks. (www.fbi.gov; accessed 18 Jun 2013)

On 8 January 2008, the President signed Presidential Directive NSPD-54/HSPD-23 which mandated the National Cyber Investigative Joint Task Force to be the focal point for all government agencies and to coordinate, integrate, and share information related to all domestic cyber threat investigations.

NCIJTF Mission: Ensure the U.S. Government is coordinating all its efforts to address national security cyber intrusions, including intelligence operations and investigations. The NCITF's functions are structured in three groups: the Information Operations Group, the Analysis Group, and the Law Enforcement Group.

For more information on the NCIJTF see <http://www.fbi.gov/about-us/investigate/cyber/ncijtf>

National Cyber Investigative Joint Task Force - Analytical Group (NCIJTF-AG)

The Defense Cyber Crime Center (DC3) resources and manages the Analytic Group of the NCIJTF, which operates under overall FBI stewardship, joined by other national LE/CI organizations. Focused on nation-state threat actors, AG leads a collaborative analytical and technical exchange with subject matter experts from LE/CI, CND, IC, and IA agencies to build a threat picture to enable proactive LE/CI cyber operations.

National Defense Strategy (NDS). A document approved by the Secretary of Defense for applying the Armed Forces of the United States in coordination with Department of Defense agencies and other instruments of national power to achieve national security strategy objectives. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

National Detainee Reporting Center (NDRC). National-level center that obtains and stores information concerning enemy prisoners of war, civilian internees, and retained personnel and their confiscated personal property. May be established upon the outbreak of an armed conflict or when persons are captured or detained by U.S. military forces in the course of the full range of military operations. Accounts for all persons who pass through the care, custody, and control of the U.S. Department of Defense. (JP 1-02 and JP 3-63, Detainee Operations, 30 May 2008)

National Disclosure Policy (NDP-1). A document that promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance required by U.S. departments and agencies having occasion to disclose classified information to foreign governments and international organizations. NDP-1 establishes and provides for management of interagency mechanisms and procedures required for effective implementation of the national policy.

National Disclosure Policy Committee. Central authority for formulation, promulgation, administration, and monitoring of the NDP-1.

National Emergency. A condition declared by the President or the Congress by virtue of powers previously vested in them that authorize certain emergency actions to be undertaken in the national interest. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

National Essential Functions. That subset of Government functions that are necessary to lead and sustain the Nation during a catastrophic emergency. (PDD-21, 12 Feb 2013)

National Foreign Intelligence Program. All programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of Central Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by US Armed Forces. (50 USC §401a)

National Geospatial-Intelligence Agency (NGA). A member of the US Intelligence Community, as well as a Combat Support Agency of the Department of Defense, that provides timely, relevant and accurate geospatial intelligence in support of national security objectives.

The term “geospatial intelligence” or “GEOINT” means the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence and geospatial (e.g., mapping, charting and geodesy) information.

-- See NGA website at <https://www1.nga.mil/>

The National Imagery and Mapping Agency (NIMA) transitioned to the National Geospatial-Intelligence Agency (NGA) in 2003. NIMA established its internal CI element on 1 April 2002. See the official history of the NGA and predecessors, *Advent of the National Geospatial-Intelligence Agency*, September 2011, by the Office of the NGA Historian, available at <www.nga1.mil>

National HUMINT Collection Directive (NHCD). A set of national-level strategic collection requirements for a particular country, geographic area, or transnational issue, prepared by the NHRTC in coordination with IC and other organizations. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

-- Also, an integrated inter-agency mechanism for tasking human intelligence requirements to members of the Intelligence Community that have the best capability and probability of acquiring that information at the least cost and least risk. A standing / enduring intelligence requirement. (National HUMINT Glossary)

National HUMINT Requirements Tasking Center (NHRTC). Congressionally mandated to integrate all HUMINT collection and reporting capabilities within the US Government. [Staffed by] senior officers from the Department of State, Department of Defense, and CIA; the center produces National HUMINT Collection Directives (NHCDs) and Collection Support Briefs (CSBs). (National HUMINT Glossary)

> The NHRTC reports to the National HUMINT Manager. See DCID 3/7, *National HUMINT Requirements Center (U)*, 1 Jun 1992 (classified CONFIDENTIAL).

National Industrial Security Program (NISP). National program established by EO 12829 for the protection of information classified under EO 12958 as amended, or its successor or predecessor orders, and the Atomic Energy Act of 1954, as amended. The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense is the Executive Agent for the NISP. The Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies. (DoD 5220.22-M, NISPOM, 28 Feb 2006) Also see the *Defense Security Service (DSS); industrial security.*

> The Defense Security Service (DSS) is designated as the DoD Cognizant Security Office (CSO) for cleared contractors within the NISP.
>
> For additional information see Information Security Oversight Office (ISSO) website at: <http://www.archives.gov/isoo/policy-documents/>

National Infrastructure Coordinating Center. The national physical critical infrastructure center, as designated by the Secretary of Homeland Security, which coordinates a national network dedicated to the security and resilience of critical infrastructure of the United States by providing 24/7 situational awareness through information sharing, and fostering a unity of effort. (www.dhs.gov)

National Infrastructure Protection Center (NIPC). The FBI's NIPC is charged with detecting, preventing and responding to cyber and physical attacks on US critical infrastructure and overseeing computer crime investigation conducted by FBI field offices.

National Infrastructure Protection Plan (NIPP). A plan developed by the Department of Homeland Security [DHS] to provide the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation's critical infrastructure and key resources into a single national program. (Cyber Threats to National Security, Symposium Five, 2011)

> See <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>
>
> Copy of the NIPP 2013 also available at: <https://www.hsdl.org/?view&did=747827>

National Infrastructure Sector. One of the 18 national CI/KR [critical infrastructure and/or key resource] sectors identified in Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," 17 December 2003. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

National Insider Threat Task Force (NITTF). National Task Force focused on Insider Threat issues under joint leadership of the Attorney General and the Director of National Intelligence; established IAW EO 13587, October 2011 The NCIX and FBI co-direct the daily activities of the NITTF.

> *The NITTF assists federal agencies develop insider threat programs to help prevent, deter, and detect compromises of classified information by malicious insiders. Its goals is to prevent classified information from getting into the hands of people who can harm the national security of our country.*
> -- NITTF Fact Sheet, subj: NITTF External Communications Guidance, undated

National Insider Threat Working Group (NISTWG). Interagency, cross-discipline working group established by the National Counterintelligence Policy Board to focus exclusively on insider threat issues.

National Intelligence. All intelligence, regardless of the source from which derived and including information gathered within or outside of the United States, which pertains, as determined consistent with any guidelines issued by the President, to the interests of more than one department or agency of the Government; and that involves (a) threats to the United States, its people, property, or interests; (b) the development, proliferation, or use of weapons of mass destruction; or (c) any other matter bearing on United States national or homeland security. (Intelligence Reform and Terrorism Prevention Act of 2004, §1012; also JP 1-02 and JP 2-01, Joint & National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, intelligence which pertains to the interest of more than one department or agency of the US Government. (50 USC §401a)

> The US Government uses intelligence to improve and understand the consequences of its national security decisions.

National Intelligence Board. Serves as the senior Intelligence Community advisory body to the Director of National Intelligence (DNI) on the analytic judgments and issues related to analysis of national intelligence; functions include: production, review, and coordination of national intelligence; interagency exchanges of national intelligence information; sharing of IC intelligence products with foreign governments; protection of intelligence sources and methods; activities of common concern and other matters as may be referred to it by the DNI. (ICD 202, National Intelligence Board, 16 Jul 2007)

National Intelligence Council (NIC). The Intelligence Community's center for mid-term and long-term strategic thinking. Its primary functions are to: 1) Support the DNI in his role as head of the Intelligence Community; 2) Provide a focal point for policymakers to task the Intelligence Community to answer their questions; 3) Reach out to nongovernmental experts in academia and the private sector to broaden the Intelligence Community's perspective; 4) Contribute to the Intelligence Community's effort to allocate its resources in response to policymakers' changing needs; and 5) Lead the Intelligence Community's effort to produce National Intelligence Estimates (NIEs) and other NIC products. (ODNI website)

> The NIC is responsible for the US Intelligence Community's most authoritative assessments of major issues affecting the national security. By law [50 USC §403-3b(b)(1)], the NIC is to consist of "senior analysts within the intelligence community and substantive experts from the public and private sector, who shall be appointed by, report to, and serve at the pleasure" of the DNI. The senior analysts are known as National Intelligence Officers (NIOs).
>
> NIC responsibilities are set forth in ICD 207, *National Intelligence Council*, 9 June 2008.

National Intelligence Coordination Center (NIC-C). Provides a mechanism to strategically manage and direct collection across defense, foreign and domestic realms. [Interfaces with the Defense Intelligence Coordination Center (DIOCC]. (National Intelligence: A Consumer's Guide - 2009)

National Intelligence Estimate (NIE). The DNI's most authoritative written judgment concerning national security issues. NIEs contain the coordinated judgments of the Intelligence Community regarding the likely course of future events. (ODNI website)

-- Also, a strategic estimate of the capabilities, vulnerabilities, and probable courses of action of foreign nations produced at the national level as a composite of the views of the intelligence community. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

National Intelligence Priorities Framework (NIPF). The Director of National Intelligence's guidance to the IC on the national intelligence priorities approved by the President. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, the DNI's sole mechanism for establishing national intelligence priorities. The NIPF consists of: intelligence topics approved by the President; a process for assigning priorities to countries and non-state actors relevant to the approved intelligence topics; and a matrix showing those priorities. It is updated semi-annually. The NIPF is used by the ODNI and IC elements in allocating collection and analytical resources. (ICD 204, 13 Sep 2007)

> *A key instrument for keeping the IC attentive to both policymaker concerns and potential shocks… The NIPF process gathers the needs of senior decision makers across the US government on a semi-annual basis to support prudent allocation of both collection and analytical resources for the following 6-to-12 months.*
>
> – DNI 2006 Annual Report of the US Intelligence Community (Feb 2007)

National Intelligence Program (NIP). All programs, projects, and activities of the IC, as well as any other programs of the IC designated jointly by the DNI and the head of a US department or agency or by the President. It does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by US Armed Forces. (National Security Act §3(6) and ICD 1, 1 May 2006)

> Formerly known as the National Foreign Intelligence Program (NFIP), the NIP provides the resources needed to develop and maintain intelligence capabilities that support national priorities. The DoD Foreign Counterintelligence Program or FCIP is part of the NIP.
>
> ———————————
>
> The Federal Budget (FY 2012) disclosed for the first time the aggregate funding for NIP – $55 billion in 2012. However, detailed funding requests for intelligence activities remain classified. See White House Factsheet at: <http://www.whitehouse.gov/omb/factsheet_department_intelligence>

National Intelligence Strategy. A strategy document prepared by the ODNI in consultation with the relevant departments that establishes the strategic objectives for the Intelligence Community (IC); it sets forth the framework for a more unified, coordinated and effective IC [and] guides IC policy, planning, collection, analysis, operations, programming, acquisition, budgeting, and execution. (ODNI News release 4-05)

> The National Intelligence Strategy (NIS) sets forth the framework for a more unified, coordinated, and effective US Intelligence Community (IC) and guides IC policy, planning, collection, analysis, operations, programming, acquisition, budgeting, and execution. The strategy outlines strategic objectives that are referred to as either mission or enterprise objectives. The unclassified *National Intelligence Strategy* (Aug 2009) is available at <http://www.dni.gov/reports/2009_NIS.pdf>
>
> CI is one of six mission objectives of the NIS (Mission Objective 4 is *Integrate Counterintelligence*). This is the first time that CI was identified as a mission objective within the NIS; see NIS pp 8-9.

National Intelligence Support Plan (NISP). The NISP, in conjunction with the Combatant Command's Annex B: [Intelligence Plan or IPLAN] supports COCOM operational plans directed by the President and the Secretary of Defense. The NISP defines the national Intelligence Community (IC) agencies' and related organizations' intelligence collection, and analysis & production support roles and responsibilities within the COCOM area of responsibility and the national IC to ensure integrated intelligence operations, synchronized with the COCOM operational plan. The NISP supports the COCOM's operational objectives during all phases of the operation and contributes to the achievement of the COCOM's desired operational effects. (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007) Also see *Counterintelligence Functional Support Plan (CI FSP).*

National Joint Terrorism Task Force (NJTTF). The NJTTF was established in July 2002 to serve as a coordinating mechanism with the FBI's partners on terrorism issues. Over 40 agencies are represented in the NJTTF, which has become a focal point for information sharing and the management of large-scale projects that involve multiple partners. Also see *Joint Terrorism Task Force (JTTF)*. (DoJ website: <http://www.usdoj.gov/jttf/>)

-- Also, the NJTTF was created to act as a liaison and conduit for information on threats and leads from FBI Headquarters to the local JTTFs and to 40 participating agencies including representatives from members of the Intelligence Community; components of the departments of Homeland Security, Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and Interior; NYPD; Nuclear Regulatory Commission; Railroad Police; U.S. Capitol Police; and others. (FBI)

See FBI web site at: <http://www.fbi.gov/news/stories/2008/august/njttf_081908>

National Media Exploitation Center (NMEC). A Director of National Intelligence (DNI) Center composed of DIA, CIA, FBI, NSA, and Defense Cyber Crime Center (DCCC) as partner organizations; DIA is the Executive Agent. NMEC acts as a DOMEX [document and media exploitation] service of common concern and ensures prompt and responsive DOMEX support to meet the needs of intelligence, defense, homeland security, law enforcement, and other US Government Consumer's, to include provision of timely and accurate collection, processing, exploitation, and dissemination consistent with the protection of intelligence sources and methods. (ICD 302, Document and Media Exploitation, 6 Jul 2007)

Director DIA is the IC Executive Agent for the NMEC (para 2d, DoDD 3300.03).

National Military Strategy (NMS). A document approved by the Chairman of the Joint Chiefs of Staff for distributing and applying military power to attain national security strategy and national defense strategy objectives. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013) Also see *national security strategy*.

The NMS defines the national military objectives, establishes the strategy to accomplish these objectives, and addresses the military capabilities required to execute the strategy. The Chairman develops the NMS by deriving overall security policy guidance from the President's NSS, and through consulting with the other JCS members and combatant commanders. The NMS describes the strategic landscape and includes a discussion of the potential threats and risks.

-- CJCSI 3100.01A, *Joint Strategic Planning System*, 1 Sep 1999

National Policy. A broad course of action or statements of guidance adopted by the government at the national level in pursuit of national objectives. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

National Reconnaissance Office (NRO). Responsible for integrating unique and innovative space-based reconnaissance technologies, and the engineering development, acquisition, and operation of space reconnaissance systems and related intelligence activities. (JP 2-0, Joint Intelligence, 22 Oct 2013)

The NRO is responsible for research and development (R&D), acquisition, launch, deployment, and operation of overhead reconnaissance systems, and related data-processing facilities to collect

intelligence and information to support national and DoD missions and other United States Government (USG) needs (DoD Directive 5105.23, NRO, 28 June 2011).

The NRO designs, builds and operates the nation's reconnaissance satellites. According to the NRO, their satellites provide constant global access to critical information otherwise unavailable to the President, his cabinet, other national leaders and numerous customers in the Defense and Intelligence communities. These satellites provide services in three broad categories: GEOINT, SIGINT, and Communications.

In recent years, the NRO has implemented a series of actions declassifying some of its operations. The existence of the organization was declassified in September 1992.

On 6 Sep 1961, the NRO was established as a joint CIA-Air Force operation. Throughout the 1960s, U.S. operation of reconnaissance satellites was officially classified. It was not until Jan 1971 that the NRO's existence was first disclosed by the media, when it was briefly mentioned in a New York Times article. A more extensive discussion of the NRO appeared in the Washington Post (9 Dec 1973) as a result of the inadvertent disclosure in a Congressional report.

In September 1992 DoD acknowledged the existence of the NRO, an agency established in 1961 to manage the development and operation of the nation's reconnaissance satellite systems.

See NRO website at <www.nro.gov/ > For additional information see Jeffrey T. Richelson, "Undercover in Outer Space: The Creation and Evolution of the NRO," *International Journal of Intelligence and Counterintelligence*, 13, 3 (Fall 2000): pp. 301-344.

National Security. A collective term encompassing both national defense and foreign relations of the United States with the purpose of gaining: a) a military or defense advantage over any foreign nation or group of nations; b) a favorable foreign relations position; or c) a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

-- Also, the national defense or foreign relations of the United States. (EO 13526, Classified National Security Information, 29 Dec 2009)

National Security Act. The National Security Act of 1947 realigned and reorganized the United States' armed forces, foreign policy, and Intelligence Community apparatus in the aftermath of World War II. The Act merged the Department of War and the Department of the Navy into the National Military Establishment (NME) headed by the Secretary of Defense. It was also responsible for the creation of a separate Department of the Air Force from the existing United States Army Air Forces. Initially, each of the three service secretaries maintained quasi-cabinet status, but the act was amended in 1949 to assure their subordination to the Secretary of Defense. At the same time, the NME was renamed as the Department of Defense. Aside from the military reorganization, the act established the National Security Council, a central place of coordination for national security policy in the Executive Branch, and the Central Intelligence Agency, the United States' first peacetime intelligence agency. (Public Law No. 235, 80 Cong., 61 Stat. 496)

The cornerstone of the current national security system is the National Security Act of 1947 as amended, designed to meet the challenges of the post-WWII, Cold War world. That legislation laid the foundations of a new national security regime, including the creation of the National Security Council, the Central Intelligence Agency, the Department of Defense, a separate Department of the Air Force, and a permanent Joint Chiefs of Staff. See National Security Act of 1947, P.L. 80-235.

The National Security Act has been amended numerous times since its enactment. Reference to the *"National Security Act of 1947, as amended"* indicates the legal authority cited is legislation passed after 1947 that replaced one or more provisions of the original act.
-- See <http://www.intelligence.gov/0-natsecact_1947.shtml>

National Security Agency (NSA). The U.S.'s cryptologic organization, with responsibility for protecting U.S. National Security information systems and collecting and disseminating foreign signals intelligence. Areas of expertise include cryptanalysis, mathematics, computer science, and foreign language analysis. (National Intelligence: A Consumer's Guide - 2009)

-- Also, a member of the US Intelligence Community, as well as a Combat Support Agency of the Department of Defense. NSA/Central Security Service leads the community in delivering responsive, reliable, effective, and expert Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Network Warfare operations to gain a decisive information advantage for the Nation and our allies under all circumstances. (www.nsa.gov)

NSA is the U.S. Government lead for cryptology, and its mission encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) activities. The Central Security Service (CSS) conducts SIGINT collection, processing, analysis, production, and dissemination, and other cryptologic operations as assigned by the Director, NSA/Chief, CSS. NSA/CSS provides SIGINT and IA guidance and assistance to the DoD Components, as well as national customers.

-- DoDD 5100.20, *NSA/CSS*, 26 Jan 2010

The Central Security Service (CSS) oversees the function of the military cryptologic system, develops policy and guidance on contributions of military cryptology to the Signals Intelligence / Information Security (SIGINT/INFOSEC) enterprise, and manages the partnership of NSA and the Service Cryptologic Components. NSA as a whole is known as "NSA/CSS."

-- National Intelligence: A Consumer's Guide – 2009. p. 43

The U.S. SIGINT effort… employs space and airborne collection ground stations, covert listening posts, surface ships, and submarines.

-- Jeffrey T. Richelson, *The US Intelligence Community* (2012, Sixth Edition)

I think it's fair to say that the demands on the Agency approach infinity.
Everybody wants to know everything about everything.

-- Louis Tordella, a longtime deputy director of NSA (1995)

See *60 Years of Defending Our Nation*, National Security Agency, 2012; available at : <http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf>

Also see –

Matthew M. Aid, *The Secret Sentry: The Untold History of the National Security Agency.* New York: Bloomsbury, 2009.

James Bamford, The *Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York: Anchor Book, 2008.

National Security Branch (NSB). Major element of the FBI that executes the FBI's national security mission to lead and coordinate intelligence efforts that drive actions to protect the United States. The NSB is composed of the Counterterrorism Division (CTD), Counterintelligence Division (CD), Directorate of Intelligence (DI), Weapons of Mass Destruction Directorate (WMDD), Terrorist Screening Center (TSC), and High-Value Detainee Interrogation Group (HIG). (www.fbi.gov; accessed 31 Jul 2013)

The FBI's national security and intelligence missions are unified under the authority of the Executive Assistant Director (EAD) who reports to the Deputy Director FBI. The EAD-NSB has full operational and management authority over all FBI Headquarters and field national security programs, including the authority to initiate, terminate, or reallocate any of the investigations or other activities within the NSB.

The EAD-NSB is also responsible for the continued development of a specialized national security workforce and is the lead FBI official responsible for coordination and liaison with the Director of National Intelligence (DNI) and the Intelligence Community (IC).

-- See <http://www.fbi.gov/about-us/nsb/national-security-branch-brochure>

National Security Council (NSC). A governmental body specifically designed to assist the President in integrating all spheres of national security policy. (JP 1, Doctrine for the Armed Forces of the United States. 25 Mar 2013)

> The NSC was established by the National Security Act of 1947 as the principal forum to consider national security issues that require presidential decision. Congress envisioned that the NSC would allow military and civilian government departments and agencies to work more effectively together on national security matters.
>
> ---
>
> *The National Security Council (NSC) is the President's principal forum for considering national security and foreign policy matters with the senior national security advisors and cabinet officials. For DOD, the President's decisions drive strategic guidance promulgated by the Office of the Secretary of Defense (OSD) and refined by the Joint Strategic Planning System (JSPS). To carry out Title 10, United States Code (USC), statutory responsibilities, the Chairman of the Joint Chiefs of Staff (CJCS) utilizes the JSPS to provide a formal structure in aligning ends, ways, and means, and to identify and mitigate risk for the military in shaping the best assessments, advice, and direction of the Armed Forces for the President and SecDef.*
>
> -- JP 5-0, *Joint Operation Planning* (11 Aug 2011)

National Security Council Intelligence Directive (NSCID). A formal statement of policy by the National Security Council, binding upon those US Government agencies within the purview of NSC authority. (National HUMINT Glossary)

> Regarding counterintelligence, see NSCID 5, *US Espionage and Counterintelligence Activities Abroad,* 17 Feb 1972.

National Security Crimes. Crimes likely to impact upon the national security, defense, or foreign relations of the United States, including but not limited to espionage, spying, sabotage, treason, and sedition.

National Security Division (NSD). Element of the Department of Justice (DoJ) created by the reauthorization of the USA PATRIOT Act in March 2006, the Division merges the primary national security elements of DoJ, fulfilling a key recommendation of the March 2005 report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission). The Division consists of the Counterterrorism and Counterespionage Sections; the Office of Intelligence Policy and Review; and a Law & Policy Office. (DoJ website at <http://www.usdoj.gov/nsd/>)

> The Counterespionage Section (CES), NSD, DoJ, supervises the investigation and prosecution of cases affecting national security, foreign relations, and the export of military and strategic commodities and technology.
>
> CES has executive responsibility for authorizing the prosecution of cases under criminal statutes relating to espionage, sabotage, neutrality, and atomic energy. It provides legal advice to U.S. Attorney's Offices and investigative agencies on all matters within its area of responsibility, which includes 88 federal statutes affecting national security. It also coordinates criminal cases involving the application of the Classified Information Procedures Act (CIPA). In addition, the Section administers and enforces the Foreign Agents Registration Act of 1938 (FARA) and related disclosure statutes.
>
> The Office of Intelligence Policy and Review (OIPR), NSD, DoJ, prepares and files all applications for electronic surveillance and physical search under the Foreign Intelligence Surveillance Act of 1978 (FISA). The Office also advises the National Security Division and various client agencies, including the CIA, FBI, and the Defense and State Departments, on questions of law, regulation, and guidelines, as well as on the legality of domestic and overseas intelligence operations.

National Security Emergency. Any occurrence, including natural disaster, military attack, technological, or other emergency, that seriously degrades or threatens the national security of the United States. (DoDD 5111.13, ASD(HD&ASA), 16 Jan 2009)

National Security Information (NSI). Any information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is so designated. (IC Standard 700-1, 4 Apr 2008)

Note: EO 12958 superseded by EO 13526, *Classified National Security Information*, 29 Dec 2009. For additional information see Information Security Oversight Office (ISSO) website at: <http://www.archives.gov/isoo/policy-documents/ >

National Security Interests. The foundation for the development of valid national objectives that define United States goals or purposes. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

National Security Letter (NSL). An administrative demand for documents or records that are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

-- Also, a NSL seeks customer and consumer transaction information in national security investigations from communications providers, financial institutions, and credit agencies. Five statutory provisions vest government agencies responsible for foreign intelligence investigations with authority to issue written commands comparable to administrative subpoenas. (CRS Report RS22406, 27 Sep 2010)

National security letters, which are analogous to administrative subpoenas and are authorized by five federal statutes. They are only available for authorized national security investigations (international terrorism or foreign intelligence/CI investigations), not general criminal investigations or domestic terrorism investigations. NSLs are issued directly by federal agency officials.

NSLs can only be used to seek certain transactional information permitted under the five NSL provisions, and cannot be used to acquire the content of any communications. The scope of documents which may be obtained pursuant to a national security letter is more limited than that which might be authorized in a FISA order. Statutory provisions at 18 USC §2709, 12 USC §3414, 15 USC §1681u, 15 USC §1681v and 50 USC §436; as amended by PL 109-177 and PL 109-178.

"FBI currently issues an average of nearly 60 NSLs per day."

-- CRS Report RL 33320 (3 Jan 2014), p. 22, footnote 139

For additional information see <http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm>

Also see CRS Report RS22406 at <http://www.fas.org/sgp/crs/intel/RS22406.pdf> and CRS Report RL33320 at <https://www.fas.org/sgp/crs/intel/RL33320.pdf>

National Security Strategy (NSS). A document approved by the President of the United States for developing, applying, and coordinating the instruments of national power to achieve objectives that contribute to national security. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

National Special Security Event (NSSE). A designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

-- Also, major event considered to be nationally significant as designated by the President or his designated representative, the Secretary of the Department of Homeland Security. Some events categorized as NSSE include presidential inaugurations, major international summits held in the United States, major sporting events, and presidential nominating. NSSE designation factors include: anticipated attendance by U.S. officials and foreign dignitaries; size of the event; and significance of the event. (CRS Report RS22752, updated 19 Mar 2008)

The US Secret Service is the lead federal agency responsible for coordinating, planning, exercising, and implementing security for NSSEs. Designated the lead agency in PL 106-544.

National Threat Identification and Prioritization Assessment (NTIPA). A strategic threat assessment produced by the Office of the National Counterintelligence Executive (ONCIX) that defines and prioritizes threats to the US posed by traditional and emerging foreign intelligence activities. It is designed to assist senior policymakers and officials with CI responsibilities focus on the current and emerging foreign intelligence threats that could cause unacceptable damage to US national security. The NTIPA fulfills the reporting requirement outlined in the Counterintelligence Enhancement Act of 2002. (ONCIX)

"The NTIPA informs the President if the United States of the gravest threats to our nation."

-- National Counterintelligence Strategy of the United States of America – 2012

"*The NTIPA is a compendium of foreign intelligence threat data, mandated by statute to be produced annually by the Office of the National Counterintelligence Executive and submitted to the President for approval.... Community work on the NTIPA (the first of which submitted in 2004 and approved in 2005) revealed broad challenges in collection and analysis on these difficult targets. Prioritizing foreign intelligence threats is an even more demanding analytical task, depending as it does on the consumer's interests (for example, foreign threats to [CIA] DO operations in country X or to deployed forces in country Y may be far different from the rank ordering of country threats to U.S. national security information at home) and the national security context in which they arise (that is, threat priorities do not directly correlate to foreign intelligence capability alone but must be measured against the potential for harm or disruption to U.S. national security concerns and objectives, as prioritized by policy leadership)."*

-- Michelle K. Van Cleave (former NCIX), Counterintelligence and National Strategy, School for National Security Executive Education, National Defense University, April 2007, footnote 36, pp. 33-34

The NTIPA does not go into effect until approved by the President. The NCIX submits each approved NTIPA or modification thereof to the congressional intelligence committees.

NTIPA *versus* NIPF – CI action is driven by the approved NTIPA and foreign intelligence (FI) collection is driven by the NIPF (National Intelligence Priorities Framework). Each has different focus and priorities, as well as a totally different operational dynamic.

Need for CI action is much different from the need for FI collection.

National Virtual Translation Center (NVTC). Provides timely and accurate translations of foreign intelligence for all elements of the IC. Its mission includes acting as a clearinghouse for facilitating interagency use of translators; partnering with elements of the U.S. Government, academia, and private industry to identify translator resources and engage their services; building a nationwide team of highly qualified, motivated linguists and translators, connected virtually to the program office in Washington, D.C.; and applying state-of-the-art technology to maximize translator efficiency. (National Intelligence: A Consumer's Guide - 2009)

The NVTC is a DNI Center and the FBI is the IC Executive Agent.

Naval Criminal Investigative Service (NCIS). The federal law enforcement agency charged with conducting investigations of felony-level offenses affecting the Navy and Marine Corps – that is, crimes punishable by confinement for more than one year. NCIS also performs investigations and operations aimed at identifying and neutralizing foreign intelligence, international terrorist, and cyber threats to the Department of the Navy. In addition, it provides warning of threats and specialized defensive force protection support to U.S. naval forces around the world. Criminal investigation is at the foundation of virtually all the organization does, but the NCIS mission is broad. Transnational terrorism has been and remains a key focus area for the agency. Today, NCIS' mantra is: *Prevent Terrorism, Protect Secrets, and Reduce Crime*. (www.ncis.navy.mil; accessed 28 Jun 2012)

Mission: NCIS is a federal law enforcement agency that protects and defends the DON [Department of Navy] against terrorism and foreign intelligence threats, investigates major criminal offenses, enforces the criminal laws of the United States and the UCMJ, assists commands in maintaining good order and discipline, and provides law enforcement and security services to the Navy and Marine Corps on a worldwide basis.

Director NCIS reports directly to the Secretary of the Navy and is the senior official for criminal investigations, counterintelligence, and security with the DON. Additionally, the Director NCIS is the senior official within DON for terrorism investigations and related operations designed to identify, detect, neutralize, or prevent terrorist planning and activities, and provides antiterrorism expertise and services to DON components.

-- SECNAV Instruction 5430.107, Mission and Functions of the NCIS, 28 Dec 2005

Also see SECNAV Instruction 3850.2C, *Department of the Navy Counterintelligence*, 20 Jul 2005

"Criminal investigation is at the foundation of virtually all the organization does…"
-- <http://www.ncis.navy.mil/AboutNCIS/Pages/default.aspx> (accessed 28 June 2012)

NCIS. Acronym, see *Naval Criminal Investigative Service*.

Near Real Time. Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP 1-02 and TRADOC Pam 525-2-1, US Army Functional Concept for Intelligence, 13 Oct 2010) Also see *real time*.

Need-to-know. A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, a determination that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012)

-- Also, a determination within the executive branch in accordance with directives issued pursuant to this order [EO 13526] that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (EO13526, Classified National Security Information, 29 Dec 2009)

"The need-to-know principle is fundamental to the intelligence business."
-- Duane R. Clarridge, *A Spy For All Seasons: My Life in the CIA* (1997), p. 310

The "need-to-know" principle, simply put, is that a person in authorized possession of classified information must determine that another person requires access to that information in order to perform a specific and authorized function and that such person has appropriate clearances and access approvals.

…A major tightening up of the "need-to-know" practice is in order. It is particularly disturbing to see the proliferation of detailed knowledge about intelligence sources and methods.

-- HPSCI Report (#100-5), "United States Counterintelligence and Security Concerns – 1986," 100th Congress 1st session, 4 Feb 1987, p. 9

Net-Centric. The ability to provide a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Network. [In critical infrastructure protection usage] a group or system of interconnected or cooperating entities, normally characterized as being nodes (assets), and the connections that link them. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Network Operations (NetOps). Activities conducted to operate and defend the Global Information Grid. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010)

Neutralize. 1) As pertains to military operations, to render ineffective or unusable. 2) To render enemy personnel or material incapable of interfering with a particular operation. 3) To render safe mines, bombs, missiles, and booby traps. 4) To make harmless anything contaminated with a chemical agent. (JP 1-02)

Neutrality. In international law, the attitude of impartiality during periods of war adopted by third states toward a belligerent and subsequently recognized by the belligerent, which creates rights and duties between the impartial states and the belligerent. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Neutral State. In international law, a state that pursues a policy of neutrality during war. (JP 1-02)

Nickname. A combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes. (JP 1-02) Also see *codeword*.

Non Attributable Internet Access. Use of a commercial internet service provider to access publicly available information on the internet while protecting the unit's U.S. government affiliation, disclosing essential elements of friendly information, or exposing U.S. government information systems to intrusion or manipulation. (AR 381-20, Army CI Program, 25 May 2010)

Noncustodial Interview. Interview conducted when subjects are interviewed without depriving them of their freedom in any significant manner (e.g., arrest or detention). Subjects voluntarily consent to the interview and are advised that they may depart at any time. (Army FM 2-22.2, CI, Oct 2009)

Non-Disclosure Agreement (NDA). An official authorized contract between an individual and the United States (U.S.) Government signed by an individual as a condition of access to classified national intelligence. The NDA specifies the security requirements for access and details the penalties for non-compliance. (DSS Glossary)

Nongovernmental Organization (NGO). A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011)

-- Also, a legally-constituted organization created by persons having the legal authority to do so with no participation or representation of any government. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Non-Official Cover (NOC). Term used by case officers who operate overseas outside the usual diplomatic cover. (Spy Book)

-- Also, NOC, pronounced as "knock," an acronym for "nonofficial cover." Primarily a CIA term used where one is operating without cover of diplomatic protection or US government employment. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

> *Case officers that have no visible affiliation with the U.S. government. NOCs, as they are called, might typically operate as business executives, students, writers, or in some other nongovernmental capacity. They perform those jobs in addition to doing their espionage. If they are caught in the act of spying, they do not have diplomatic immunity and are subject to the full force of the local law, including prosecution for espionage and imprisonment. NOCs usually receive less scrutiny and surveillance from the local authorities than their official colleagues.*
>
> -- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

> According a Congressional Research Service report, placing U.S. intelligence officials in foreign countries under "nonofficial cover" (NOC) in businesses or other private capacities is possible, but it presents significant challenges to U.S. agencies. Administrative mechanisms are vastly more complicated [than those] for officials formally attached to the embassy; special arrangements have to be made… The responsibilities of operatives under nonofficial cover to the parent intelligence agency have to be reconciled with those to private employers, and there is an unavoidable potential for conflicts of interest…
>
> -- CRS Report RL33539, *Intelligence Issues for Congress*, 14 Sep 2011, p. 6

Non-Permissive Environment. An operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct, do not have effective control of the territory and population in the intended operational area (Uncertain Environment); or an operational environment in which hostile forces have control as well as the intent and capability to oppose or react effectively to the operations a unit intends to conduct (Hostile Environment). (National Military Strategy to Combat Weapons of Mass Destruction, Feb 2006)

Non-Title 50 (NT50). Refers to those federal departments and organizations whose authorities derive from portions of United States Code other than Title 50, which addresses U.S. intelligence activities. NT50s are involved in many activities that affect national security, such as conducting foreign affairs; combating pandemic diseases; halting illicit trafficking; conducting scientific and medical research; regulating finance, commerce, and transportation; and protecting food, water and nuclear infrastructures.

Notice of Intelligence Potential (NIP). A document alerting consumers of a potential collection opportunity involving sources, It is often associated with travel by the source or attendance at some event. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Notional. Fictitious; most commonly used to refer to a nonexistent agent but also used to refer to fictitious organizations, individuals, or sources of information. (FBI FCI Terms)

-- Also, fictitious, imaginary, existing only in the perception of the target. Antonym of real, true, genuine, or legitimate. (CIA, D&D Lexicon, 1 May 2008)

-- Also, Notionals: fictious [sic], private commercial entities which exist on paper only. They serve as the ostensible employer of intelligence personnel, or as the ostensible sponsor of certain activities in support of clandestine operations. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Notorious Individual. Someone who is widely known and has an unfavorable public reputation. (DoDD S-5200.37, Management and Execution of Defense HUMINT (U), 9 Feb 2009 w/. chg 2)

O ==========

OFCO. Acronym, see *Offensive Counterintelligence Operation*.

Offensive Counterintelligence Operation (OFCO). A clandestine CI activity conducted for military, strategic, DoD, or national CI and security purposes against a target having suspected or known affiliation with FISS [Foreign Intelligence & Security Service], international terrorism, or other foreign persons or organizations, to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the Department or the United States. The two types of OFCO are double agent operations and Counterintelligence Controlled Source Operations (CSO). (DoDI S-5240.09, OFCO, 29 Oct 2008)

If defensive counterintelligence is checkers, then offensive counterintelligence is chess.

-- Steven Aftergood, "DIA Takes on Offensive Counterintelligence," *Secrecy News* (12 Aug 2008)

An ideal counterintelligence system anticipates the enemy's move, notionally satisfies his needs, and indeed operates a notional intelligence service for him.

-- Eric W. Timm, "Countersabotage--A CI Function" *Studies in Intelligence*, V7:2 (Spring 1963), p. 67

Offensive CI operations – CI folks call OFCO – are clandestine CI activities run in support of DoD military national security objectives and programs against individuals known or suspected to be foreign intelligence officers with connections to foreign intelligence or international terrorist activities. And they're run to counter the foreign intelligence operations, espionage, against DoD national activities and, of course, terrorist operations against DOD or national. These are very tightly controlled departmental activities run by a small group of specially selected people within DoD. There are only four organizations in the department that can run these operations – Army Counterintelligence, Naval Criminal Investigative Service, Air Force Office of Special Investigations, and now DIA with the center [Defense CI & HUMINT Center].

-- Toby Sullivan, Director of Counterintelligence for USD/I, 5 Aug 2008;
see Federal News Service transcript at <http://www.fas.org/irp/news/2008/08/dia-dchc.pdf>

Offensive counterintelligence could exploit knowledge of secret adversary infrastructures to keep adversaries off-balance and to force them to divert critical resources to defend against the offensive thrusts of well-informed enemies. Offensive counterintelligence can also deceive and manipulate the leaders of hostile coalitions, as Western governments did repeatedly in WWII, and in the Gulf War.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence*, with new introduction by the author (paperback 2001), p. xxx

---

For detailed information concerning DoD OFCO see DoDI S-5240.09, *OFCO (U),* 29 Oct 2008

Many… offensive operations have changed history,
but remain a misunderstood, and even unappreciated, CI penetration methodology.

-- CI Centre (www.cicentre.com)

-- Also (previously defined in DoDD O-5240.02, dated 20 Dec 2007), an approved CI operation involving a formally recruited human source conducted for DoD or national purposes against a target having suspected or known foreign intelligence and security services affiliation, international terrorist affiliation, or other foreign persons or organizations, to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the Department and/or the United States. *Note: this definition was deleted from DoDD O-5240.02 with change 1 dated 30 Dec 2010*.

Offensive Cyber Operations (OCO). Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 1-02 and JP 3-12, Cyberspace Operations, 5 Feb 2013)

-- Also, includes all US Government programs and activities that, through the use of cyberspace, 1) actively gather information from computers, information systems or networks or 20 manipulate, disrupt, deny, degrade, or destroy targeted adversary computers, information systems, or networks. (NSPD-38)

-- Also, offensive operations to destroy, disrupt, or neutralize adversary cyberspace capabilities both before and after their use against friendly forces, but as close to their source as possible. The goal of Offensive Cyberspace Operations (OCO) is to prevent the employment of adversary cyberspace capabilities prior to employment. This could mean preemptive action against an adversary. (DSS Glossary)

Official Information. Information that is owned by, produced for or by, or is subject to the control of the United States Government. (JP 1-02 and JP 3-61, Public Affairs, 25 Aug 2010)

Office of Foreign Missions (OFM). An office in the Department of State, Bureau of Diplomatic Security that has three missions: 1) Protecting the interests of the US and its citizens from foreign diplomats' abuses of privileges and immunities; 2) Improving the treatment of US· personnel assigned abroad by imposing reciprocal treatment on foreign diplomats assigned to the US; and 3) Services to the foreign diplomatic community in a variety of areas. Programs include the review of all notifications by foreign missions of any intent to acquire property in the US and monitoring of foreign diplomatic travel.

Office of the National Counterintelligence Executive (ONCIX). [The U.S. Government agency] charged with integrating the activities of all CI programs to make them coherent and efficient, coordinating CI policy and budgets to the same end, and evaluating the performance of the CI community against the [National CI] strategy. (National Intelligence: A Consumer's Guide - 2009) Also see *National Counterintelligence Executive.*

-- Also, ONCIX provides effective leadership and support to the counterintelligence and security activities of the US Intelligence Community, the US Government, and US private sector entities who are at risk of intelligence collection or attack by foreign adversaries. (www.ncix.gov; accessed 9 Jun 2014)

> The ONCIX is part of the Office of the Director of National Intelligence and is staffed by senior counterintelligence (CI) and other specialists from across the national intelligence and security communities. The ONCIX develops, coordinates, and produces:
> - Annual foreign intelligence threat assessments and other analytic CI products
> - An annual national CI strategy for the US Government
> - Priorities for CI collection, investigations, and operations
> - CI program budgets and evaluations that reflect strategic priorities
> - In-depth espionage damage assessments
> - CI awareness, outreach, and training standards policies.
>
> -- www.ncix.gov (accessed 9 Jun 2014)

Office of Special Investigations (OSI). See Air *Force Office of Special Investigations* (AFOSI).

One-Time Pad (OTP). Sheets of paper or silk printed with random five-number group ciphers to be used to encode and decode enciphered messages. (CI Centre Glossary)

-- Also, groups of random numbers or letters arranged in columns, used for encoding and decoding messages. Since the codes are only used once, a properly employed OTP is theoretically unbreakable. (Spycraft)

-- Also, sheets of randomly generated numbers, usually formatted into four- or five-digit groups. Each party to the secret communication… uses the same one-time pad. By a simple process of alphabetic substitution, along with "false subtraction" and "false addition," the two sides can securely communicate with each other. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

-- Also, manual one-time cryptosystem produced in pad form. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

An unbreakable cipher when used properly

One-time pad (OTP), also called Vernam-cipher or the perfect cipher, is a crypto algorithm where plaintext is combined with a random key. It is the only known method to perform mathematically unbreakable encryption. See <http://users.telenet.be/d.rijmenants/en/onetimepad.htm>

One-Time Source. A source who, may not reasonably be expected to provide information on a regular or continuing basis by reason of limited knowledgeability or circumstances of contact. (HDI Lexicon, April 2008)

-- Also, a source of information of value that was, and will be, encountered only once. (US Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

A one-time source cannot be tasked to collect information, but can be sensitized to information in which the collector is interested.

For more information see: <http://users.telenet.be/d.rijmenants/en/onetimepad.htm>

One-Way Radio Link (OWRL). The method of transmitting over radio (by voice, key, or impulses) messages to intelligence personnel who, by prearrangement, are in possession of a time schedule, signal, code, or cipher that enables them to receive and decipher messages. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

One-Way Voice Link (OWVL). One-way radio link that transmits a coded voice message to intelligence personnel who, by prearrangement, are in possession of a time schedule, signal, code, or cipher that enables them to receive and decipher messages. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, shortwave radio link used to transmit prerecorded enciphered messages to an operative, who is usually working in place in a hostile area. (CI Centre Glossary)

Open. Not classified or concealed. (CIA, D&D Lexicon, 1 May 2002)

Open Source. Any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure. (Army Techniques Publication 2-22.9, Open-Source Intelligence, 10 Jul 2012)

Open Source Acquisition. The act of gaining possession of, or access to open source information synonymous with "open source collection." The preferred term is acquisition because by definition, open sources are collected and disseminated by others[,] open source exploiters acquire previously collected and publicly available information second-hand. (ICD 301, National Open Source Enterprise, 11 Jul 2006) Also see *open source information* and *open source intelligence*.

Open Source Center (OSC). Advances the Intelligence Community's exploitation of openly available information to include the Internet, databases, press, radio, television, video, geospatial data, photos and commercial imagery; functions include collection, analysis and research, training and information technology management to facilitate government-wide access and use. The Director CIA will administer the Center on behalf of the DNI. (ODNI News Release 6-05, 8 Nov 2005)

-- Also, the OSC acts as a service of common concern to advance the IC's exploitation of open source material and nurtures acquisition, procurement, analysis, dissemination, and sharing of open source information, products, and services throughout the USG; established at CIA and builds on the former Foreign Broadcast Information Service and will include personnel from across the IC and other USG organizations; Dir CIA serves as the DNI's Executive Agent for the Center. (ICD 310, National Open Source Enterprise, 11 Jul 2006)

Open Source Collection. See *Open Source Acquisition*.

Open Source Information. Publicly available information which anyone can lawfully obtain by request or observation. (ICD 301, National Open Source Enterprise, 11 Jul 2006)

-- Also, information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access. (JP 2-0, Joint Intelligence, 22 Oct 2013)

We have no need for spies. We have the Times.
-- Tsar Nicholas I cited in Haswell, *Spies and Spymasters* (1977)

Open Source Intelligence (OSINT). Intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (PL109-163 § 931 and ICD 1, 1 May 2006)

"Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond."
-- Lieutenant General Samuel V. Wilson, USA (Ret.), Former Director, Defense Intelligence Agency

-- Also, relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, publicly available information appearing in print or electronic form, including information from radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings used to enhance intelligence analysis and reporting. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to intelligence requirements. (Army FM 2-22.9, Open Source Intelligence, Dec 2006)

-- Also, the discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (Army FM 2-0, Intelligence, 23 Mar 2010)

OSINT generally falls into four categories: 1) widely available data and information; 2) targeted commercial data; 3) individual experts; and 4) "gray" literature, which consists of written information produced by the private sector, government, and academe that has limited availability, either because few copies are produced, existence of the material is largely unknown, or access to information is constrained.

OSINT can include: media such as newspaper, magazines, radio, television, and computer-based information; public data such as government reports, and official data such as budgets and demographics, hearings, legislative debates, press conferences, and speeches; information derived from professional and academic sources such as conferences, symposia, professional associations, academic papers, dissertations and theses, and experts; commercial data such as commercial imagery; *gray literature* such as trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, and market surveys; and information, which although unclassified, could be considered company proprietary, financially sensitive, legally protected, or personally damaging, as well as information derived from Internet blogs.

-- CRS Report RL34270, 5 Dec 2007

Clandestine technical and humint sources can be used to confirm this kind of special take from open sources—and open sources can be used to confirm the information from clandestine sources.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 204

Operation Order (OPORD). A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Operation Plan (OPLAN). 1) Any plan for the conduct of military operations prepared in response to actual and potential contingences; 2) A complete and detailed joint plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment data. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Operational Control (OPCON). The authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Operational Cycle (Ops Cycle). See *recruitment cycle*.

Operational Environment. A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Operational Intelligence. Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *strategic intelligence; tactical intelligence*.

Operational Interest (OI). [Within HUMINT usage] exclusive contact with a source, as established by a HUMINT organization. Within DoD, established for all sources upon IDSRS Deconfliction and assignment of a NFN. Between DoD and other national agencies, granted for clandestine leads and sources by the Interagency Source Registry (ISR). (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, see classified definition in AR 381-20, Army CI Program (U), 25 May 2010.

Operational Level of War. The level of war at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *tactical level of war; strategic level of war*.

Operational Proposal. A formal document prepared by DoD collection elements to outline a proposed activity or operation. (HDI Lexicon, April 2008)

Operational Testing. A continuing process of evaluation that may be applied to either operational personnel or situations to determine their validity or reliability. (JP 1-02)

-- Also, any means or process employed to establish authenticity, reliability, or control. (HDI Lexicon, April 2008)

Operational Warning. A warning to theater level or equivalent decision makers of developing situations or ongoing event which may initiate operational planning or trigger the execution or change in status of standing operations or contingency plans. (DoDD 3115.16, The Defense Warning Network,5 Dec 2013)

Operations Officer - CIA. A career track within the *Core Collector* profession of the National Clandestine Service (NCS), Central Intelligence Agency (CIA). Operations Officers (OO's) are focused full time on clandestinely spotting, assessing, developing, recruiting, and handling individuals with access to vital foreign intelligence on the full range of national security issues. OO's use their sound judgment, high integrity, strong interpersonal skills, and ability to assess the character and motivations of others to establish strong human relationships and trust that provides the foundation needed to acquire high-value intelligence from foreign sources. An OO's career can include assignments in the NCS's three key areas of activity—human intelligence collection, counterintelligence, and covert action—on issues of highest interest to US national security, such as international terrorism, weapons proliferation, international crime and narcotics trafficking, and capabilities and intentions of rogue nations. Operations Officers serve the bulk of their time in overseas assignments that range typically from 2-3 years. (CIA; see <https://www.cia.gov/careers/jobs/view-all-jobs/core-collector.html>; accessed 19 Mar 2009)

Operations Security (OPSEC). A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level. (DoDD 5205.02E, DoD OPSEC Program, 20 Jun 2012)

-- Also, a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) identify those actions that can be observed by adversary intelligence systems; b) determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

OPSEC's most important characteristic is that it is a process and not a collection of specific rules and instructions that can be applied to every operation or activity

Although good operational security (Opsec) does not guarantee the success of any intelligence operation, faulty Opsec almost surely guarantees worse than failure.

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 33

OPSEC… is a systematic and proved process… [to] deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.

-- NSDD 298, *National Operations Security Program*, 22 Jan 1988, p.1

[T]here is a clear and compelling need for operational security in a military environment and in the conduct of sensitive operations.

-- Joint Security Commission, *Redefining Security*, 28 Feb 1994, p. 66

Director, DIA provides intelligence and counterintelligence threat analysis to support OPSEC planning to all DoD Components. .

– DoDD 5205.02E, *DoD OPSEC Program*, 20 Jun 2012, p. 5

National OPSEC Program

In 1988, President Ronald Reagan signed *National Security Decision Directive 298* (NSDD 298). This directive established the "National Operations Security Program" as a means to identify, control, and protect unclassified information and evidence associated with U.S. national security programs and activities.

NSDD 298 named the Director, National Security Agency, as the Executive Agent for interagency OPSEC training and included in his responsibilities the establishment and maintenance of the **Interagency OPSEC Support Staff (IOSS).**

The primary responsibility of the IOSS is to act as a consultant to other U.S. government departments or agencies by providing technical guidance and assistance that will result in self-sufficient OPSEC Programs for the protection of U.S operations. Members of the IOSS staff assess OPSEC programs, assist in OPSEC program development, conduct surveys, assessments and provide OPSEC training.

See IOSS web site at: <https://www.iad.gov/ioss/>

Operations Security Assessment (OPSEC Assessment). An evaluative process, usually exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

Operations Security Countermeasures (OPSEC Security Countermeasures). Methods and means to gain and maintain essential secrecy about critical information. (JP 1-02 and 3-13.3, Operations Security, 4 Jan 2012)

Operations Security Indicators (OPSEC Indicators). Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

Operations Security Process (OPSEC Process). A process that examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by adversaries. It is an analytical, risk-based process that incorporates five distinct elements: 1) critical information identification; threat analysis; 3) vulnerability analysis; 4) risk assessment; and 5) OPSEC countermeasures. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

The operations security process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate countermeasures.
-- NSDD 298, *National Operations Security Program*, 22 Jan 1988

Operations Security Survey (OPSEC Survey). An application of the OPSEC process by a team of subject matter experts to conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries. (DoDD 5205.02E, DoD OPSEC Program, 20 Jun 2012)

-- Also, a collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

Operations Security Vulnerability (OPSEC Vulberability). A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decisionmaking. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

Operations Support Element (OSE). An element that is responsible for all administrative, operations support and services support functions within the counterintelligence and human intelligence staff element of a joint force intelligence directorate. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) [Normally in the J2X]

OPSEC, See *Operations Security*,

Organized Cyber Intruders/Attackers. Those individuals, groups or organizations who violate international law or conventions relating to computer networks or who otherwise use the cyberspace domain to interfere with, disrupt, or deny computer network services. (OSD, *Guidance for Employment of the Force*)

Original Classification Authority (OCA). An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to initially classify information. (DoD IG Evaluation Guide, 22 Jan 2013)

-- Also, an individual authorized in writing, either by the United States (U.S.) President, or by agency heads or other officials designated by the President, to classify information in the first instance. OCAs must receive training to perform this duty. (DSS Glossary)

> *OCAs and other individuals delegated declassification authority in writing by the head of the IC element may declassify information within their purview pursuant to EO 13526 and 32 CFR Part 2001 guidelines. Only the DNI may declassify space-based national imagery, pursuant to EO 12951.*
>
> -- ICD 710, *Classification Management and Control Markings System*, 21 Jun 2013

Other Government Agency (OGA). Within the context of interagency coordination, a non Department of Defense agency of the United States Government. (JP 1-02)

Overhead Reconnaissance. Activities carried out by space-based capabilities whose principal purpose is conducting and/or enabling intelligence collection. These activities are comprised of associated R&D, acquisition, test and evaluation, and system operations performed on or by satellites, communications, and facilities for data processing as well as command and control of spacecraft and payloads. (DoDD 5105.23, NRO, 28 Jun 2011)

Overt. Activities that are openly acknowledged by or readily attributable to the US Government, and include activities designed to acquire information through legal and open means without concealment. Overt information may be collected by observation, elicitation, or from knowledgeable human sources. (ICD 304, HUMINT, 6 Mar 2008; DoDD S-5200.37, 9 Feb 2009; JP 1-02; and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, refers to being in the open, without any attempt to deceive or mislead, with full knowledge of coordinating units or agencies; activity done without attempt to conceal it. (CI Community Lexicon)

-- Also, methods of conducting DoD activities that may be acknowledged by or attributable to the U.S. Government. (HDI Lexicon, April 2008)

Overt Collection. Intelligence activities with the ultimate goal of intelligence information collection which are not designed or executed to conceal sponsorship, collection activity, identity of operators, or methodologies employed. (Previously in DoDI S-5240.17, CI Collection, 12 Jan 2009) Also see *open source intelligence.*

-- Also, the acquisition of intelligence information in the public domain. (CI Community Lexicon)

> ***"While the importance of clandestine collection should not be underestimated, many of the pieces of the jigsaw puzzle which is 'finished foreign intelligence' can be overtly collected by a well-organized information gathering system."***
>
> -- Rockefeller Commission Report (June 1975), p. 209

Overt Intelligence. Information collected openly from public or open sources. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Overt Operation. An operation conducted openly, without concealment. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Overt [HUMINT] Operations. Openly acknowledged by, or are readily attributable to, the US Government. Overt HUMINT methods include: debriefing, interrogation, elicitation, and observation. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

P ==========

Packet Sniffer. Software that observes and records network traffic. (NIST, Glossary of Key Information Security Terms, May 2013)

Parallel Investigative Jurisdiction. One or more agencies with differing objectives having simultaneous authority to investigate a matter or incident. An example would be a criminal matter that has a national security implication, which might require investigation by both a CI organization and a criminal investigative organization. (AR 381-20, Army CI Program, 25 May 2010)

Paramilitary Forces. Forces or groups distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission. (JP 1-02 and JP 3-24, Counterinsurgency, 22 Nov 2013)

Parole. A prearranged verbal exchange used for recognition and identification between intelligence personnel. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, a prearranged verbal exchange used by intelligence personnel to identify themselves to each other. (FBI FCI Terms)

Passive Source. An individual recruited by a military CI agency to act as a listening post for CI purposes in a location associated with the individual's job or social status. This source undertakes no actions unless associated with such status. A passive source is recruited or placed in an area that foreign intelligence would consider a priority target and there is evidence of foreign intelligence spotting, assessing, or recruiting activities. (AFOSI Manual 71-119, CI Investigations, 27 Oct 2009)

Pattern Recognition. An inductive process of recognizing a commonality or trend in an aggregate of indications from which as plausible explanation or model can be developed. (Word of Intelligence, 2nd Edition, 2011)

Patterns. [In CI usage,] …repeated incidents that may be similar in nature or dissimilar events that occur in a specific location or time span that may indicate potential FISS and ITO [international terrorist organization] targeting or information exploitation. (Army FM 2-22.2, CI. Oct 2009)

Patriot Act (aka USA Patriot Act). The official title is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." An act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. (PL 107-56, 26 Oct 2001; codified as amended at 50 USC § 1861)

The Patriot Act substantially expanded the authority of U.S. law enforcement agencies for the stated purpose of fighting terrorism in the United States and abroad. Among its provisions, the Act:

-- increased the ability of law enforcement agencies to search telephone and e-mail communications and medical, financial and other records;
-- eased restrictions on foreign intelligence gathering within the United States;
-- expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and
-- enhanced the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts.

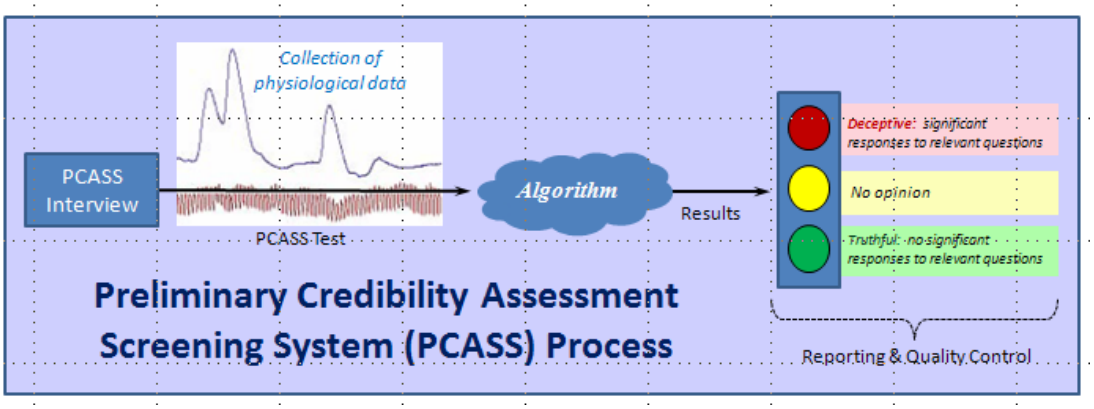
The act also expanded the definition of terrorism to include "domestic terrorism," thus enlarging the number of activities to which the Patriot Act's expanded law enforcement powers can be applied.

The Patriot Act made a number of changes to U.S. law. Key acts changed were the Foreign Intelligence Surveillance Act of 1978 (FISA), the Electronic Communications Privacy Act of 1968 (ECPA), the Money Laundering Control Act of 1986, and Bank Secrecy Act (BSA), as well as the Immigration and Nationality Act.

Additional information on the Patriot Act available on NCIX website at: <http://www.ncix.gov/publications/law/index.html>

PCASS. Acronym for "Preliminary Credibility Assessment Screening System." (DoDI 5210.91, Polygraph and Credibility Assessment Procedures, 12 Aug 2010 with change 1 dated 15 Oct 2013) Also see *PCASS Instrument; polygraph examination*.

PCASS Instrument. A diagnostic instrument used during an interview capable of monitoring, recording, and/or measuring electrodermal and vasomotor activity. The PCASS instrument uses an algorithm to evaluate the physiological responses recorded by the two components. (DoDI 5210.91, Polygraph and Credibility Assessment Procedures, 12 Aug 2010 with chg 1 dated 15 Oct 2013) See *PCASS*.



The PCASS shall only be used as a field-expedient tool to screen persons of interest for intelligence and security purposes. Only certified personnel may conduct PCASS examinations.

Per DoD policy, the PCASS will not be used to test U.S. persons (however does not apply to PCASS examinations conducted for training); see Enclosure 5, DoD Instruction 5210.91.

Peace Operations (PO). A broad term that encompasses multiagency and multinational crisis response and limited contingency operations involving all instruments of national power with military missions to contain conflict, redress the peace, and shape the environment to support reconciliation and rebuilding and facilitate the transition to legitimate governance. Peace operations include peacekeeping, peace enforcement, peacemaking, peace building, and conflict prevention efforts. (JP 3-07.3 Peace Operations, 17 Oct 2007)

Peace Building. Stability actions, predominately diplomatic and economic, that strengthen and rebuild governmental infrastructure and institutions in order to avoid a relapse into conflict. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Peace Enforcement. Application of military force, or the threat of its use, normally pursuant to international authorization, to compel compliance with resolutions or sanctions designed to maintain or restore peace and order. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Peacekeeping. Military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Peacemaking. The process of diplomacy, mediation, negotiation, or other forms of peaceful settlements that arranges an end to a dispute and resolves issues that led to it. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Pen Register. A device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider, or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any devise used by a provider, or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; see 18 USC §3127(3). (AR 381-10, US Army Intelligence Activities, 3 May 2007) Also see *trap and trace*.

-- Also, [a device that] records or decodes dialing, routing addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

> A *pen register* captures all outgoing phone numbers a particular telephone has called. A *trap and trace device* identifies all incoming phone numbers to a particular telephone.
>
> *Pen register and trap and trace (PR/TT) devices enable the prospective collection on non-content traffic information associated with wire and electronic communications, such as: the phone numbers dialed from or to a particular telephone, including electronic communications; messages sent from or to a particular telephone; or the internet protocol (IP) address of communications on the Internet and other computer networks.*
>
> -- FBI Domestic Investigations and Operations Guide, 15 Oct 2011, p. 18-123

Penetration. [In intelligence usage,] the recruitment of agents within or the infiltration of agents or technical monitoring devices in an organization or group for the purpose of acquiring information or of influencing its activities. (ICS Glossary)

> *Note: This term was previously in JP 1-02, however rescinded by JP 2-01.2, 16 Mar 2011.*

-- Also, the recruitment of agents within, or the planting of agents or technical monitoring devices within, a target organization to gain access to its secrets or to influence its activities. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, a principal counterintelligence objective is penetration of an adversary, and this can be achieved by the recruitment of a key source within an opponent's organization. Ideally, the penetration will be the recruitment of a senior figure with sufficient access to compromise all the service's operations, but lower-level penetrations, such as the management of a double agent, may be sufficient to reveal the identities of case officers and their operational premises. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

> ***The best way to catch a spy is to recruit a spy***
>
> -- Counterespionage Maxim
>
> (cited in Stuart A. Herrington, *Traitors Among US: Inside the Spy Catcher's World*, 1999, p. 255)

Penetration – a time-honored espionage practice
…oh what a tangled web we weave

The key to CI success is penetration. For every American spy, there are several members of the opposition service who know who he or she is. No matter what it takes, we have to have penetrations.

-- James M. Olson, "The Ten Commandments of Counterintelligence," *Studies in Intelligence*, Vol. 54 No. 5; see <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol45no5/html/v45i5a08p.htm>

Almost every spy that we have found, both in the CIA and FBI, has been found with the aid of recruited sources of our own on other hostile intelligence services.

-- William Webster, Former FBI Director and DCI, in Senate testimony (9 Apr 2002)

If the purpose of counterespionage is to manipulate enemy intelligence, as it is, then to have controlled agents in the staff of an enemy service is the most important objective of counterintelligence.

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

…[C]ounterespionage has one purpose which transcends all others in importance: ***penetration.*** *The only way to be sure that an enemy has been contained is to know his plans in advance and in detail. Moreover, only a high-level penetration of the opposition can tell you whether your own service is penetrated.*

…Conducting CE without the aid of penetrations is like fighting in the dark. Conducting CE with penetrations can be like shooting fish in a barrel. The famous case of Col. Oleg Penkovskiy… illustrates the great value of penetrations. There can never be enough of them.

-- Austin B. Matschulat, "Coordination and Cooperation in Counterintelligence," *Studies in Intelligence*, V13: 2 (Spring 1969), pp. 29-30.

Penetrating an adversary's intelligence service, especially the counterintelligence units, is one of the most valuable counterintelligence techniques. Often it is also notoriously difficult.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 207

All countries… strive hard to secure penetration agents; and they constitute the counter-intelligence officer's worst nightmare.

-- Chapman Pincher. *Traitors: The Anatomy of Treason*, First U.S. Edition (1987), p. 29

Penetrations - selected examples:

-- Colonel L Oleg V. Penkovsky was a British-US penetration of Soviet military intelligence (GRU).
-- Harold A.R. "Kim" Philby was a Soviet penetration of British intelligence.
-- Aldrich "Rick" Ames was a Soviet/Russian penetration of the CIA.
-- Robert (Bob) Hanssen was a Soviet/Russian penetration of the FBI.

Penetration Operation. The recruitment of agents within, the infiltration of agents, or the introduction of technical monitoring devices into an organization or physical facility to acquire information or influence the organization's activities. (AR 381-47, OFCO, 17 Mar 2006) Also see *recruitment-in-place*.

Penetration Testing. [In computer usage] a test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Pentagon Force Protection Agency (PFPA). [DoD agency that] provides force protection, security, and law enforcement to safeguard personnel, facilities, infrastructure, and other resources for the Pentagon Reservation and designated DoD facilities within the National Capital Region (NCR). (DoDD 5105.68, PFPA, 5 Dec 2013)

Perception Management. *Within DoD: None -- term removed from JP 1-02.*

Periodic Reinvestigation (PR). An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation. The scope consists of a personal interview, National Agency Check (NAC), Local Agency Check (LAC), credit bureau checks, employment records, employment references, and developed character references, and normally will not exceed the most recent 5-year period. (DSS Glossary)

Permissive Environment. Operational environment in which host country military and law enforcement agencies have control as well as the intent and capability to assist operations that a unit intends to conduct. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

PERSEREC. See *Defense Personnel Security Research Center*.

Persistent Conflict. The protracted confrontation among state, nonstate, and individual actors that are increasingly willing to use violence to achieve their political and ideological ends. (Army FM 3-0, Operations, Feb 2008)

Persistent Surveillance. *Within DoD: None -- term removed from JP 1-02.*

> Previously defined in JP 1-02 and JP 2-0, Joint Intelligence (22 Jun 2007) as: a collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in near or real-time. Persistent surveillance facilitates the prediction of an adversary's behavior and the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action

Persona. The social façade or image a person projects in public. A persona may be true or false. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

Persona Non Grata (PNG). An international diplomatic term meaning "person who is not acceptable or not welcome." It is a legal status applied to diplomats who have been caught by the host country in espionage or other unlawful activities and are expelled and thereafter denied access to the host country. (CI Community Lexicon)

> Latin for "unwelcome person." The provision for declaring a person *persona non grata* is codified in international law; see Article 9 of the Vienna Convention on Diplomatic Relations of 1961.

-- Also, a diplomatic expulsion by flag accrediting country. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, the official act of declaring a foreign national unwelcome in this country. (FBI FCI Terms)

-- Also, in diplomatic usage and under international law, the official act of declaring a foreign national, usually an official of a foreign government, as no longer welcome and forcing his/her expulsion. In tradecraft terminology, the undesirable individual is *PNG'd*. The most common use of *PNG* is for foreign diplomatic or official personnel caught in the act of engaging in illegal espionage activities. (*The CIA Insider's Dictionary*, 1996)

Personal Meeting (PM). Face-to-face contact between a handler and a lead or asset. (HDI Lexicon, April 2008)

-- Also, a clandestine meeting between two operatives, always the most desirable but a more risky form of communication. (CI Centre Glossary)

> *Personal meetings may be held to give an agent his next assignment and instructions for carrying it out, to train him in tradecraft or the use of technical or communications equipment, to transmit documents, reports, technical equipment, money, or other items, or to fulfill several of these purposes. In actual practice several purposes are usually served by a meeting. In addition to its particular objectives more general needs can be filled. A meeting held for training purposes may be a means for clarifying biographic data on the agent or his views on various subjects. At every meeting with an agent one should study him and obtain new data on his potential and talents, thereby providing a better basis for judging his sincerity and deciding how much trust to place in him.*
>
> -- L.K. Berrenev, 'Operational Contacts," *Studies in Intelligence*, Vol 9, Winter 1965, p.64 [declassified 18 Sep 1995; originally classified SECRET].

Personal Protective Security Detail. Security personnel assigned to protect individuals who, by their grade, assignment, symbolic value, or relative isolation, are likely attractive or accessible terrorist targets. These trained and armed personnel are capable of providing continuous protection for designated individuals. (DoDD 5105.68, PFPA, 5 Dec 2013)

Personally Identifiable Information (PII). Information which can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual. Includes information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc). (DoDD 5400.11, DoD Privacy Program, 8 May 2007)

-- Also, information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. (DSS Glossary)

Personnel Security. The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012, w/ chg 1)

-- A security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information. (IC Standard 700-1, 4 Apr 2008)

-- Also, [with US Army] the application of standards and criteria to determine whether or not an individual is eligible for access to classified information, qualified for assignment to or retention in sensitive duties, and suitable for acceptance and retention in the total Army consistent with national security interests. (AR 380-67, Personnel Security Program, 24 Jan 2014)

> *The essence of personnel security is to determine that those who have access to secrets as a result of their jobs are people of sufficient probity and responsibility who will safeguard that data.*
>
> -- Frederick L. Wettering, "Counterintelligence: The Broken Triad." *International Journal of Intelligence and Counterintelligence* 13 (Fall 2000), pp. 265-299.
>
> ---
>
> ***Personnel Security—The First and Best Defense***
>
> *The personnel security system is a the very heart of the government's security mission. …{The main purpose of personnel security programs is to protect the national security interests of the United States by insuring the reliability and trustworthiness of those whom information vital to those interests is entrusted.*
>
> -- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, p. 39
>
> ---

For additional information see -- Personnel Security References

EO 12968, *Access to Classified Information*

EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*

DoD 5200.2-R, *Personnel Security Program*

For Army policy see: AR 380-67, *Personnel Security Program*

Personnel Security Investigation (PSI). An inquiry into the activities of an individual, designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to loyalty, character, emotional stability, and reliability. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

DoD generates 90% of the security investigation requirements in the Executive Branch….
-- Security and Suitability Process Reform: Strategic Framework, Feb 2010

A PSI is an inquiry into an individual's loyalty, character, trustworthiness, and reliability to ensure that he/she is eligible to access classified information, or for an appointment to a sensitive position or position of trust. DoD uses PSIs to determine an individual's eligibility for a security clearance.

In 2005, DoD transferred most of its PSI workload to U.S. Office of Personnel Management (OPM). All PSIs are conducted by the designated investigative service provider. In the case of DoD, OPM is the designated investigative service provider.

The types of PSIs vary based on the level of security clearance necessary for a given sensitive position. The personnel security clearance process is governed primarily by EO 12968 (Access to Classified Information), EO 13467 (Reforming Processes Related to Suitability for Government Employment) and the Federal Investigative Standards. DoD Regulation 5200.2-R, "Personnel Security Program," outlines criteria for sensitive positions and the corresponding clearance levels.

-- Also, any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations…conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position. (AR 380-67, Personnel Security Program, 24 Jan 2014)

Pharming. Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential data, e.g., mimicking bank websites.
(FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Phishing. Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, usually an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

-- Also, a form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. (McAfee.com; accessed 15 Nov 2010)

-- Also, Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. (Words of Intelligence, 2nd Edition, 2011)

Phreaking. Gaining unauthorized access to telecommunication systems. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Physical Search. Any intrusion upon a person or a person's property or possessions to obtain items of property or information. The term does not include examination of areas that are in plain view and visible to the unaided eye if no physical trespass is undertaken, and does not include examinations of abandoned property left in a public place. (DoD 5240.1-R, Dec 1982) Also see *search*.

> Types include consented physical search, plain view search, search incident to a lawful apprehension, and nonconsensual physical search. See USC §1821(5).
>
> For DoD CI see Chapter 7, Procedure 7-Physical Searches, DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 Dec 1982

Physical Security. The security discipline concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012 w/ chg 1 dated 24 Apr 2013)

> The physical protection of information, assets and personnel is fundamental to nay security system.
> -- Joint Security Commission Report, *Redefining Security*, 28 Feb 1994, p. 56

-- That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02 and JP 6-0, Joint Communications Systems, 10 Jun 2010)

-- Also, the security discipline concerned with physical measures designed to: protect personnel; prevent unauthorized access to facilities, equipment, material, and documents; and defend against espionage, terrorism, sabotage, damage, and theft. (IC Standard 700-1, 4 Apr 2008)

Physical Security Investigation. All inquires, inspections, or surveys of the effectiveness of controls and procedures designed to provide physical security; and all inquires and other actions undertaken to obtain information pertaining to physical threats to DoD personnel or property. (JP 1-02)

Physical Surveillance. A systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance. (DoD 5240.1-R, Dec 1982) Also see *surveillance*.

> *Surveillance, the job of following and observing designated persons without being noticed, is intrinsic to counterintelligence.*
> -- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)
>
> For DoD CI see Chapter 9, Procedure 9 - Physical Surveillance, DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 Dec 1982

-- Also, physical surveillance (not requiring a court order): the deliberate observation… of persons, places, or events, on either a limited or continuous basis, in areas where there may or may not be a reasonable expectation of privacy. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

-- Also, physical surveillance (with a warrant or court order): a physical search constitutes any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in the seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011, p. 18-152)

Piracy. An illegal act of violence, depredation (e.g., plundering, robbing, or pillaging), or detention in or over international waters committed for private ends by the crew or passengers of a private ship or aircraft against another ship or aircraft or against persons or property on board such ship or aircraft. (JP 1-02)

Pitch. [In intelligence usage] the effort made to recruit a source. (HDI Lexicon, April 2008)

Placement. An individual's proximity to information of intelligence interest. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *access; placement & access.*

-- Also, the rationale for a HUMINT source or operational asset's presence in an operational area. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

Placement and Access (P&A). An individual's proximity to and ability to collect information of intelligence interest. (HDI Lexicon, April 2008) Also see *access.*

Plain Text. Unencrypted information. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Planned Target. Target that is known to exist in the operational environment, upon which actions are planned using deliberate targeting, creating effects which support commander's objectives. (JP 3-60, Joint Targeting, 13 Apr 2007)

Planning. The ability to establish a framework to employ resources to achieve a desired outcome or effect. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

-- Also, the process by which commanders (and the staff, if available) translate the commander's visualization into a specific course of action for preparation and execution, focusing on the expected results. (Army FM 3-0, Operations, Feb 2008)

Planning and Direction. In intelligence usage, the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Planning Order (PLANORD). A planning directive that provides essential planning guidance and directs the initiation of execution planning before the directing authority approves a military course of action. (JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *execute order (EXORD).*

Plant. [In intelligence usage,] 1) to insert information into a target's intelligence channel; 2) an individual infiltrated into a foreign organization (a penetration); 3) a forged document provided to a foreign organization. (CIA in D&D Lexicon, 1 May 2002)

Planted Information. False or misleading information that the target has been permitted or helped to collect. (CIA in D&D Lexicon, 1 May 2002)

Platform. In collection parlance, the conveyance for collection sensors.

Plausible Denial. Official disclaimer supported by a believable cover story. (CIA in D&D Lexicon, 1 May 2002) Also see *plausible deniability*.

Plausible Deniability. The concept that allows the United States government, specifically the U.S. president himself, to claim no knowledge of or involvement in a covert action that goes public, particularly if it has gone badly. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Pocket Litter. The usual litter found in pockets: coins, tickets, keys, etc. In this case, pocket litter is planted so that if the agent is caught, incidental-looking items will reinforce his cover story. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

Police Information. All available information concerning known and potential enemy and criminal threats and vulnerabilities collected during police activities, operations, and investigations. Analysis of police information produces police intelligence. (ATTP 3-39.20, Police Intelligence Operations, Jul 2010)

Police Intelligence. Police intelligence results from the application of systems, technologies, and processes that analyze applicable data and information necessary for situational understanding and focusing policing activities to achieve social order. (ATTP 3-39.20, Police Intelligence Operations, Jul 2010)

Political Intelligence. Intelligence concerning foreign and domestic policies of governments and the activities of political movements. (JP 1-02)

Polygraph and Credibility Assessment (PCA). The overarching term covering programs, research, training, and procedures that employ technologies to assess an individual's truthfulness with the aid of technical devices that measure physiological data or behavioral activity. (DoDI 5210.91, PCA Procedures, 12 Aug 2010 with chg 1 dated 15 Oct 2013) Also see *polygraph examination*.

Polygraph Examination. A process that encompasses all activities that take place between a polygraph examiner and examinee during a specific series of interactions. (DoDD 5210.48, PCA Program, 25 Jan 2007 with change 2 dated 15 Nov 2013) Also see *credibility assessment; polygraph instrument*.

-- Also, a highly structure technique conducted by specialty trained CI personnel certified by proper authority as polygraph examiners. (Army FM 2-22.2, CI, Oct 2009)

Polygraph – Greek for "many writings"

The most significant contribution of the polygraph is its success in eliciting information and its value as a deterrent; however, the polygraph should be one of several investigative tools.

-- Webster Commission Report (*A Review of FBI Security Programs*), March 2002 (p. 68)

The polygraph is a multichannel instrument that records changes in respiration, cardiovascular activity, and skin resistance in response to questions. According to polygraph theory, when a subject gives a false response to a relevant question…, the physiological reaction will be greater than the reaction to others questions (control or irrelevant questions). However, contrary to popular belief, there is no physiological response that is unique to deception. The reactions measured by the polygraph can be caused by a variety of emotions. This fact underlies much of the controversy surrounding the polygraph. […]

Two types of polygraphs are currently used in personnel security screening the counterintelligence-scope(CI-scope) polygraph and the full-scope polygraph. The CI-scope polygraph focuses on espionage, sabotage, terrorism, mishandling classified information, and unauthorized contacts with representatives of foreign governments. […] Screening polygraphs arguably have a deterrent effect.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, pp.61-70

The evidence is overwhelming that the polygraph, in the hands of a skilled examiner, is a very useful tool to elicit information from an applicant or an employee that might otherwise be obtained only after lengthy and costly investigation—or not at all.

-- DCI's Blue Ribbon Panel on the Polygraph, *CIA's Use of Polygraph in Personnel Screening*, Redacted Copy approved for public release 29 May 2012. Copy available at:
<http://www.nationalsecuritylaw.org/files/received/CIA/Poly_Use_of_Polygraphy_in_Personnel_Screening.pdf>

For additional information, see --

"Your Polygraph Examination" at:
<http://www.cdse.edu/multimedia/polygraph_videos/polygraph.pdf>

Committee to Review the Scientific Evidence on the Polygraph, *The Polygraph and Lie Detector (Washington,* DC: National Academies Press, 2003).

Ken Alder, *The Lie Detector: The History of an American Obsession* (New York: Free Press, 2007)

John F. Sullivan, *Gatekeeper: Memories of a Polygraph Examiner* (Washington, DC: Potomac Books, 2007)

Also see the American Polygraph Association (APA) web site at <http://www.polygraph.org/>

Polygraph Instrument. A diagnostic instrument to measure and record respiration, electrodermal, blood volume, and heart rate responses to verbal or visual stimuli. (DoDI 5210.91, Polygraph and Credibility Assessment Procedures, 12 Aug 2010 with chg 1 dated 15 Oct 2013) Also see *polygraph examination*.

PORTICO. The nickname for the DoD Counterintelligence Community's enterprise information capability that promotes information sharing and provides standardized CI activity reporting across the Department. PORTICO operates in a secure network environment and facilitates standardization of DoD CI business processes by providing a common interface for shared results of core CI functions (i.e., collection, investigations, analysis & production, operations, and functional services).

Port Security. The safeguarding of vessels, harbors, ports, waterfront facilities, and cargo from internal threats such as destruction, loss, or injury from sabotage or other subversive acts; accidents; thefts; or other causes of similar nature. (JP 1-02 and JP 3-10, Joint Security Operations in Theater, 3 Feb 2010)

Positive Intelligence. A term of convenience sometimes applied to foreign intelligence to distinguish it from foreign counterintelligence. (ICS Glossary, 1978)

-- Also, information gathered concerning a foreign power that is significant to national security, foreign relations, economic interest, and other plans and policies of a government. (CI Community Lexicon)

In the early 1900's military intelligence consisted of two separate fields of endeavor: positive intelligence and negative intelligence. Positive intelligence focused on "seeking information on our enemies or potential enemies" and negative intelligence focused on "preventing enemies or potential enemies from acquiring information of value about the United States." Following World War I, the term *negative intelligence* was replaced by *counterintelligence*.

-- Source: Bruce W. Bidwell, *History of the MI Division… Army General Staff: 1775 - 1941* (1986)

Posse Comitatus Act. Prohibits search, seizure, or arrest powers [by] US military personnel [in civilian law enforcement matters in the US unless authorized by legislation]. Amended in 1981 under Public Law 97-86 to permit increased DoD support of drug interdiction and other law enforcement activities [Title 18, USC § 1385]. (JP 1-02)

Posse Comitatus Act (PCA) places strict limits on the use of federal military personnel for law enforcement. Enacted in 1878, PCA prohibits the willful use of the US Army (and later, the US Air Force) to enforce laws, except as authorized by the Congress or the US Constitution. Although the PCA, by its terms, refers only to the Army and Air Force, DoD policy extends the prohibitions of the Act to the US Navy and Marine Corps, as well.

Specifically prohibited activities include: interdiction of a vehicle, vessel, aircraft, or similar activity; search and/or seizure; arrest, apprehension, "stop-and-frisk" detentions, and similar activities; and use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators. Additionally, federal courts have recognized exceptions to the PCA. These common law exceptions are known as the "military purpose doctrine" and the "indirect assistance" exceptions.

Exceptions and/or circumstances not falling under PCA include:
1) Actions that are taken for the primary purpose of furthering a military or foreign affairs function of the United States;
2) Federal troops acting pursuant to the President's Constitutional and statutory authority to respond to civil disorder;
3) Actions taken under express statutory authority to assist officials in executing the laws, subject to applicable limitations; and
4) Civil Disturbance operations authorized by statute.

The PCA does not apply to National Guard forces operating in state active duty or Title 32 USC status, nor to the USCG, which operates under Title 14 USC authority.

For an overview of the Posse Comitatus Act, see CRS Report R42659, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law* (16 Aug 2012), by Charles Doyle and Jennifer K. Elsea; copy available at: <http://www.fas.org/sgp/crs/natsec/R42659.pdf>

Also see Craig T. Trebilcock, *The Myth of Posse Comitatus*, October 2000; copy available at: < http://www.homelandsecurity.org/journal/articles/trebilcock.htm>

Also see DoDI 3025.21, *Defense Support of Civilian Law Enforcement Agencies*, 27 Feb 2013.

Preliminary Credibility Assessment Screening System (PCASS) Instrument. A diagnostic instrument used during an interview capable of monitoring, recording, and/or measuring electrodermal and vasomotor activity. The PCASS instrument uses an algorithm to evaluate the physiological responses recorded by the two components. (DoDI 5210.91, PCA Procedures, 12 Aug 2010 with change 1 dated 15 Oct 2013)

Only certified personnel may conduct PCASS examinations. Also IAW current DoD policy the PCASS will not be used to test U.S. persons.

Preliminary Inquiry. An unobtrusive review of the facts and circumstances of an incident or allegation to determine if the preliminary information or circumstances is sufficient to warrant the initiation of an investigation or referral to an investigative entity. The limited objective will be determined by the policy of individual agencies and may include the collection of information from other agencies and/or other records such as travel, financial, HR, security, and badgeing [sic], etc.; which may be used to make an informed determination if the incident involved is part of a pattern. (ONCIX Insider Threat Detection – Glossary) Also see *counterintelligence investigation*, *counterintelligence inquiry*, *investigation; preliminary counterintelligence investigation; Section 811 referral*.

Within DoD the proper term of use is *Counterintelligence Inquiry* or *CI Inquiry*; see DoDI O-5240.21, Counterintelligence Inquiries, 14 May 2009 with change 2 dated 15 Oct 2013.

Preliminary Investigation [counterintelligence related]. A limited scope inquiry into the circumstances surrounding a reported incident or matter of potential CI interest to determine if there are specific facts giving reason to believe that a threat to national security may exist or if a full field CI investigation is warranted. (AR 381-20, Army CI Program, 25 May 2010)

Preparation of the Environment (PE). An umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operations. (JP 3-05, Special Operations, 18 Apr 2011)

President's Daily Brief (PDB). An all-source, analytic document produced for the President of the United States and members of his/her Cabinet and senior staff. Production is overseen by the ODNI with contributions from the Intelligence Community.

Preventive Deployment. The deployment of military forces to deter violence at the interface or zone of potential conflict where tension is rising among parties. Forces may be employed in such a way that they are indistinguishable from a peace operations force in terms of equipment, force posture, and activities. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Prisoner of War (POW or PW). A detained person (as defined in Articles 4 and 5 of the Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949) who, while engaged in combat under orders of his or her government, is captured by the armed forces of the enemy. (JP 1-02 and JP 3-50. Personnel Recovery, 20 Dec 2011)

Private Information. Data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization. (Army Techniques Publication 2-22.9, Open-Source Intelligence, 10 Jul 2012)

Private Sector. An umbrella term that may be applied in the United States and in foreign countries to any or all of the nonpublic or commercial individuals and businesses, specified nonprofit organizations, most of academia and other scholastic institutions, and selected nongovernmental organizations. (JP 3-57, Civil Military Operations, 8 Jul 2008)

Privacy Act. The Privacy Act of 1974 (5 U.S.C. 552a) establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by an individual's name or by some other identifier assigned to the individual. The Privacy Act requires that agencies provide public notice of their systems of records through publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records absent the written consent of the individual who is the subject of the information search, unless the disclosure is pursuant to one of 12 statutory exceptions. The Privacy Act also provides individuals with a means by which to seek access to and amend their records and sets forth various agency record-keeping requirements. (ODNI, U.S. National Intelligence – An Overview 2011)

> For DoD policy see DoD Regulation 5400.11-R, DoD Privacy Act Program.
>
> The Privacy Act regulates the way certain types of information may be acquired and used by the Federal Government and provides certain rights to individuals whose information is acquired by the government.
>
> A 240-page overview of the Act can be found at: <http://www.justice.gov/opcl/1974privacyact.pdf>

Proactive TSCM. CI-focused TSCM targeting using a risk-based approach with the goal of identifying and exploiting technical collection efforts targeting DoD interests. (DoDI 5240.05, TSCM, 3 Apr 2014)

Probable Cause. Would a prudent individual believe that a fact is probably true. (Congressional Research Memorandum, Subject: Probable Cause, Reasonable Suspicion, and Reasonableness Standards in the Context of the Fourth Amendment and the Foreign Intelligence Surveillance Act, 30 Jan 2006; at <http://www.fas.org/sgp/crs/intel/m013006.pdf>) Also see *reasonable belief*.

-- Also, 1) To search: A reasonable belief that a crime has been committed and that the person, property, or evidence sought in connection with the crime is located in the place or on the person to be searched; and/or 2) To apprehend: A reasonable belief that a crime has been committed and that the person to be apprehended committed it. (AR 190-20, Military Police Investigations, 1 Nov 2005)

Probable Cause / Reasonable Belief

The facts and circumstances are such that a trained and experienced reasonable person would hold the belief.

- Fact Specific / Situation Dependant
- Must be based on facts and circumstances that can be articulated
- Can be based on experience, training and knowledge as it applies to the facts and circumstances
- "Hunches" and "intuitions" don't count
- Often requires education of non-intelligence personnel

-- Briefing, *Legal Fundamentals for Counterintelligence Professionals*, Staff Judge Advocate, US Army Intelligence and Security Command, nd. circa 2012

Probe. In information operations, any attempt to gather information about an automated information system or its on-line users. (JP 3-13, Information Operations, 13 Feb 2006) Also see *information operations*.

-- Also, [In computer usage / information operations] a technique that attempts to access a system to learn something about the system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Processing. A system of operations designed to convert raw data into useful information. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Processing and Exploitation. In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Production. The preparation of reports based on analysis of information to meet the needs of intelligence users (Consumer's) within and outside the Intelligence Community. (CIA, *A Consumer's Guide to Intelligence*, July 1995) Also see *intelligence production*.

-- Also, conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of data from all available sources and the preparation of intelligence products in support of known or anticipated user requirements. (AR 381-20, Army CI Program, 25 May 2010)

Production results in the creation of intelligence, that is, value-added actionable information tailored to a specific customer. In government parlance, the term 'finished intelligence" is reserved for products issued by analysts responsible for synthesizing all available sources of intelligence, resulting in a comprehensive assessment of an issue or situation, for use by senior analysts or decision makers.

-- DIA, *Intelligence Essentials for Everyone*, June 1999

Production is the development of intelligence through the analysis of collected information and existing intelligence. Analysts create intelligence products, conclusions, or projections regarding threats and relevant aspects of the operational environment to answer known or anticipated requirements in an effective format.

-- ADRP 2-0, Intelligence, Aug 2012, p. 3-7

Production Requirement (PR). A customer's formal request for analytic support, identifying the topic or issue of interest, type of information or analysis required, date required, preferred format, and classification. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

-- Also, an intelligence requirement that cannot be met by current analytical products resulting in tasking to produce a new product that can meet this intelligence requirement. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Proliferation. The transfer of weapons of mass destruction, related materials, technology, and expertise from suppliers to hostile state or non-state actors. (JP 1-02 and JP 3-40, Combating WMD, 10 Jun 2009)

Program Protection Plan (PPP). A risk-based, comprehensive, living plan to protect CPI that is associated with an RDA program. (DoDI 5200.39, CPI Protection within the DoD, 16 Jul 2008 with change 1 dated 28 Dec 2010) Also see *counterintelligence support plan (CISP); critical program information (CPI)*.

Note: DoDI 5200.39 is under revision. A proposed *draft* definition for PPP: a risk-based, comprehensive, living plan to identify and protect CPI and mission-critical functions and components associated with an RDA program.

Program Protection is the integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle.

The **purpose of the PPP** is to help programs ensure that they adequately protect their technology, components, and information. The PPP is used to develop tailored protection guidance for dissemination and implementation throughout the program for which it is created. The layering and integration of the selected protection requirements documented in a PPP provide for the integration and synchronization of CPI protection activities throughout DoD.

Once a PPP is in place, it should guide program office security measures and updated as threats and vulnerabilities change or are better understood. Appendix B to the PPP is the **Counterintelligence Support Plan (CISP),** which should be cited/referenced here.

See "Program Protection Plan Outline & Guidance," Version 1.0, July 2011; copy available on line at: < http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf >

Prominent Individual. Someone who is widely known and has a favorable public reputation. (DoDD S-5200.37, Management & Execution of Defense HUMINT, 9 Feb 2009)

Propaganda. Any form of adversary communication, especially of a biased or misleading nature, designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. (JP 1-02 and JP 3-13.2, Psychological Operations, 7 Jan 2010)

Proprietaries. A term used… to designate ostensibly private commercial entities capable of doing business which are established and controlled by intelligence services to conceal governmental affiliation of intelligence personnel and/or governmental sponsorship of certain activities in support of clandestine operations. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Protection. The ability to prevent, mitigate adverse effects of attacks on personnel (combatant /non-combatant) and physical assets of the United States, allies, and friends. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

-- Also, preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Protective Service Detail. Trained and armed protective security officials capable of providing continuous protection for a designated individual. (DoDI 2000.12, DoD AT Program, 1 Mar 2012 w/ change 1 dated 9 Sep 2013)

Protective Intelligence (PI). CRIMINT [criminal intelligence] used to identify, analyze, and provide leads for investigation into various direct and indirect threats to DoD personnel and property. It may provide further details about persons who may have the interest, motive, intention, and capability of mounting attacks against the DoD and its personnel. Additionally, it can aid DoD LEAs in gauging the potential threat to and vulnerability of a targeted individual or property and may be used in determining or preventing violence. (DoDI 5525.18, Law Enforcement Criminal Intelligence in DoD 18 Oct 2013)

Protective Measures. Those actions, procedures, or designs implemented to safeguard protected information. (DSS Glossary)

Provocation. Activity designed to induce an individual, organization, intelligence service, or governments to take action damaging to itself. (FBI FCI Terms) Also see *dangle; double agent.*

-- Also, activity intended to cause an individual, organization, intelligence service, or government to take actions that can cause damage to itself. (Spy Book)

Provocation [aka *Dangle*]

"A *provocation* is an agent deployed by you to be recruited by an opponent and to perform his or her secret work *under your control* as a channel to and weapon against your opponent."

-- William R. Johnson, *Thwarting Enemies at Home and Abroad*, Georgetown University Press (2009), p.98

Prudent Risk. A deliberate exposure to potential injury or loss when the commander judges the outcome in terms of mission accomplishment as worth the cost. (ADRP 6-0, Mission Command, May 2012)

Pseudonym. A code name assigned to an individual, place, or activity to enhance operational, administrative, and communication security. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, an assigned identity that is used to protect an individual's true identity. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Psychological Operations (PSYOP). *Within DoD: None -- term rescinded. See Military Information Support Operations (MISO).*

Term changed to MISO IAW SECDEF Memo dated 3 Dec 2010.

Public Affairs (PA). Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. (JP 1-02 and JP 3-61, Public Affairs, 25 Aug 2010)

Public Diplomacy. 1). Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. 2). In peace building, civilian agency efforts to promote an understanding of the reconstruction efforts, rule of law, and civic responsibility through public affairs and international public diplomacy operations. Its objective is to promote and sustain consent for peace building both within the host nation and externally in the region and in the larger international community. (JP 1-02 and JP 3-07.3, Peace Operations, 17 Oct 2007)

Public Domain. In open view; before the public at large and not in private or employing secrecy or other protective measures. (DSS Glossary)

Public Information. Within public affairs, that information of a military nature, the dissemination of which is consistent with security and approved for release. (JP 1-02 and JP 3-61, Public Affairs, 25 Aug 2010)

Publicly Available Information. Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could lawfully be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any vent that is open to the public. (Attorney General Guidelines for National Security Investigations and Foreign Intelligence Collection, 31 Oct 2003)

--Also, data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public. (Army Techniques Publication 2-22.9, Open-Source Intelligence, 10 Jul 2012)

Q ==========

Questionable Intelligence Activity. An intelligence activity, as defined in EO 12333, that may be unlawful or contrary to E.O., Presidential directive, or applicable DoD policy governing that activity. (DoDD 5148.11, ATSD/IO, 24 Apr 2013) Also see *intelligence oversight*.

> DoD Policy: See DoD 5240 1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,* 7 Dec 1982.
>
> Also see DTM 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*, 17 Jun 2009 with chg 4 dated 21 Aug 2013; copy at <http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-052.pdf>

Quit Claim. A document in which an asset acknowledges that all commitments due have been met by the handler's organization. (HDI Lexicon, April 2008)

R ==========

Rabbit. [Tradecraft jargon] The target in a surveillance operation. (CI Centre Glossary)

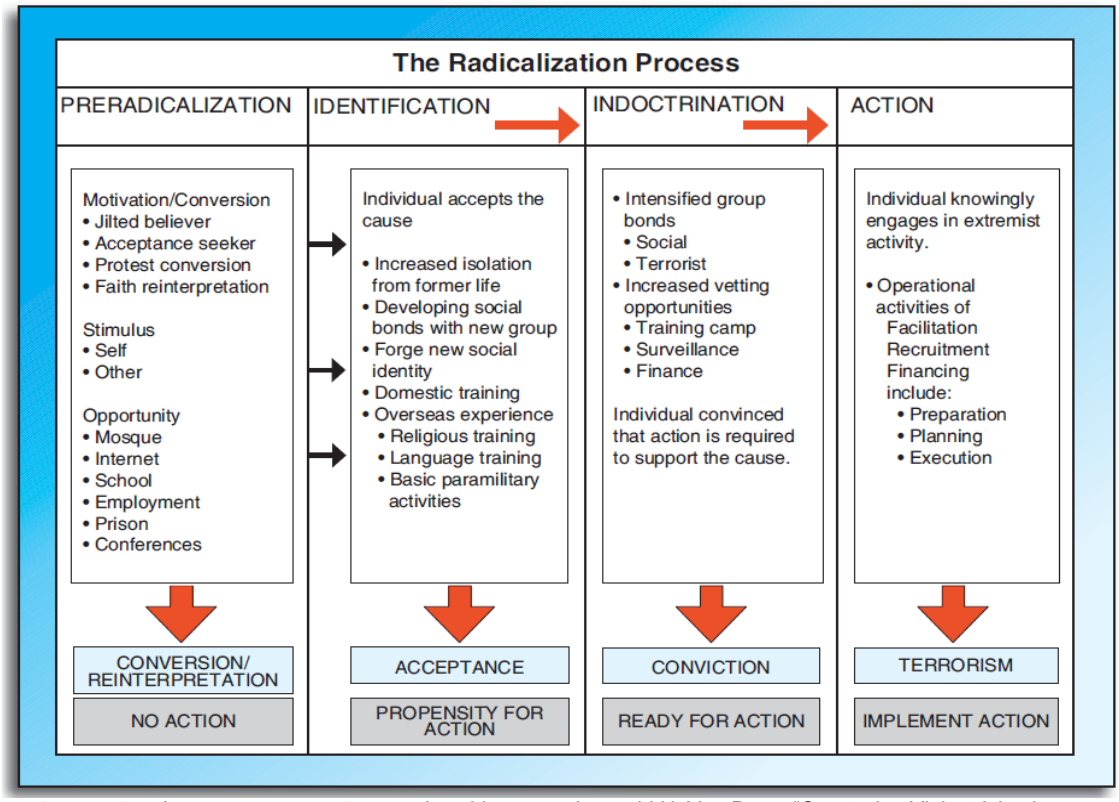
Radiogram. Coded bursts of data sent by a radio transmitter that can be picked up by a radio receiver that has been set to the proper frequency; as transmitted, radiograms generally sound like the transmission of Morse code. (FBI Affidavit, 25 June 2010)

Radicalization. The process of acquiring and holding radical or extremist beliefs. (Congressional Research Service Report R42553, *Countering Violent Extremism in the United States,* 19 Feb 2014) Also see *self-radicalization*; *violent extremism, violent radicalization*.

-- Also, the social and behavioral process whereby people adopt and embrace extremist attitudes, values or behaviors. It is a risk factor for involvement in terrorism, but involvement in terrorism does not always result from radicalization. JP1-02 does not include a definition for radicalization. (Defense Science Board Report, *Predicting Violent Behavior*, Aug 2012, citing Horgan's *The Psychology of Terrorism 2nd Edition*, 2012)

Radicalization Process

The FBI model describes the radicalization process – the "way stations" – as four incremental stages of development: 1) Preradicalization, 2) Identification, 3) Indoctrination, and 4) Action. Each one is distinct, and a radicalized individual may never reach the final stage.
See chart—*The Radicalization Process*—below…



Source: Carol Dyer, Ryan E. McCoy, Joel Rodriguez, and Donald N. Van Duyn, "Countering Violent Islamic Extremism: A Community Responsibility, *FBI Law Enforcement Bulletin*, Vol 76, No 12, Dec 2007*

* Copy available at <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2007-pdfs/dec07leb.pdf>

-- Also, the process by which an individual, group, or mass of people undergoes a transformation from participating in the political process via legal means to the use or support of violence for political purposes. (Army Tactical Reference Guide, Radicalization into Violent Extremism – A Guide for Military Leaders, April 2011

The growth in social media and the terrorist use of chat rooms, Facebook, Twitter, YouTube, and other sites has facilitated radicalization inside the United States.

-- Seth G. Jones, The RAND Corporation, "The Extremist Threat to the U.S. Homeland," Testimony Before the Committee on Homeland Security United States House of Representatives, 15 January2014 (This testimony available at <http://www.rand.org/pubs/testimonies/CT403.html>)

There is no easily identifiable terrorist-prone personality, no single path to radicalization and terrorism. Many people may share the same views, and only a handful of the radicals will go further to become terrorists. The transition from radical to terrorist is often a matter of happenstance. It depends on whom one meets and probably on when that meeting occurs in the arc of one's life.

-- Brian M. Jenkins*

* Brian Michael Jenkins, *Would Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001* (Santa Monica, CA: The RAND Corporation, 2010), p. 7.

Studies by the Department of Homeland Security's Office of Intelligence and Analysis indicate that the radicalization dynamic varies across ideological and ethno-religious spectrums, different geographic regions, and socio-economic conditions. Moreover, there are many diverse "pathways" to radicalization and individuals and groups can radicalize or "de-radicalize" because of a variety of factors.

-- U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Written Testimony of Charles E. Allen, Assistant Secretary of Intelligence and Analysis and Chief Intelligence Officer, Department of Homeland Security, "Threat of Islamic Radicalization to the Homeland," 110th Cong., 1st sess., March 14, 2007, p. 5.

Also see US Army Asymmetric Warfare Group, Tactical Reference Guide, *Radicalization into Violent Extremism, A Guide for Military Leaders, August 2011*—copy available at: <http://www.wired.com/images_blogs/dangerroom/2012/10/Radicalization-FINAL090911.pdf>

Raid. An operation to temporarily seize an area in order to secure information, confuse an adversary, capture personnel or equipment, or to destroy a capability culminating with a planned withdrawal. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Rapport Building. Establishing a sense of connection between the interviewer and the interviewee to facilitate communication and information sharing. (Keats, 1993)

Raw Data. Bits of collected data that individually convey little or no useful information and must be collated, aggregated, or interpreted to provide meaningful information. (ODNI, U.S. National Intelligence – An Overview 2011)

Raw Intelligence. A colloquial term meaning collected intelligence information that has not yet been converted into finished intelligence. (ODNI, U.S. National Intelligence – An Overview 2011)

Reachback. The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 1-02 and JP 3-30, Command and Control for Joint Air Operations, 12 Jan 2010)

Reactive Operation. An operation initiated in response to a FIS personal contact. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Real Time. Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays. (Previously in JP 2-0, Joint Intelligence) Also see *near real time*.

Reasonable Belief. A reasonable belief arises when the fact and circumstances are such that a reasonable person would hold the belief. Reasonable belief must rest on the facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or counterintelligence work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not. (DoD 5240.1-R, December 1982) Also see *probable cause*; *reasonable suspicion.*

Reasonable Expectation of Privacy. In U.S. constitutional law the expectation of privacy is a legal test which is crucial in defining the scope of the applicability of the privacy protections of the Fourth Amendment to the United States Constitution.

> The extent to which a reasonable person in the particular circumstances involved is entitled to believe his or her actions are not subject to outside observations. Must be both objectively and subjectively reasonable [as well as] very fact specific. (SJA Office, USAINSCOM)
>
> _____
>
> As a general matter the Supreme Court has held that there may be circumstances in which a government employee has a legitimate expectation of privacy in the contents of governmental property that the employee uses or controls at work, such as an office or a locked desk drawer. See: O'Connor, 480 U.S. at 716-19 (1987) (plurality) (public employee has a reasonable expectation of privacy in personal items, papers, and effects in office, desk, and file cabinets provided by public employer); see id. at 730-31 (Scalia, J., concurring) (government employee has a legitimate expectation of privacy in the contents of his office).
>
> Instead, whether, in a particular circumstance, a government employee has a legitimate expectation of privacy in his use of governmental property at work is determined by "[t]he operational realities of the workplace" and "by virtue of actual office practices and procedures, or by legitimate regulation." See: O'Connor, 480 U.S. at 717 (plurality); see United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) ("[O]ffice practices, procedures, or regulations may reduce legitimate privacy expectations.").

Reasonable Suspicion. Specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch of criminal activity. (United States v. Mason, 628 F.3d 123, 128 – 4th Cir. 2010 [quoting United States v. Branch, 537 F.3d 328, 336 – 4th Cir. 2008])

Recognition Signal. Any prearranged signal by which individuals or units may identify each other. (JP 1-02 and JP 3-50. Personnel Recovery, 20 Dec 2011)

-- Also, prearranged visual indicator used for recognition and identification between intelligence personnel. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, prearranged visual signal used by intelligence personnel to identify each other. (FBI FCI Terms)

Reconnaissance (RECON). A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Records Check. The process whereby a Special Agent obtains relevant information about Sources or Subjects from the records and information holdings of military, civilian or government agencies, as well as certain commercial companies and vendors, during the conduct of an investigation or operation. Types include military agency checks (MACs), local agency checks (LACs) and national agency checks (NACs).

-- *Military Agency Check* (MAC): a records or files check conducted at any military agency within the jurisdiction of the CI element conducting the check.

-- *Local Agency Check* (LAC): a records or files check of official or publically available information retained by any local office or government agency within the jurisdiction of the CI element conducting the check. Records may include holdings and databases maintained by local and state law enforcement agencies, local courts, local offices of federal agencies, etc.

-- *National Agency Check* (NAC): formal requests to federal agencies for searches of their records and supporting databases and files for information of investigative or operational interest. NACs include DoD agencies, as well as other federal agency holdings, e.g., FBI, CIA, DHS, ICE, IRS, OPM, State Department, FINCEN, etc.

Recovery Operations. Operations conducted to search for, locate, identify, recover, and return isolated personnel, human remains, sensitive equipment, or items critical to national security. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Recruitment. The deliberate and calculating effort to gain control of an individual and to induce him or her to furnish information or to carry out intelligence tasks for an intelligence or CI service. (DoDI S-5240.17, CI Collection Activities, 14 Mar 2014)

-- Also, authorized personnel establishing control over an foreign individual who, witting or unwitting of USG involvement, accepts tasking as a result of the established relationship; authorized personnel establishing control over a U.S. person who, fully aware of USG involvement, accepts tasking as a result of the established relationship. (DoDI S-5200.42, Defense HUMINT and Related Activities (U), 8 Dec 2009 w/ chg 1 dated 16 Aug 2010)

-- Also, the acquisition of an individual's services who, witting or unwitting of U.S. Government involvement, accepts directions and control thus obligating both parties to an act in a prescribed manner. (HDI Lexicon, April 2008)

-- Also, the establishment of a degree of control over an individual who, witting or unwitting of U.S. Government involvement accepts tasking as a result of the relationship established. (Army TC 2-22.307, Aug 2009)

-- Also, the process of enlisting an individual to work for an intelligence or counterintelligence service. (FBI FCI Terms)

-- Also, term for the tradecraft process of enlisting a target individual to work for an intelligence or security service. (*The CIA Insider's Dictionary*, by Leo D. Carl, 1996)

-- Also, the tradecraft process of enlisting a target individual to work for an intelligence service—in most cases against his own country. The process includes spotting, assessing, developing, and recruitment. Motivation may be ideological, financial, or other, such as revenge. (A Spy's Journey)

Recruitment… is a process of salesmanship, almost of seduction.
-- SSCI Report 99-522 (1986)

Agent recruiting is the most important task of both strategic and operational intelligence. No real problems can be solved without agent penetration in basic government, military and technological centres of the enemy.

-- Victor Suvorov, *Inside Soviet Military Intelligence* (1984); see Chapter 4 - Agent Recruiting.

Agent recruitment is a tedious process with a low rate of success and a high rate of return. Of every ten agents recruited, eight will fall by the wayside because they lose their access or they tire of the commitment, one will be a problem—mainly of security—and one will work as a productive agent, perhaps for decades.

-- Joseph W. Wippl (35 year CIA career with the National Clandestine Service), "The Qualities That Make a Great Case Officer," *International Journal of Intelligence and Counterintelligence*, Vol 25 No 3 (Fall 2012), p. 602

Recruitment… is an art form

How do you do recruitment? *"How do you sell anything in life? You have to have a product, you have to develop a relationship, and in that relationship you have to be able to identify people's strengths and weaknesses. And then you have to be able to ask that tough question: Will you help me? There is a sense of timing in it. It's an art form, very frankly."*

-- Jack Devine, 32-year CIA veteran in "Ten Questions," *Time* Magazine, Vol. 183 No. 23, 16 June 2014. p. 60

Recruitment Cycle. The… process by which intelligence services recruit agents (aka the agent acquisition process). (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

"The recruitment cycle is the essence of spying"

Seven steps of the recruitment cycle: 1) Spotting; 2) Assessing; 3) Developing; 4) Pitching; 5) Formalizing; 6) Producing; and 7) Terminating.

-- James M. Olson (CIA Retired), Former Chief CIA Counterintelligence

-- Also, *Agent Recruitment Cycle* (ARC): the systematic method for acquiring agents HUMINT sources) who will satisfy intelligence collection requirements and meet intelligence needs.

*The **Agent Recruitment Cycle** consists of six steps:*

+ *Spotting (or identifying) individuals who can meet intelligence needs as identified by analyst or policymakers.*
+ *Assessing whether the spotted individuals have the placement and access to provide the desired information as well as beginning the process of determining their motivations, vulnerabilities, and suitability.*
+ *Developing a relationship with the individual to further assess the factors above and to explore whether they will be responsive to initial tasking for intelligence information.*
+ *The actual recruitment.*
+ *Training and handling meetings with the agent, including taskings and debriefings.*
+ *Either turning an agent over to another case officer or terminating the relationship.*

-- Randy Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCALS," *Studies in Intelligence*, Vol 57, No 1 (March 2013), p. 55

Seven basic areas: 1) Spotting; 2) Evaluation; 3) Recruiting; 4) Testing; 5) Training; 6) Handling; and 7) Termination.

+ *Spotting: the process of identifying foreigners or other persons who might be willing to spy…*
+ *Evaluation: a thorough review of all information available…*
+ *Recruiting: the recruitment "pitch".… People volunteer or agree to spy on their governments for many reasons. It is the task of the recruiter to determine what reason—if one exists—is most likely to motivate the potential agent.*
+ *Testing: [testing the asset's] loyalty and reliability …*

+ Training: [tradecraft training] instructed in one of several methods of covert communications… learn the use of clandestine contacts. And… will be given training on security precautions, such as the detection and avoidance of surveillance.
+ Handling: Successful handling of an agent hinges on the strength of the relationship that the case officer is able to establish with the agent. ….a good case officer must combine the qualities of a master spy, a psychiatrist, and a father confessor. …One of the biggest problems in handling an agent is caused by the changeover of case officers.
+ Termination: All clandestine operations ultimately come to an end. …[need for] resettlement

-- Victor Marchetti and John D. Marks, *The CIA and the Cult of Intelligence*, 2nd Edition (1980), pp 215-228

Agent recruitment [cycle]: 1) Spot; 2) Assess; 3) Develop & Recruit; 4) Test; 5) Train; 6) Handle; and 7) Terminate.

-- Jefferson Mack, *Running a Ring of Spies* (1996)

Recruitment-in-Place (RIP). An official who overtly continues to work for his government and clandestinely provides information of intelligence value to a foreign government; will in many instances be connected with a foreign government's intelligence service. (CI Community Lexicon) Also see *penetration; penetration operation*.

-- Also, a person who agrees to become an agent and retain his position in his organization or government while reporting on it to an intelligence or security organization of a foreign country. (ICS Glossary)

-- Also, inducement of a person to become an informant or agent of an intelligence service while he or she remains in the same position and status. This term applies to personnel of foreign establishments, diplomatic or other, who continue to occupy their regular posts instead of defecting. (AFOSI Instruction 71-101, 6 Jun 2000)

-- Also, a foreign national who overtly continues to work for his government and covertly provides the U.S. with information of intelligence value. (FBI FCI Terms)

Recruitment-in-place, one of the most difficult and sensitive activities in counterintelligence.

-- William H. Webster, Director FBI, Speech on 22 March 1986

Recruiting anybody to be a spy is an act of seduction. Recruiting hostile intelligence officers amounts to seducing seducers—an art in itself.

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 337

A recruitment who stays on the job… is the ultimate prize, the crown jewel of any counterintelligence operation. At great personal risk, a recruitment in place is in a position to provide continuous and up-to-date information. By contrast, a defector, while usually welcome, is of less value. Once debriefed of the information he or she knows, and with no further access to secrets, a defector has diminished worth.

-- David Wise, *Tiger Trap: America's Secret Spy War with China* (2011), p. 177

It is axiomatic in intelligence work that 'there is no better counterintelligence than recruiting the other side's intelligence officers.'

-- James M. Olson (CIA Retired), Former Chief CIA Counterintelligence

Reconstitution. The process of restoring critical assets and their necessary infrastructure support systems (or their functionality) to pre-incident operational status. (DoDI 3020.45, DCIP Management, 21 Apr 2008)

RED. In cryptographic systems, refers to information or messages that contain sensitive or classified information that is not encrypted. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *BLACK*.

RED EYE. The RED EYE Task Force, hosted by AFMC [Air Force Material Command] and sponsored by Region 1 [AFOSI] is a multi-agency operation consisting of nine federal law enforcement and intelligence agencies working together to identify, exploit, neutralize and mitigate threats of illicit procurement and illegal export of sensitive U.S. technology to foreign adversaries. (AFOSI 2012 Fact Book)

Red Team. An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *red team analysis*.

> A "CI Red Team" is a simulation of a foreign intelligence collection activities of a specified friendly/Blue target, such as a RDA project/program, installation, military operation, etc. May include the identification of physical, electronic, acoustic, or visual patterns of the supported activity/agency as may be seen through the eyes of ad adversary.

Red Team Analysis. Models the behavior of an individual or group by trying to replicate how an adversary would think about an issue. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005) Also see *red team*.

> Red Team analysis tries to consciously place the analyst in the same cultural, organizational, and personal setting -- "putting them in their shoes" -- in which the target individual or group operates. Red Team analysis is not easy to conduct. It requires significant time to develop a team of qualified experts who can think like the adversary.
>
> ***Contrarian methods and "Red Teams" should be a routine part of the analytical process.***
>
> -- Jeffrey R, Cooper, *Curing Analytical Pathologies*, Center for the Study of Intelligence (Dec 2005), p. 43

Redaction. For purposes of declassification, the removal of exempted information from copies of a document. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012)

Refugee. A person who owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his or her nationality and is unable or, owing to such fear, is unwilling to avail himself or herself of the protection of that country. See also *dislocated civilian; displaced person; evacuee; expellee; stateless person*. (JP 1-02 and JP 3-29, Foreign Humanitarian Assistance, 17 Mar 2009)

Regional Security Officer (RSO). A security officer responsible to the chief of mission (ambassador), for security functions of all US embassies and consulates in a given country or group of adjacent countries. (JP 1-02 and JP 3-10, Joint Security Operations in Theater, 3 Feb 2010)

-- Also, Diplomatic Security Special Agents of the U.S. Department of State (DoS), assigned to U.S. diplomatic missions overseas as the personal advisor to the ambassador or chief of mission on all security issues and coordinate all aspects of a mission's security program. They develop and implement effective security programs to protect DoS employees from terrorist, criminal, and technical attack both at work and at home. The RSO serves as the primary liaison with foreign police and security services overseas in an effort to obtain support for U.S. law enforcement initiatives and investigations. (DoS)

> See Department of State website at: <http://www.state.gov/m/ds/protection/c8756.htm>

Reid Technique. A method of questioning subjects and assessing their credibility. The technique consists of a non-accusatory interview combining both investigative and behavior-provoking questions. If the investigative information indicates that the subject committed the crime in question, the *Reid Nine Steps of Interrogation* are utilized to persuade the subject to tell the truth about what they did. The Reid technique involves three different components — factual analysis, interviewing, and interrogation. (Wikipedia; accessed 21 Aug 2013)

> The term *"Reid Technique"* is a registered trademark of the firm John E. Reid and Associates, which offers training courses in the method they have devised. The technique is widely used by numerous law-enforcement agencies. For more information see: <http://www.reid.com/>

Remediation. Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the act of mitigating a vulnerability or a threat. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Rendition. An extra-territorial activity to apprehend and return a person to the US or another country, with or without permission from the country in which the subject is apprehended. (National HUMINT Glossary)

> *The term "rendition" in the counterterrorism context means nothing more than moving someone from one country to another, outside the formal process of extradition.*
> -- Daniel Benjamin, Former Director for Counterterrorism, National Security Council
>
> ---
>
> For additional information see CRS Report (RL32890) *Renditions: Constraints Imposed by Laws on Torture,* 8 Sep 2009; copy available at: <http://www.fas.org/sgp/crs/natsec/RL32890.pdf>

Repatriate. A person who returns to his or her country or citizenship, having left said native country either against his or her will, or as one of a group who left for reason of politics, religion, or other pertinent reasons. (JP 1-02)

Repatriation. 1) The procedure whereby American citizens and their families are officially processed back into the United States subsequent to an evacuation. (JP 3-68, Noncombatant Evacuation Operations, 23 Dec 2010); and 2) The release and return of enemy prisoners of war to their own country in accordance with the 1949 Geneva Convention Relative to the Treatment of Prisoners of War. (JP 1-0, Personnel Support to Joint Operations, 16 Oct 2006)

Report of Investigation (ROI). An executive summary of all results of investigative activity conducted in an investigation. (902d MIG Investigations Handbook, updated 17 Oct 2012) .

Reportable Incident. Any suspected or alleged violation of Department of Defense policy or of other related orders, policies, procedures or applicable law, for which there is credible information. (JP 1-02 and JP 3-63, Detainee Operations, 30 May 2008)

Request For Assistance (RFA). A request based on mission requirements and expressed in terms of desired outcome, formally asking for assistance.

Request For Information (RFI). 1) Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. 2) A term used by the National Security Agency/Central Security Service to state ad hoc signals intelligence requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Research, Development, and Acquisition (RDA). All activities associated with research and engineering, acquisition, international transfers of technology, and disposal of defense-related technology. (DoDI O-5240.24,CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

Residency. An office or location in a country used by foreign intelligence officers from which to plan, coordinate, and execute intelligence activities. Also refers to the number of foreign intelligence agents present in a given area. (AR 381-20, Army CI Program, 25 May 2010)

Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (PPD-21, 2013)

Resiliency. The characteristic or capability to maintain functionality and structure (or degrade gracefully) in the face of internal and external change. (DoDI 3020.45, DCIP Management, 21 Apr 2008)

Resistance Movement. An organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability. (JP 1-02 and JP 3-05, Special Operations, 18 Apr 2011)

Responsible Analytical Center (RAC). The Intelligence organization that has responsibility for providing integrated all-source analysis, or application of analysis, to produce an intelligence product to answer a specific COCOM Intelligence Task List (ITL) task or sub-task. DoD organizations that qualify as RACs include: DIA analytical offices [including DAC-1C] and Intelligence Centers, the COCOM Joint Intelligence Operations Centers (JIOCs), and the Service intelligence production centers (MCIA, NASIC, NGIC, and ONI). (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007)

Restraint. In the context of joint operation planning, a requirement placed on the command by a higher command that prohibits an action, this restricting freedom of action. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Restricted Area. An area (land, sea or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity commander/director, properly posted, and shall employ physical security measures. Additionally, Controlled Areas may be established adjacent to Restricted Areas for verification and authentication of personnel. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, 1) An area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize interference between friendly forces; and 2) An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry. (JP 1-02)

Restricted Target. A valid target that has specific restrictions placed on actions authorized against it due to operational considerations. Also see *restricted target list*. (JP 3-60, Joint Targeting, 13 Apr 2007)

Restricted Target List (RTL). A list of restricted targets nominated by elements of the joint force and approved by the joint force commander. This list also includes restricted targets directed by higher authorities. Also see *restricted target*. (JP 3-60, Joint Targeting, 13 Apr 2007)

Returnee. A displaced person who has returned voluntarily to his or her former place of residence. (JP 3-29, Foreign Humanitarian Assistance, 17 Mar 2009)

Revolution. The overthrow or renunciation of one government or ruler and the substitution of another by the governed. (Army FM 3-24-2, Tactics in Counterinsurgency, April 2009)

Risk. Probability and severity of loss linked to threats or hazards and vulnerabilities. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, probability and severity of loss linked to hazards (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

-- Also, a measure of consequence of peril, hazard or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability). (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, a measure of the potential degree to which protected information is subject to loss through adversary exploitation. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (DHS, National Infrastructure Protection Plan - 2009)

When you hear "calculated risk," don't ask to see the calculations.
-- Dr. Gus Weiss, Former Assistant Secretary of Defense for Space Policy
(quoted in *Intelligence Analysis: A Target-Centric Approach*)

Risk, in the context of critical infrastructure and terrorism, can be defined as the potential consequence associated with a particular kind of attack or event against a particular target, discounted by the likelihood that such an attack or event will occur (threat) and the likelihood that the target will sustain a certain degree of damage (vulnerability).

Threat includes not only the identification of specific adversaries, but also their intentions and capabilities (both current and future). Consequences include lives and property lost, short term financial costs, longer term economic costs, environmental costs, etc.

Given this definition, risk is not threat, nor vulnerability to a threat, nor the estimated consequences associated with a specific attack, but some integration of the three.
-- CRS Report, RL30153, 8 Jan 2007

Risk Avoidance. A security philosophy which postulates that adversaries are all-knowing and highly competent, against which risks are avoided by maximizing defenses and minimizing vulnerabilities. (DSS Glossary) Also see *risk management*.

Risk Analysis. A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information. (DSS Glossary)

-- Also, examination of information to identify the risk to an information system. See risk assessment. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Risk Assessment. A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the identification and assessment of hazards (first two steps of risk management process). (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, a process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, a defined process used to fuse the procedures of analyzing threat, risks, and vulnerabilities, into a cohesive, actionable product. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, the process of evaluating security risks based on analyses of threats, vulnerabilities, and probable adverse consequences to a facility, system, or operation. (IC Standard 700-1, 4 Apr 2008)

Risk Assessment

The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).

-- CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010

Risk Management (RM). The process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

*The basic concept for a cost effective security system is **risk management** rather than the unattainable and unaffordable goal of risk avoidance.*

-- Joint Security Commission II Report, 24 August 1999, p.12

-- Also, a process by which decision makers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, process and resultant risk of systematically identifying, assessing and controlling risks. Commanders/Directors are required to identify critical assets and their subsequent protection requirements, including future expenditures required for the protection requirements. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, the process of selecting and implementing security countermeasures to accept or mitigate the risk of a known or suspected threat to an acceptable level based on cost and effectiveness. (IC Standard 700-1, 4 Apr 2008)

-- Also, *Antiterrorism (AT) Risk Management*: the process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits. AT risk management is one of the five minimum elements of an AT program. The end products of the AT program risk management process shall be the identification of DoD elements and personnel that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT risk management (threat assessment, criticality assessment, and vulnerability assessment), the commander or DoD civilian manager must determine which DoD elements and personnel are at greatest risk and how best to employ given resources and FP measures to deter, mitigate, or prepare for a terrorist incident. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

Risk Mitigation. Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/ countermeasures recommended from the risk management process. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Risk Response. Actions taken to remediate or mitigate risk, or to reconstitute capability in the event of loss or degradation. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Romeo Spies. Men whose task is to seduce women who have access to confidential material, in the hope that through pillow talk the women will reveal secrets. (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd revised edition 2012)

Rolling Car Pickup. A clandestine car pickup executed so smoothly that the car hardly stops at all and seems to have kept moving forward. (CI Centre Glossary) Also see *car pick-up*.

Rule of the Least Intrusive Means. The collection of information by a DoD intelligence component must be accomplished by the **least intrusive means** or lawful investigative technique reasonably available. (DIA Intelligence Law Handbook, Sep 1995)

> This rule prescribes a hierarchy of collection techniques which must be considered before an intelligence component engages in collection of information about US persons. The methodologies below become progressively more intrusive as one proceeds through this hierarchical framework:
>
> -- First, to the extent feasible, information must be collected from publically available materials, or with the consent of the person or persons concerned.
>
> -- Second, if collection from these sources is not feasible, then cooperating sources may be used.
>
> -- Third, if neither publically available information nor cooperating sources are sufficient or feasible, and then collection may be pursued using other lawful investigative techniques that require neither a judicial warrant nor the approval of the Attorney General of the United States.
>
> -- Finally, when none of the first three approaches has been sufficient or feasible, then the collecting intelligence component may seek approval for use of one of the techniques that require a warrant or approval of the Attorney General.
>
> DoD Policy: see DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 7 Dec 1982 (para C2.4.2, page 18).

Rules of Engagement (ROE). Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. (JP 1-02 and JP 1-04, Legal Support to Military Operations, 17 Aug 2011)

Ruse. In military deception, a trick of war designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

S ==========

Sabotage. An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the willful destruction of government property with the intent to cause injury, destruction, or defective production of national defense or war materials by either an act of commission or omission. (IC Standard 700-1, 4 Apr 2008)

Sabotage is a violation of Title 18 USC, §§ 2151-2156.

[S]abotage is the destruction of material by covert means in order to destroy the capability of a country to pursue its policies.

-- Tucker, David. *Illuminating the Dark Arts of War*, New York: Continuum International Publishing Group, 2012, p. 136

Safe House. An innocent-appearing house or premises established by an organization for the purpose of conducting clandestine or covert activity in relative security. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, a facility use to afford security for operations. (HDI Lexicon, April 2008)

-- Also, house or premises controlled by an intelligence service that affords at least temporary security for individuals engaged in intelligence operations. (CI Community Lexicon)

-- Also, any house, apartment, office, or other building or quarters used to afford security for persons engaged in clandestine activities or for intelligence collection purposes. Safe houses may be used as refuge for or holding of agents or defectors; lodging and feeding of couriers, escapees, or evaders; lodging and working space for agents; rendezvous training, briefing, or questioning; or storage of supplies and equipment. (National HUMINT Glossary)

-- Also, a location controlled by an intelligence service that provides a secure place for individuals engaged in intelligence operations to meet. (FBI FCI Terms)

-- Also, a secure facility, unknown to adversary intelligence and security services, used for agent meetings, defector housing or debriefing, and similar support functions. (CIA in D&D Lexicon, 1 May 2002)

-- Also, [safehouse] a secure location used by intelligence services to meet with agents or for other clandestine purposes. The renter or purchaser of a safehouse is usually a cutout, someone who has no visible connection with intelligence work or with any official organization. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

-- Also, [safehouse] a sterile location, normally a house or apartment—but could be a hotel room as well—used to meet agents securely. (A Spy's Journey)

Safeguarding. Measures and controls that are prescribed to protect classified information. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012)

Sanction Enforcement. Operations that employ coercive measures to control the movement of certain types of designated items into or out of a nation or specified area. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Sanitization. The editing of intelligence to protect sources, methods, capabilities, and analytical procedures to permit wider dissemination (IC Standard 700-1, 4 Apr 2008)

Sanitize. To revise a report or other document in such a fashion as to prevent identification of sources, or of the actual persons and places with which it is concerned, or of the means by which it was acquired. Usually involves deletion or substitution of names and other key details. (JP 1-02)

Sanitizing. The removal of information from the media or equipment such that data recovery using any known technique or analysis is prevented. Sanitizing shall include the removal of data from the media, as well as the removal of all classified labels, markings, and activity logs. Properly sanitized media may be subsequently declassified upon observing the organization's respective verification and review procedures. (DSS Glossary)

Satellite Reconnaissance Advanced Notice (SATRAN) Program. Advanced warning of reconnaissance satellite orbits so military commanders can take appropriate action. (Center for Army Lessons Learned, http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=26671, accessed 4 Mar 2014)

> *In response to the intelligence threat from Soviet imagery satellites, the United States initiated the Satellite Reconnaissance Advanced Notice (SATRAN) program… in 1966.*
>
> -- Jeffrey T. Richelson, *The US Intelligence Community* (2012, Sixth Edition), pp. 270-271
>
> ---
>
> *The mission of the SATRAN Program is to provide the US military, US Government agencies… with warning of periods where their equipment or activities are vulnerable to reconnaissance by foreign spacecraft. The SATRAN program provides accurate overflight information in a timely manner so that foreign spacecraft are denied the opportunity to collect useful intelligence data.*
>
> -- Intellipedia (accessed 4 Mar 2014)

SATRAN. Acronym, see *Satellite Reconnaissance Advanced Notice Program* above.

Scams. [Cyber usage] Fake deals that trick people into providing money, information, or service in exchange for the deal. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Scattered Castles. The IC [Intelligence Community] security clearance repository and the Director of National Intelligence's authoritative source for clearance and access information for all IC, military services, DoD civilians, and contractor personnel. DoD information is furnished by JPAS. (IC Standard 700-1, 4 Apr 2008)

Scientific and Technical Intelligence (S&TI). The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information that covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Scientific Method. [One of the four basic types of reasoning applied to intelligence analysis, it] combines deductive and inductive reasoning: induction is used to develop the hypothesis, and deduction is used to test it. (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *abduction; deduction; induction.*

> For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003).

Screening. In intelligence, [the] evaluation of an individual; or a group of individuals to determine their potential to answer collection requirements or to identify individuals who match a predetermined source profile coupled with the process of identifying and assessing the areas of knowledge, cooperation, and possible approach techniques for an individual who has information of intelligence value. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> For additional information see Chapter 6 "Screening," FM 2-22.3, *Human Intelligence Collection Operations*.

SCRM. See *Supply Chain Risk Management*.

Search. An examination, authorized by law, of a specific person, property, or area for specified property or evidence, or for a specific person for the purpose of seizing such property, evidence, or person. (AR 190-20) Also see *physical search*, *search warrant*, *seizure*.

Search Warrant. An express authorization to search and seize issued by competent civilian authority. (AR 190-20) Also see *search, seizure*.

> A search warrant is a court order authorizing law enforcement to search a specified location and seize evidence. Under the Fourth Amendment, searches must be reasonable and specific.
>
> The Fourth Amendment prohibits unreasonable searches and seizures (U.S. Constitution. Amendment. IV). Searches and seizures are presumptively unreasonable, unless they are conducted pursuant to a warrant issued by a neutral magistrate upon a sworn showing of probable cause (*Terry v. Ohio*, 393 U.S. 1, 20, 1968).

Sector-Specific Agency. Federal departments and agencies identified in Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," 7 December 2003 as responsible for CI/KR [critical infrastructure and/or key resource] protection activities in specified national CI/KR sectors. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, a Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (PPD-21, 2013)

> PDD 21 identifies 16 critical infrastructure sectors and designates associated Federal SSAs. For the critical infrastructure sector "Defense Industrial Base" the Department of Defense is the designated SSA by PDD 21.

Secret, Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe. (EO 13526) Also see *security classification*.

SECRET Internet Protocol Router Network (SIPRNet). The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010)

Secret Writing (SW). Invisible writing. (FBI FCI Terms)

-- Also, any tradecraft technique employing invisible messages hidden in or on innocuous materials. This includes invisible inks and microdots, among many other variations. (CI Centre Glossary)

-- Also, tradecraft term that describes the act of using special inks or special carbons papers (impregnated with chemicals) to write messages clandestinely. The utilization of special inks is known as the "wet system." The utilization of special carbon papers is known as the "dry system." (*Encyclopedia of the CIA*, 2003]

The simplest secret writing uses organic inks: milk, vinegar, lemon juice, even urine. These inks dry invisibly and can be developed by applying heat. Espionage agencies have produced many inks made of chemicals that could be developed only by a specific chemical.

-- Spy Book

The chief difficulty with secret inks was their inability to handle great volume of information that spies had to transmit in a modern war.

-- David Kahn, *The Codebreakers* (1967)

The techniques of secret writing are the same the world over. First the spy writes his cover letter. Then he writes the secret message on top, using a special sheet of carbon paper treated with a colorless chemical. Tiny particles of the chemical; are transferred to the letter, which can then be developed by the recipient. Most developing agents make the chemical traces grow, so that the message becomes legible, and unless the correct agent is known, the message remains undetectable.

-- Peter Wright, *Spy Catcher* (1987), p.119

For an explanation of secret inks, see Robert Wallace and H. Keith Melton, *Spycraft: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda* (2008), pp. 427-437.

Section 603 Referral. Section 603 of the "Intelligence Authorization Act for FY 1990" states: "Subject to the authority of the Attorney General, the FBI shall supervise the conduct of all investigations of violations of the espionage laws of the United States by persons employed by or assigned to United States diplomatic missions abroad. All departments and agencies shall report immediately to the FBI any information concerning such a violation. All departments and agencies shall provide appropriate assistance to the FBI in the conduct of such investigations. Nothing in this provision shall be construed as establishing a defense to any criminal, civil, or administrative action." (Public Law 101-193, 30 Nov 1989) Also see *Section 811 Referral*.

See <http://www.intelligence.senate.gov/laws/pl101-193.pdf>

Section 811 Referral. Section 811 of the Intelligence Authorization Act of 1995 (50 USC 402a) is the legislative act that governs the coordination of counterespionage investigations between Executive Branch agencies and departments and the FBI. Section 811 referrals are the reports – made by the Executive Branch agencies or departments to the FBI under Section 811(c)(1)(a) – that advise the FBI of any information, regardless of origin, which may indicate that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power. (CI Community Lexicon)

Section 811 was enacted in response to the damage to US national security caused by the Aldrich Ames espionage case. The Ames case led to a legislative call for agencies to share data in counterespionage investigations and for the FBI to be involved earlier in the process of evaluating information concerning the possible compromise of classified information.

Within DoD, all *811 Referrals* are considered "significant CI activities" and as such must also be reported to DIA Office of Counterintelligence - Counterespionage Division (OCI-2)

See <http://www.intelligence.senate.gov/laws/pl103-359.pdf>

"811" referrals… allow our operational counterintelligence sections to concentrate solely on detecting and countering foreign intelligence operations, focus on emerging strategic threats, and protecting United States secrets from compromise.

-- Robert S. Muller, III, Director FBI
Before the Senate Committee on the Judiciary (6 June 2002)

Security. Proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012 w/ chg 1 dated 24 Apr 2013) Also see *operational security (OPSEC); security disciplines; security profession, security professional.*

DoD Policy

Security is a mission critical function of the DoD and its proper execution has a direct impact on all DoD missions and capabilities and on the national defense.

Security is the personal responsibility of all DoD personnel….

-- DoD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012

-- Also, 1) Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. 2) A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 3) With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (JP 1-02; JP 2-0, Joint Intelligence, 22 Oct 2013; and JP 3-10, Joint Security Operations in Theater, 3 Feb 2010)

-- Also, the protection of information to assure it is not accidentally or intentionally disclosed to unauthorized personnel. (DSS Glossary)

Security is not counterintelligence – counterintelligence is not security.

"People like to confuse counterintelligence (CI) with security. In practice, the two are related but not identical."

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

"…[C]ounterintelligence measures deal directly with foreign intelligence service activities, while security programs are indirect defensive actions that minimize vulnerabilities."

-- SSCI Report 99-522 (1986)

"Counterintelligence investigates the enemy, or if you will in the modern world, the opposition, to learn their capabilities, intentions, methods and focus. ***It is not security work. Security protects. It does not attack.*** *[Emphasis added] CI attacks the actor. It attacks the opposition intelligence structures. It is not speculative. CI feeds security because it helps them focus on meaningful measures and safeguards. Using CI to help security is just smart security."*

-- Robert P Hanssen (Soviet Spy, Former FBI Agent and current Federal inmate) as quoted in "Diary of a Spy" by Paul M. Rodriquez, *Insight on the News*, 16 July 2001.

Security *vs.* Counterespionage -- *"[T]he security effort seeks primarily to protect its assigned material against compromise, deliberate or accidental, while the counter-espionage effort operates actively to identify, thwart. mislead, and destroy an opposing espionage capability."*

-- George P. Morse, *America Twice Betrayed: Reversing Fifty Years of Government Security Failure* (1995), p. 50

"Counterintelligence… is often confused with security—that is, merely with protecting secrets and protecting against subversion. Yet whereas the objective of security is to cut and prevent all contacts between hostiles and those who are to be protected the objective of CI is to engage hostile intelligence, control what it knows, and if possible control what it does. In principle, neither security people nor CI people deny the validity of the others approach, but CI people think of security as flatfooted cops, and the latter think of the former as game-playing spooks."

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 26

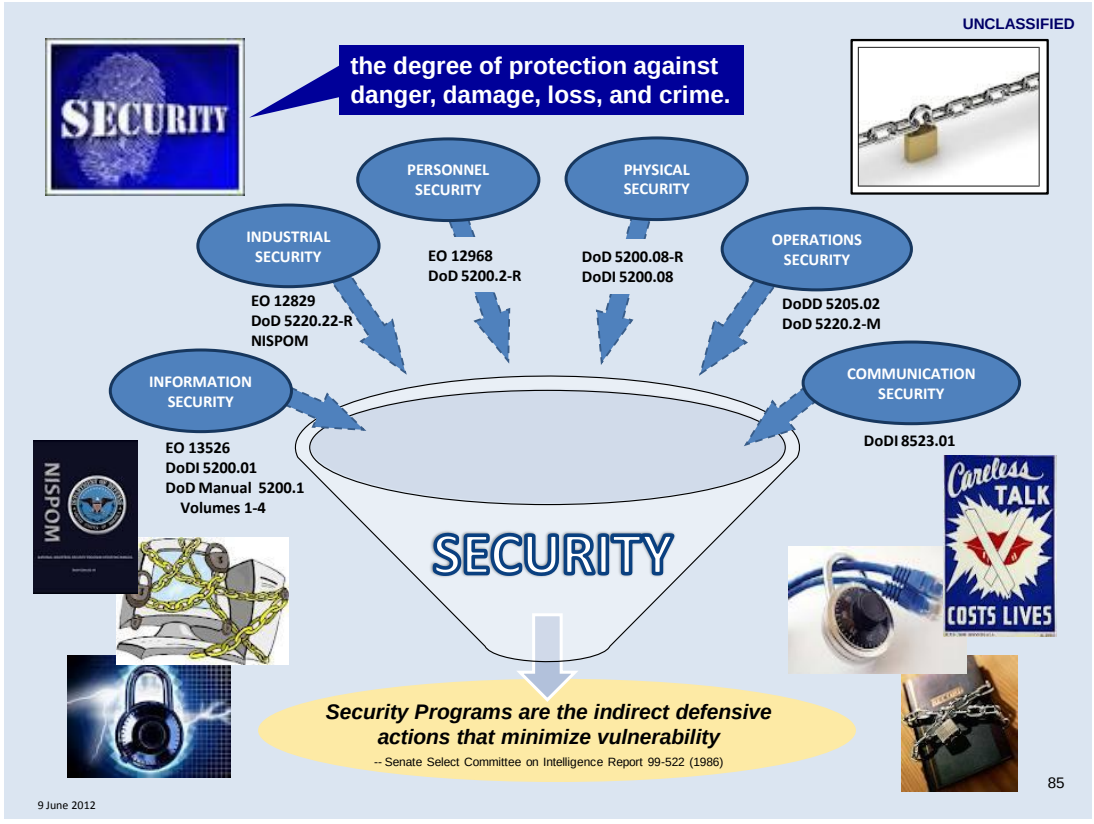
"Security is a dimension of clandestinity in espionage, counterespionage, counterintelligence, adultery, and poker. It is to these activities what style is to a writer, an athlete, or a musician, but it is not itself a work, a game, or a performance. Its purpose is prophylactic: it excludes toxic and infectious organisms and conserves vital fluids."

-- William R. Johnson, "Clandestinity and Current Intelligence." *Studies in Intelligence*, vol 20, no. 3, (Fall 1976), pp. 15-69. Originally classified "Secret / No Foreign Dissem" [declassified].

"CI and security shall be regarded as interdependent and mutually supportive disciplines with shared objectives and responsibilities associated with the protection of secrets and assets."

"Security programs establish appropriate personnel, physical, information, operations, industrial and technical security, safeguards, and countermeasures to protect information and information systems, personnel, operations, resources, technologies, and facilities from threats."

-- ICD 700, Protection of National Intelligence, 7 Jun 2012



"Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness."

-- President Ronald Reagan, NSDD-145, 17 Sep 1984

General functions and responsibilities performed by security professionals, including communications security, counterintelligence awareness, security systems, international programs, operations security, research and technology protection, sensitive compartmented information security, special access program security, and security program policy.

-- DoDI 3305.13, DoD Security Education, Training, and Certification, 13 Feb 2014

Security--Four Basic Principles

According to the Joint Security Commission, security is a dynamic and flexible system guided by four basic principles:

1) Security policies and services must be realistically matched to the threats we face. The processes we use to formulate policies and deliver services must be sufficiently flexible to facilitate their evolution as the threat changes.

2) Security policies and practices must be consistent and coherent across the Defense and Intelligence Communities, thereby reducing inefficiencies and enabling us to allocate scare resources efficiently.

3) Security standards and procedures must result in the fair and equitable treatment of the members of our communities upon whom we rely to guard the nation's security.

4) Security policies, practices, and procedures must provide the security we need at a price we can afford.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, p. 3

Security is a highly decentralized government function. […] Effectively addressing security generates costs that must be balanced against risk and threats. Security, as a discipline, has historically been dominated by "police" type management, processes, and enforcement approaches. Although the police function is still required, today's security vulnerabilities are increasingly technical in nature and related to information technology systems, software, and hardware.

-- WMD Report (31 March 2005), p. 545

Security Classification. A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. (JP 1-02)

There are three categories of security classification:

1) ***Top Secret***--National security information or material that requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

2) ***Secret***--National security information or material that requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

3) ***Confidential***--National security information or material that requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

For additional information see website at: <http://www.archives.gov/isoo/policy-documents/>

Security Classification Guide (SCG). A documentary form of classification guidance issued by an OCA [original classification authority] that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012)

Security Clearance. An administrative determination by competent authority that an individual is eligible, from a security stand-point, for access to classified information. (JP 1-02)

> Within DoD, a security clearance is a determination that a person is eligible under DoD policy for access to classified information. Clearances allow personnel to access classified information categorized into three levels: top secret, secret, and confidential. The damage to national defense and foreign relations that unauthorized disclosure could reasonably be expected to cause ranges from "exceptionally grave damage" for top secret information to "damage" for confidential information.
>
> ———————————
>
> *The security clearance process is designed to determine the trustworthiness of an individual prior to granting him or her access to classified national security information. The process has evolved since the early 1950s, with antecedents dating to World War II.*
>
> *A security clearance is a determination that an individual—whether a direct federal employee or a private contractor performing work for the government—is eligible for access to classified national security information.*
>
> *A security clearance alone does not grant an individual access to specific classified materials. Rather, a security clearance means that an individual is eligible for access. In order to gain access to specific classified materials, an individual should also have a demonstrated "need to know" the classified information for his or her position and policy area responsibilities. In addition, prior to accessing classified information, an individual must sign an appropriate nondisclosure agreement.*
>
> -- CRS Report R43216, *Security Clearance Process: Answers to Frequently Asked Questions*, 9 Sep 2013 *
>
> * Copy available at: <http://www.fas.org/sgp/crs/secrecy/R43216.pdf>

Security Clearance Investigation. An inquiry into an individual's loyalty, character, trustworthiness and reliability to ensure that he or she is eligible for access to national security information. (ONCIX, <http://www.ncix.gov/SEA/reform/secvssuit.php>; accessed 18 Sep 2012) Also see *suitability investigation*.

> "*The Director of National Intelligence shall serve as the **Security Executive Agent**. As the Security Executive Agent the Director of National Intelligence shall direct the oversight of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position made by any agency; shall be responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position."*
>
> – EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, 2 Jul 2008

Security Compromise. The disclosure of classified information to persons not authorized access thereto. (DSS Glossary)

Security Countermeasures (SCM). Actions, devices, procedures, and/or techniques to reduce security risks. (IC Standard 700-1, 4 Apr 2008)

-- Also, those protective activities required to prevent espionage, sabotage, theft, or unauthorized use of classified or controlled information, systems, or material of the Department of Defense. (JP 1-02; and in previous edition JP 2-01.2, dated 13 Jun 2006)

Security Detainee. Those detainees who are not combatants, but who may be under investigation or pose a threat to US forces if released. (Army FM 2-22.3, HUMINT Collector Operations, Sep 2006)

Security Disciplines. Core functions and responsibilities performed by security professionals with a concentration in personnel, physical, information, and industrial security. (DoDI 3305.13, DoD Security Education, Training, and Certification, 13 Feb 2014) Also see *security; security professional*.

Security Environment Threat List. A list of countries with United States Diplomatic Missions that is compiled by the Department of State and updated semi-annually. The listed countries are evaluated based on: transnational terrorism; political violence; human intelligence; technical threats; and criminal threats [and rated via] four threat levels: Critical, High, Medium and Low. (DSS Glossary)

> Four Threat Levels:
>
> ***Critical*** – defined as a definite threat to United States assets based on adversary's capability, intent to attack, and targeting conducted on a recurring basis;
>
> ***High*** – defined as a credible threat to United States assets based on knowledge of an adversary's capability, intent to attack, and related incidents at similar facilities;
>
> ***Medium*** – defined as a potential threat to United States assets based on knowledge of an adversary's desire to compromise the assets and the possibility that the adversary could obtain the capability to attack through a third party who has demonstrated such a capability; and
>
> ***Low*** – defined as little as no threat as a result of the absence of credible evidence of capability, intent, or history of actual or planned attack against United States assets.

Security Executive Agent (SecEA). The Director of National Intelligence shall serve as the Security Executive Agent. (EO 13467, 30 Jun 2008)

> For additional information see Security Executive Agent Directive 1 "Security Executive Agent Authorities and Responsibilities," 13 Mar 2012.
>
> Copy at: <http://www.ncix.gov/SEA/docs/2012-03-13_SEAD-1_Directive.pdf>

Security Incident. A security compromise, infraction, or violation. (DSS Glossary)

Security In-Depth. A concept of security calling for layered and complementary controls sufficient to detect and deter infiltration and exploitation of an organization, its information systems and facilities. (IC Standard 700-1, 4 Apr 2008)

-- Also, a combination of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the installation and/or facility and the ability to delay and respond with force. Examples include the use of perimeter fences, employee and visitor entry and/or exit controls, sensors and intrusion detection systems, closed circuit video monitoring, security patrols during working and non-working hours, or other safeguards that mitigate vulnerabilities. (DTM 09-012, 8 Dec 2009, w/ chg 2 dated 9 Sep 2012)

-- Also, an array of security measures which, considered as a whole, provide a level of security greater that that by any one measure individually. Includes identification checks, perimeter fences, police patrols, motion detectors, and other security measures. (DoD Manual S-5240.09, OFCO Procedures and Security Classification Guide, 13 Jan 2011 w/ change 1 dated 16 Oct 2012)

Security Infraction. A security incident that is not in the best interest of security and does not involve the loss, compromise, or suspected compromise of classified information. (DSS Glossary)

Security Measures: [Actions] taken by the government and intelligence departments and agencies, among others, for protection from espionage, observation, sabotage, annoyance, or surprise. With respect to classified materials, it is the condition which prevents unauthorized persons from having access to official information which is safeguarded in the interests of national defense. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Security Profession. An occupation dedicated to the protection of people, facilities, information, operations, and activities. (DoDI 3305.13, DoD Security Education, Training, and Certification, 13 Feb 2014) Also see *security; security disciplines; security professional*.

Security Professional. An individual who is educated, trained, and experienced in one or more security disciplines and provides advice and expertise to senior officials on the effective and efficient implementation, operation, and administration of the organization's security programs. (DoDI 3305.13, DoD Security Education, Training, and Certification, 13 Feb 2014) Also see *security; security profession*.

Security Service. Entity or component of a foreign government charged with responsibility for counterespionage or internal security functions. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; and CI Community Lexicon)

Sedition. Willfully advocating or teaching the duty or necessity of overthrowing the US government or any political subdivision by force or violence. (JP 1-02; also in previous edition JP 2-01.2, dated 13 Jun 2006)

> Sedition and criminal subversion of military forces are violations of Title 18 USC, §§ 2384-2390 and is a punishable offense under UCMJ Article 94. It is a term of law which refers to overt conduct that is deemed by the legal authority as tending toward insurrection against the established order. It is the crime of creating a revolt, disturbance, or violence against lawful civil authority with the intent to cause its overthrow or destruction. Sedition often includes subversion of a constitution and incitement of discontent (or resistance) to lawful authority. A seditionist is one who engages in or promotes the interests of sedition.
>
> The difference between sedition and treason consists primarily in the subjective ultimate object of the violation to the public peace. Sedition does not consist of levying war against a government nor of adhering to its enemies, giving enemies aid, and giving enemies comfort. Nor does it consist, in most representative democracies, of peaceful protest against a government, nor of attempting to change the government by democratic means (such as direct democracy or constitutional convention).
>
> Sedition is the stirring up of rebellion against the government in power. Treason is the violation of allegiance to one's sovereign or state, giving aid to enemies, or levying war against one's state. Sedition is encouraging one's fellow citizens to rebel against their state, whereas treason is actually betraying one's country by aiding and abetting another state.

Seizure. The taking or dispossession of property from the possessor by an authorized person or the restriction of the freedom of movement of an individual against his or her will by an agent of the Government. (AR 190-20) Also see *search*.

Self-radicalization. Significant steps an individual takes in advocating or adopting an extremist belief system for the purpose of facilitating ideologically-based violence to advance political, religious, or social change. The self-radicalized individual has not been recruited by and has no direct, personal influence or tasking from other violent extremists. The self-radicalized individual may seek out direct or indirect (through the Internet for example) contact with other violent extremists for moral support and to enhance his or her extremist beliefs. (DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 2013) Also see radicalization; violent radicalization.

-- Also, the process whereby people seek out opportunities for involvement in terrorist activity absent a formal involvement in a terrorist group and/or recruitment by others. (DSB Report, *Predicting Violent Behavior*, Aug 2012, citing Horgan's *The Psychology of Terrorism 2nd Edition*, 2012)

-- Also, *self radicalization*: a phenomenon in which individuals become terrorists without joining an established radical group, although they may be influenced by its ideology and message. (DSB Report, *Predicting Violent Behavior*, Aug 2012)

Senate Select Committee on Intelligence (SSCI). Created pursuant to Senate Res. 400, 94th Congress: to oversee and make continuing studies of the intelligence activities and programs of the United States Government, and to submit to the Senate appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs. Provides legislative oversight over US intelligence activities to assure that such activities are in conformity with the Constitution and laws of the United States. (www.intelligence.senate.gov)

> The 1980 Intelligence Oversight Act charged the SSCI and the House Permanent Select Committee on Intelligence (HPSCI) with authorizing the programs of US intelligence agencies and overseeing their activities.
>
> *It is IC policy that IC elements shall, in a timely manner, keep the Congressional intelligence committees fully informed, in writing, of all significant anticipated intelligence activities, significant intelligence failures, significant intelligence activities, and illegal activities.*
>
> -- ICD 112, *Congressional Notification*, 16 Nov 2011
>
> See an interested article entitled "Congressional Oversight of Intelligence: One Perspective," by Mary Sturtevant, Senate Committee Staff, in *American Intelligence Journal*, Summer 1992; copy available on line at: <http://www.fas.org/irp/eprint/sturtevant.html>

Senior Defense Official / Defense Attaché (SDO/DATT). Principal DoD official in a U.S. embassy, as designated by the Secretary of Defense. (DoDD 5105.75, DoD Operations at Defense Embassies, 21 Dec 2007) Also see *Defense Attaché Office*.

> The SDO/DATT is the Chief of Mission's (COM's) principal military advisor on defense and national security issues, the senior diplomatically accredited DoD military officer assigned to a US diplomatic mission, and the single point of contact for all DoD matters involving the embassy or DoD elements assigned to or working from the embassy.
>
> All DoD elements assigned or attached to or operating from U.S. embassies are aligned under the coordinating authority of the SDO/DATT. See DoD Directive 5105.75, DoD Operations at U.S. Embassies.

Sensitive. Requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. May be applied to an agency, installation, person, position, document, material, or activity. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Sensitive Activities [within DoD]. Operations, actions, activities, or programs that are generally handled through special access, compartmented, or other sensitive control mechanisms because of the nature of the target, the area of operation, or other designated aspects. Sensitive activities also include operations, actions, activities, or programs conducted by any DoD Component that, if compromised, could have enduring adverse effects on U.S. foreign policy, DoD activities, or military operations; or cause significant embarrassment to the United States, its allies, or the DoD. (DoDI O-5100.94, Oversight, Coordination, Assessment, and Reporting of DoD Intelligence and Intelligence-Related Sensitive Activities, 27 Sep 2011 w/ change 1 dated 15 Oct 2013)

Sensitive Compartmented Information (SCI). All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the DNI. (National Intelligence: A Consumer's Guide – 2009).

-- Also, classified national intelligence information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the DNI. (DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information, 9 Oct 2008 w/ chg 1)

Sensitive Compartmented Information Facility (SCIF). An accredited area, room, group of rooms, or installation where sensitive compartmented information (SCI) may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, a subset of CNI [Classified National Intelligence] concerning or derived from intelligence sources, methods or analytical processes that is required to be protected within formal access control systems established by the DNI [Director of National Intelligence]. (ICD 703, Protection of Classified National Intelligence, Including Sensitive Compartmented Information, 21 Jun 2013)

-- Also, an accredited area where Sensitive Compartmented Information may be stored, used, discussed, and/or processed. Only those Intelligence Community Agencies with SCIF Accreditation Authority may officially accredit facilities to handle, process, and store SCI materials. (National Intelligence: A Consumer's Guide - 2009).

> For additional information on SCIFs see *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, IC Standard Number 705-1, 17 Sep 2010, and *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information*, IC Standard Number 705-2, 17 Sep 2010.

Sensitive Information. Information that the loss, misuse, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code, but that has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of National defense or foreign policy. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Sensitive Site. A geographically limited area that contains, but is not limited to, adversary information systems, war crimes sites, critical government facilities, and areas suspected of containing high value targets. (JP 1-02 and JP 3-31, Command and Control for Joint Land Operations, 29 Jun 2010)

-- Also, a designated, geographically limited area with special diplomatic, informational, military, and economic sensitivity for the United States. This includes factories with technical data on enemy weapon systems, war crimes sites, critical hostile government facilities, areas suspected of containing persons of high rank in a hostile government or organization, terrorist money-laundering areas, and document storage areas for secret police forces. (Army FM 2-0, Intelligence, 23 Mar 2010)

Sensitive Site Exploitation (SSE). *Within DoD, term rescinded.* See *site exploitation*.

> This term was previously defined in JP 1-02 as: a related series of activities inside a captured sensitive site to exploit personnel documents, electronic data, and material captured at the site, while neutralizing any threat posed by the site or its contents.
>
> Note: Army Tactics, Techniques and Procedures (ATTP) 3-90.15 [FM 3-90.15] (8 Jul 2010) also rescinded *"sensitive site exploitation"* as a doctrinal term.

Sensitive Sources and Methods. A collective term for those persons, organizations, things, conditions, or events that provide intelligence information and those means used in the collection, processing, and production of such information which, if compromised, would be vulnerable to counteraction that could reasonably be expected to reduce their ability to support US intelligence activities. (ICS Glossary)

Sensemaking. A set of philosophical assumptions, substantive propositions, methodological framings, and methods. (*Sensemaking: A Structure for an Intelligence Revolution* by David T. Moore) Also see *sensemaking*. Also see *intelligence sensemaking*.

> Sensemaking goes beyond analysis, a disaggregative process, and also beyond synthesis, which meaningfully integrates factors relevant to an issue. It includes an interpretation of the results of that analysis and synthesis. It is sometimes referred to as an approach to creating situational awareness "in situations of uncertainty."
>
> Copy of *Sensemaking: A Structure for an Intelligence Revolution* by David T. Moore available at <http://ni-u.edu/ni_press/pdf/Sensemaking.pdf>

Serials. Individual items of evidence in a counterintelligence case are known as serials. They may not necessarily reach a standard required for a criminal prosecution but the objective is not necessarily to achieve a public trial and conviction, but to develop an investigation to the point where some advantage can be achieved. While serials may include entirely circumstantial evidence, unsubstantiated allegations, and coincidence, until verified or dismissed through inquiry and research, they remain valid and may stay in a dossier for decades. (Historical Dictionary of Cold War Counterintelligence, 2007)

Shape. The ability to conduct activities to affect the perceptions, will, behavior, and capabilities of partner, competitor, or adversary leaders, military forces, and relevant populations to further U.S. national security or shared global security interests. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Shielded Enclosure. Room or container designed to attenuate electromagnetic radiation, acoustic signals, or emanations. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Short-Range Agent Communication (SRAC). A device that allows agent and [case] officer to communicate clandestinely over a limited distance. (Spycraft)

Signal. A prearranged visual or audio sign that a dead drop has been filled or emptied or that an emergency meeting is needed. (FBI FCI Terms) Also see *signals*.

-- Also, prearranged visual or audio indicator having a designated significance for intelligence personnel involved. For example, to signify that a dead drop has been filled or emptied or to call an emergency or unscheduled personal meeting. (AFOSI Manual 71-142, OFCO, 9 June 2000)

Signal Flags. The IC [Intelligence Community] database containing information used to assist security and counterintelligence professionals conducting National Agency Checks on individuals applying for positions with IC organizations. (IC Standard 700-1, 4 Apr 2008)

Signal Security (SIGSEC). A generic term that includes both communications security and electronics security. (JP 1-02) Also see *security*.

Signal Site. A prearranged fixed location, usually in a public place, on which an agent or intelligence officer can place a predetermined mark in order to alert the other to operational activity. Such a mark may be made by, for example, chalk or a piece of tape. (FBI -- Affidavit: USA vs. Robert Philip Hanssen, 16 Feb 2001)

> *The operational activity signaled may be the fact that a dead drop has been "loaded" and is ready to be "cleared." A call-out signal may be used to trigger a contact between an agent and an intelligence officer.*
>
> – FBI: Affidavit USA vs. Robert Philip Hanssen, 16 Feb 2001)

-- Also, a covert means of communications using a nonalerting signal, such as a chalk mark on a lamppost, to either initiate or terminate a clandestine act, (Spycraft) Also see *signals*.

Signals. Any form of clandestine tradecraft using a system of marks, signs, or codes for signaling between operatives. (CI Centre Glossary) Also see *signal site*.

Signals Intelligence (SIGINT). 1) A category of intelligence comprising either individually or in combination all communications intelligence [COMINT], electronic intelligence [ELINT], and foreign instrumentation signals intelligence [FISINT], however transmitted. 2) Intelligence derived from communications, electronic, and foreign instrumentation signals. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

For DoD policy see DoDI O-3115.07, Signals Intelligence (SIGINT), 15 Sep 2008

-- Also, intelligence gathered from data transmissions [signals intercepts], including Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT). SIGINT includes both raw data [collection] and the analysis of that data to produce intelligence. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, information derived from intercepted communications and electronic and data transmissions. (WMD Report, 31 Mar 2005)

The collection of signals intelligence is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm.

-- PDD-28 Signals Intelligence Activities, 17 Jan 2014

The Intelligence Community refers to the collection and exploitation of signals transmitted from communication systems, radars, and weapon systems as signals intelligence or SIGINT. SIGINT consists of Communications Intelligence (COMINT) – technical and intelligence information derived from intercept of foreign communications; Electronic Intelligence (ELINT) – information collected from systems such as radars and other weapons systems; and Foreign Instrumentation Signals Intelligence (FISINT) – signals detected from weapons under testing and development.

SIGINT is collected in a variety of ways depending on the type of signal targeted. The National Security Agency (NSA) collects the raw SIGINT and then NSA translators, cryptologists, analysts, and other technical experts turn the raw data into something that an all-source analyst can use. Once the NSA has collected, processed, and analyzed SIGINT, it is passed on to CIA and Intelligence Community analysts who use it to complement information from other sources to produce finished intelligence.

The volume and variety of today's signals adds challenges to the timely production of finished intelligence for policymakers. It is a lot of work to track and analyze all the SIGINT collected.

-- www.cia.gov (accessed, 30 Nov 2010)

Signals Intelligence (SIGINT): The interception of signals, whether between people, between machines, or a combination of both. The National Security Agency (NSA) is responsible for collecting, processing, and reporting SIGINT. Within the NSA, the National SIGINT Committee advises the Director, NSA, and the Director of National Intelligence (DNI) on policy issues and manages the SIGINT requirements system.

-- www.intelligence.gov (accessed 13 Aug 2012)

Signals Intelligence (SIGINT)… comprises Communications Intelligence (COMINT) and Electronic Intelligence (ELINT) , and activities pertaining thereto….

-- NSCID 6, Signals Intelligence, 17 Feb 1972 (redacted copy, complete original version is TOP SECRET)
Available at: <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/docs/doc05.pdf>

Signature. A recognizable, distinguishing pattern. See also attack signature or digital signature. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Signatures. [In CI usage,] indicators of potential FISS and ITO [international terrorist organizations] methods of operations, including static surveillance of U.S. forces [and] installations…. (Army FM 2-22.2, CI, Oct 2009)

Sign-of-Life Signal. A signal emitted periodically to signify that an agent is safe. (FBI FCI Terms)

Silver Triangle. The South American region consisting of Peru, Bolivia, and Colombia that is historically known to be a major illegal drug production area. (JP 3-07.4**,** Joint Counterdrug Operations, 13 Jun 2007)

Single Scope Background Investigation (SSBI). Investigation for individuals requiring a top secret clearance or working in a critical sensitive position; normally covers a 5-year period and consists of a subject interview, NAC, credit checks, character references, and employment records checks and references.

-- Also, a personnel security investigation consisting of all the elements prescribed in Standard B of ICPG 704.1. The period of investigation for a SSBI varies, ranging from the immediate preceding 3 years for neighborhood checks to immediately preceding 10 years for local agency checks. (IC Standard 700-1, 4 Apr 2008)

Singleton. Intelligence operations conducted by a single intelligence officer or agent. These operations include intelligence collection, servicing agents, and courier services. (Spy Book)

Site Exploitation. A series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or materiel found during the conduct of operations. (JP 1-02 and JP 3-31, Command and Control for Joint Land Operations, 29 Jun 2010)

-- Also, systematically searching for and collecting information, material, and persons from a designated location and analyzing them to answer information requirements, facilitate subsequent operations, or support criminal prosecution. (Army Tactics, Techniques & Procedures 3-90.15 [FM 3-90.15], Site Exploitation Operations, 8 Jul 2010)

Situation Report (SITREP). A report giving the situation in the area of a reporting unit or formation. (JP 1-02 and JP 3-50, Personnel Recovery)

Situational Awareness. Immediate knowledge of the conditions of the operation, constrained geographically and in time. (Army FM 3-0, Operations, Feb 2008)

Slammer. Project Slammer was an Intelligence Community sponsored study of espionage to determine the motivation of the convicted spies and to learn the methods by which they committed their crimes.

> In 1985 U.S. intelligence agencies embarked on a 10-year benchmark study named Project Slammer, which was focused on interviewing incarcerated spies. It examined “espionage by interviewing and psychologically assessing actual espionage subjects Additionally, persons knowledgeable of subjects were contacted to better understand the subjects' private lives and how they are perceived by others while conducting espionage.” Project Slammer sought to understand of the dynamics of espionage and to incorporate of that enhanced understanding into government and industry security programs.
>
> Project Slammer research endeavor consisted of voluntary interviews with incarcerated spies and subsequent analysis of the data. The effort was essentially de-funded in the early nineties and consequently lost impetus. Nevertheless, there are currently extant several Slammer papers and tapes which are used throughout the security community. Those analyses deal with the essential and multi-faceted motivational patterns underlying espionage.
>
> Although dated, the study's findings remain significant, and the conclusions included: No offender entered a position of trust with the intent to betray; and there were two prevalent sets of personality traits: 1) highly manipulative, dominant, and self-serving; and 2) passive, easily influenced, and lacking self-esteem.

Sleeper. [Tradecraft jargon] an illegal; or agent in a foreign country who does not engage in intelligence activities until told to do so. (FBI FCI Terms)

-- Also, a spy placed in a target area but does not engage in espionage until he or she is activated at a future time. (Spy Book)

-- Also, an illegal or agent residing in a foreign country under orders to engage in no intelligence activities. The inactive status, which can endure for a considerable time, serves to strengthen the legend and permit access by a foreign power to an individual in position to be ready for action under certain circumstances should a specific need arise. (Word of Intelligence, 2nd Edition, 2011)

SMADS. See *Strategic Mission Assurance Data System*.

Social Engineering, An attempt to trick someone into revealing information (e.g., a password) that can be used to attack an enterprise. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

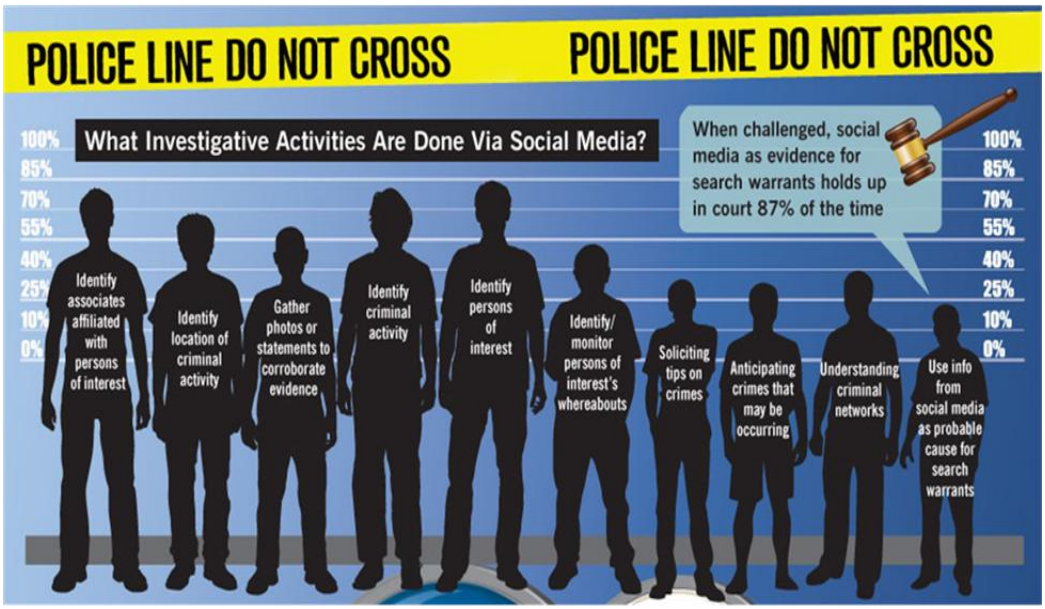
-- Also, the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. (The Ultimate Guide to Social Engineering, undated)

> Copy of "The Ultimate Guide to Social Engineering" available on line at: <http://assets.csoonline.com/documents/cache/pdfs/Social-Engineering-Ultimate-Guide.pdf>

Social Networking. Web-based services that allow individuals to create a public profile, to create a list of users with whom to share connection, and view and cross the connections within the system. (Wikipedia)

> Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as, mobile connectivity, photo/video/sharing and blogging. Social networking sites allow users to share ideas, pictures, posts, activities, events, and interests with people in their network.
>
> The main types of social networking services are those that contain category places (such as former school year or classmates), means to connect with friends (usually with self-description pages), and a recommendation system linked to trust. Popular methods now combine many of these, with American-based services such as *Facebook, Google+, YouTube, LinkedIn, Instagram, Pinterest, Tumblr* and *Twitter* widely used worldwide*; Nexopia in Canada; Badoo, Bebo, VKontakte (Russia), Delphi* (also called *Delphi Forums*), *Draugiem.lv* (mostly in Latvia), *Hi5* (Europe), *Hyves* (mostly in The Netherlands*), iWiW* (mostly in Hungary), *Nasza-Klasa*, *Soup* (mostly in Poland), *Glocals* in Switzerland, *Skyrock, The Sphere, StudiVZ* (mostly in Germany), *Tagged, Tuenti* (mostly in Spain), and *XING* in parts of Europe; *Hi5* and *Orkut* in South America and Central America; *Mxit* in Africa; and *Cyworld, Mixi, Orkut, renren, weibo* and *Wretch* in Asia and the Pacific Islands.
>
> Social networking services are increasingly being used in legal and criminal investigations. Information posted on sites such as *MySpace* and *Facebook* has been used by police (forensic profiling), probation, and university officials to prosecute users of said sites. In some situations, content posted on *MySpace* has been used in court
>
> -- Wikipedia at <http://en.wikipedia.org/wiki/Social_networking> (accessed 11 Mar 2014)
>
> ---
>
> See "Social Media: Establishing Criteria for Law Enforcement Use" by Robert D. Stuart, M.S., in FBI, *Law Enforcement Bulletin*, Feb 2013. Article available at: <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2013/february/social-media-establishing-criteria-for-law-enforcement-use>

"Under Investigation: Social Media Use by Law Enforcement"



-- http://www.lexisnexis.com/government/investigations/ (accessed 11 Mar 2014)

Socio-Cultural Dynamics. Information about the social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment. (DoDD 3600.01, Information Operations, 14 Aug 2006 with Chg 1, 23 May 2011)

Sociocultural Analysis (SCA). The analysis of adversaries and other relevant actors that integrates concepts, knowledge, and understanding of societies, populations, and other groups of people, including their activities, relationships, and perspectives across time and space at varying scales. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Sociocultural Factors. The social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment. (JP 1-02 and JP 2-01.3, Joint Intelligence Preparation of the Operational Environment)

Software Assurance. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle. (DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012)

Source. A person, thing, or activity from whom information or services are obtained. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013, with chg 1 dated 13 Jun 2013) Also see *agent; asset, controlled source; human source; HUMINT source.*

-- Also, 1) A person, thing, or activity from which information is obtained; 2) In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes; or 3) In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that the information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, a person from whom information or services are obtained. (DoDD S-5200.37, Management & Execution of Defense HUMINT, 9 Feb 2009 w/ chg 2)

-- Also, a person, device, system, or activity from which services or information are obtained. (Defense HUMINT Enterprise Manual 3301.02, Vol II Collection Operations, 23 Nov 2010)

-- Also, a person from whom information or services are obtained. (DoDD 3600.01, Information Operations, 14 Aug 2006 with Chg 1, 23 May 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, a document, interview, or other means by which information has been obtained. From an intelligence perspective, sources are individuals (or HUMINT) who collect or possess critical information needed for intelligence analysis. (ODNI, U.S. National Intelligence – An Overview 2011)

Source Directed Requirement (SDR). A HUMINT collection requirement based upon the placement and access of a source to collect and report on a specific person, place, thing, or event. (DHE-M 3301.001, DIA HUMINT Manual, Vol I, 30 Jan 2009 w/ chg 2)

Source Management. The process of registering and monitoring the use of sources involved in counterintelligence and human intelligence operations to protect the security of the operations and avoid conflicts among operational elements. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Source Registry. A source record/catalogue of leads and sources acquired by collectors and centralized for management, coordination and deconfliction of source operations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Source Validation. Vetting to determine if a source is who he/she claims to be, is free of external control, is capable of behaving in a secure manner, and possesses placement and access consistent with tasking. (HDI Lexicon, April 2008) Also see *vetting* and *counterintelligence flags*.

> All DoD human sources are vetted in accordance with National HUMINT Manager Directive 001.08 (HUMINT Source Validation).
>
> For DoD policy see DoDI S-3325.07, *Guidance for the Conduct of DoD Human Source Validation (U),* 22 Jun 2009.

Special Access Program (SAP). A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

-- Also, a program activity which has enhanced security measures and imposes safeguarding and access requirements that exceed those normally required for information at the same level. Information to be protected within the SAP is identified by an SCG [security classification guide]. (DoDI 5205.11, Management, Administration, and Oversight of DoD Special Access Programs, 6 Feb 2013)

-- Also, a sensitive program, approved in writing by a head of agency with original top secret classification authority, that imposes need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

> DoD SAPs are established and maintained only when absolutely necessary to protect the Nation's most sensitive capabilities; information; technologies; operations; and research, development, test and evaluation; or when required by statute pursuant to DoDD 5205.07, SAP Policy, 1 Jul 2010.
>
> _____

Acknowledged – Unacknowledged – Waived

Acknowledged SAP: A SAP whose existence is acknowledged, affirmed, or made known to others, but its specific details (technologies, materials, techniques, etc.,) are classified as specified in the applicable SCG.

Unacknowledged SAP: A SAP having enhanced security measures ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information.

Waived SAP: A SAP for which the Secretary of Defense has waived applicable reporting in accordance with DoD Manual 5200.01 following a determination of adverse effect to national security. An unacknowledged SAP that has more restrictive reporting and access controls than other unacknowledged SAPs.

Interestingly, the Joint Security Commission noted in its 1994 report (*Redefining Security*) that --

"Special Access Programs are used to compensate for the fact that the classification system is not trusted to protect information effectively and does not adequately enforce the 'need to know' principle."

Special Access Program Central Office (SAPCO). The office within a DoD Component or OSD PSA that, when directed, executes, manages, administers, oversees, and maintains records on the SAPs for which it has been assigned CA. Responsibilities may also include developing and implementing policies and procedures for oversight, management, execution, administration, SAP security, IA for SAP IS, and records management of SAPs under their cognizance, as directed. (DoDD 5205.07, Special Access Program Policy, 1 Jul 2010)

The DoD SAPCO is the office charged by the Deputy Secretary of Defense with responsibility as the designated proponent for developing and implementing policies and procedures for DoD SAP execution, management, and administration.

For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), these functions shall be exercised by the Director of National Intelligence.

-- EO 13526, *Classified National Security Information*, 29 Dec 2009

Special Actions. Those functions that due to particular sensitivities, compartmentation, or caveats cannot be conducted in normal staff channels and therefore require extraordinary processes and procedures and may involve the use of sensitive capabilities. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Special Activities. Activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the U .S. Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence U .S. political processes, public opinion, policies, or media and do not include diplomatic activities, the collection and production of intelligence, or related support functions. (IC Standard 700-1, 4 Apr 2008) Also see *covert action.*

-- Also, *within DoD: None -- term rescinded by JP 3-05, Special Operations, 18 Apr 2011.*

As previously defined, it was a term synonymous with "covert action" -- see *covert action.*

Special Agent. *Within DoD: None -- term rescinded by JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011.* See *Counterintelligence Special Agent.*

Previously defined in JP 1-02 as: a person, either United States military or civilian, who is a specialist in military [law enforcement,] security or the collection of intelligence or counterintelligence information.

-- Also, a United States military or civilian who is a specialist in military security or in the collection of intelligence or counterintelligence information. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Special Area Clearance. The required concurrence granted to DoD personnel by the Department of State and the Office of the USD(P) for travel to certain overseas areas designated by the Department of State as special areas. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

Special Collection Service (SCS). [According to open source,*] a joint CIA-NSA signals intelligence collection organization.

-- Also, elite, highly secret U.S. electronic intelligence group that conducts eavesdropping operations in [foreign] countries. The service is controlled by the NSA… [also] CIA experts are often assigned. (Spy Book)

* See Jeffrey T. Richelson, *The US Intelligence Community*, Sixth Edition, 2012, pp. 224-226

"According to a former high-ranking intelligence official, SCS was formed in the late 1970s after competition between the NSA's embassy-based eavesdroppers and the CIA's globe-trotting bugging specialists from its Division D had become counterproductive. While sources differ on how SCS works, some claim its agents never leave their secret embassy warrens where they perform close-quarters electronic eavesdropping, while others say agents operate embassy-based equipment in addition to performing riskier 'black-bag' jobs, or break-ins, for purposes of bugging…."

-- Jason Vest & W. Madsen , "A Most Unusual Collection Agency," *The Village Voice*, 24 Feb - 2 Mar 1999

Special Collection Techniques. Those lawful investigative techniques which are employed by a DoD intelligence component under the rule of the least intrusive means, after a determination has been made that the required information is not publicly available, available with the consent of the person or persons concerned, or available from cooperative sources. (DIA Intelligence Law Handbook, Sep 1995) Also see *rule of the least intrusive means*.

Special collection techniques -- also commonly referred to as "special investigative techniques" within CI channels -- are addressed in DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 Dec 1982,

Procedures 5-10:

* Procedure 5 - Electronic Surveillance
* Procedure 6 - Concealed Monitoring
* Procedure 7 - Physical Searches
* Procedure 8 - Searches and Examination of Mail
* Procedure 9 - Physical Surveillance
* Procedure 10 - Undisclosed Participation in Organizations

Special Communication. See definition provided in DTM 08-019, Establishment of the DoD Special Communication Enterprise Office (SCEO), 11 Jun 2008, marked FOUO.

Special Event. An international or domestic event, contest, activity, or meeting, which by its very nature, or by specific statutory or regulatory authority, may warrant security, safety, and/or other logistical support or assistance from the Department of Defense. (DODD 3025.18, Defense Support of Civil Authorities, 29 Dec 2010)

Special Event Management. Planning and conduct of public events or activities whose character may them attractive targets for terrorist attack. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Special Information Operations (SIO). Information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. (JP 3-13, Information Operations, 13 Feb 2006) Also see *information operations*.

Special Investigative Inquiry (SII). A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination. (IC Standard 700-1, 4 Apr 2008)

Special Investigative Techniques. See *Special Collection Techniques*.

Special Limiting Criteria (SLC). [Term used in document/media exploitation activities]. A narrowly-defined set of criteria intended to restrict access to data that, if compromised, could imperil planned operations, contain evidence of espionage or counterintelligence operations, identify sources and methods, and[/or] contain illegal or inappropriate material. (National Media Exploitation Center)

Special Mission Unit (SMU). A generic term to represent a group of operations and support personnel from designated organizations that is task-organized to perform highly classified activities. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Special Operations (SO). Operations requiring unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk. (JP 3-05, Special Operations, 18 Apr 2011)

Special Operations Activities. Activities that include each of the following insofar as it relates to special operations: direct action, strategic reconnaissance, unconventional warfare, foreign internal defense, civil affairs, psychological operations, counterterrorism, humanitarian assistance, theater search and rescue, and such other activities as may be specified by the president or the Secretary of Defense. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013, with chg 1 dated 13 Jun 2013)

Special Reconnaissance (SR). Reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces. (JP 3-05, Special Operations, 18 Apr 2011)

Special Security Center. The Director of National Intelligence element responsible for developing, coordinating, and overseeing Director of National Intelligence security policies and databases to support Intelligence Community security elements. The Special Security Center interacts with other Intelligence Community security organizations to ensure that Director of National Intelligence equities are considered in the development of national level security policies and procedures. (DSS Security Glossary)

Specified Task. In the context of joint operation planning, a task that is specifically assigned an organization by its higher headquarters. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Spoofing. [Tradecraft jargon] A ploy designed to deceive the observer into believing that an operation has gone bad when, in fact, it has been put into another compartment. (Spy Dust)

-- Also, [cyber usage] deceiving computers or computer users by hiding or faking one's identity. Email spoofing utilizes a sham email address or simulates a genuine email address. IP spoofing hides or masks a computer's IP address. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Spot. [In intelligence usage,] to locate and recruit people demonstrated access to intelligence targets. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

-- Also, to identify for consideration potential sources as candidates for recruitment. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Spot Report. A non-standard DoD HUMINT report (not an IR) used to report on actionable/perishable HUMINT of a non-CRITIC nature. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

-- Also, a concise narrative report of essential information covering events or conditions that may have an immediate and significant effect on current planning and operations that is afforded the most expeditious means of transmission consistent with requisite security. Also called SPOTREP. (Note: In reconnaissance and surveillance usage, spot report is not to be used.) (JP 1-02 and JP 3-09.3, Close Air Support)

For CRITIC reporting see Chapter Three - Specialized Intelligence Reporting, DHE-M 3301.001, Vol I: *Collection Requirement, Reporting, and Evaluation Procedures* (U), 30 Jan 2009, w/ chg 2, dated 1 Feb 2012.

Spotter. In intelligence, an agent or illegal assigned to locate and assess individuals in positions of value to an intelligence service. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; and CI Community Lexicon) Also see *spotter / assessor.*

-- Also, an agent or illegal assigned to locate and assess individuals who might be of value to an intelligence service. (FBI FCI Terms)

Spotter / Assessor. An asset assigned to locate and/or assess individuals of intelligence or operational interest. (HDI Lexicon, April 2008) Also see *spotter; spotter assessor operation*.

Spotter / Assessor Operation. Those actions taken to identify persons who may be in contact with or placed in contact with opposition intelligence and counterintelligence services, and to determine the potential value of these persons as intelligence or counterintelligence sources. (AR 381-47, OFCO, 17 Mar 2006)

Spy. A generic term that refers… to either a professional intelligence officer work works for an intelligence service, or to a foreign source or asset who steals secrets on behalf of that intelligence service. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

-- Also, a person employed by or in the service of a foreign government, either with or without pay, to secure information considered vital to the waging of a shooting or economic war against another country. (Committee on Un-American Activities, U. S. House of Representatives, April 1949)

[T]he spy is the greatest of soldiers. If he is the most detested by the enemy, it is only because he is the most feared.

– King George V (1865-1936)

A U.S, intelligence officer that handles clandestine human sources is normally referred to as a "case officer (C/O)" or "operations officer (OO)." The people that case officers or OOs recruit as penetrations of foreign governments and organizations are their "agents." Agents have access to important information and pass that information secretly to their case officers/OOs.

An army without secret agents is exactly like a man without eyes or ears.

-- Chia Lin, Chinese Strategist of the late eighth century

One spy in the right place is worth 20,000 men in the field.
-- Napoleon

In the circumstances of espionage and betrayal,
one county's heroic spy is another's traitor.
-- Frederick P. Hitz, Former Inspector General of the CIA (1990 - 1998)

"What do you think spies are: priests, saints, and martyrs?
They're a squalid procession of vain fools, traitors too, yes;
pansies, sadists and drunkards, people who play
cowboys and Indians to brighten their rotten lives…"
-- Alec Leamas, the protagonist in LeCarre's *The Spy Who Came in From the Cold*.

Spy Dust (also called METKA). Chemical marking compound developed by the KGB to keep tabs on the activities of a target officer. The compound is made of nitrophenyl pentadien (NPPD) and luminol. (Spy Dust)

Spying. Under Article 106, UCMJ, in time of war, the act of clandestinely or under false pretences, collecting or attempting to collect, information with the intent to convey it to a hostile party. (AR 381-20, Army CI Program, 25 May 2010)

Like war, spying is dirty business. Shed of its alleged glory, a soldier's job is to kill.
Peel away the claptrap of espionage and the spy's job is to betray trust.
-- William Hood, *Mole* (1993)

Spying is a major weapon in the state's exercise of power, according to Machiavelli. In his "Art of War.' He provides amazingly modern and sophisticated instructions on how to prevent spying by the enemy (counterintelligence), how to deceive the enemy (covert action), and how to learn its intentions (espionage).*
-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006), p. 23
* Niccolo Machiavelli (1469-1527), Florentine statesman and patriot.

Spyware. Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a wide range of unwanted programs that exploit infected computers for commercial gain. They can deliver unsolicited pop-up advertisements, steal personal information (including financial information such as credit card numbers), monitor web-browsing activity for marketing purposes, or route HTTP requests to advertising sites. (McAfee.com; accessed 15 Nov 2010)

Stability Operations. An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Staff Judge Advocate (SJA). A judge advocate so designated in the Army, Air Force, or Marine Corps, and the principal legal advisor of a Navy, Coast Guard, or joint force command who is a judge advocate. (JP 1-04, Legal Support to Military Operations, 17 Aug 2011)

Stake Out. Stationary surveillance of a person, site, or facility. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, stakeout: a surveillance point or location that has been employed (or laid out) with the benefit of prior planning. Usually meant to be occupied for an extended period of time. (Words of Intelligence, 2nd Edition, 2011)

Standard Operating Procedure (SOP). A set of instructions covering those features of operations which lend themselves to a definite or standardized procedure without loss of effectiveness. The procedure is applicable unless ordered otherwise. (JP 1-02 and JP 3-31,Command and Control for Joint Land Operations, 29 June 2010)

Star-Burst Maneuver. A countersurveillance ploy in which more than one target car or target officer is being followed and they suddenly go in different directions, forcing the surveillance team to make instant choices about whom to follow. (CI Centre Glossary)

Statement Analysis (also called Scientific Content Analysis or SCAN and Investigative Discourse Analysis). A technique for analyzing the words people use. Proponents claim this technique can be used to detect concealed information, missing information, and whether the information that person has provided is true or false. (Wikipedia, accessed 5 Mar 2014)

Station. A CIA operational center overseas… usually, but not always, located under cover in a U.S. official installation. The senior officer in charge of a station is known as the chief of station, or COS. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Status of Forces Agreement (SOFA). An agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials. (JP 1-02 and JP 3-16, Multinational Operations, 7 Mar 2007)

-- Also, an accord, either bilateral or multilateral, that defines the legal position of a visiting military force deployed in the territory of a friendly state, usually delineating matters affecting the relationship between the military force and the civilian authorities and population. (AR 381-20, Army CI Program, 25 May 2010)

Stay Behind [aka sleeper]. Agent or agent organization established in a given country to be activated in the event of hostile overrun or other circumstances under which normal access would be denied. (JP 1-02)

Steganography. The art, science, and practice of communicating in a way that hides the existence of the communication. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, the process of hiding information by embedding messages within other, seemingly harmless messages. The process works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. (US Army TRADOC DCSINT Handbook 1.02, 15 Aug 2007)

-- Also, the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. (Wikipedia; accessed 4 April 2011)

> *Steganography (from the Greek root "staganos," meaning covered or secret), or stego, is the technique of hiding data in a host file. […] Simply put, stego is hiding* a covert message within another file so that only the sender and receiver can access it.
>
> -- Eric Cole, "Steganography: More than Meets the Eye, " in *Information Security*, November 2006 (pp. 32-37)

Steganography is the process of secreting data in an image. Moscow Center uses steganographic software that is not commercially available. The software package permits the SVR clandestinely to insert encrypted data in images that are located on publicly-available websites without the data being visible. The encrypted data can be removed from the image, and then decrypted, using SVR-provided software. Similarly, SVR-provided software can also be used to encrypt data, and then clandestinely to embed the data in images on publicly-available websites.

-- FBI Affidavit, 25 June 2010

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

With the advent of digital media, steganography has come to include the hiding of digital information within digital files. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

-- Wikipedia (accessed 4 April 2011)

For additional information also see -- <http://www.steganographypro.com/> and <http://www.citi.umich.edu/u/provos/papers/practical.pdf>

Sterilize. To remove from material to be used in covert and clandestine actions any marks or devices which can identify it as originating with the sponsoring organization or nation. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Strategic Communication. Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. (JP 1-02)

Strategic Debriefing. Debriefing activity conducted to collect information or to verify previously collected information in response to national or theater level collection priorities. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; and Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

Sources for strategic debriefing operations include but are not limited to émigrés, refugees, displaced persons, defectors, and selected U.S. personnel.

Strategic Intelligence. Intelligence required for the formation of policy and military plans at national and international levels. Strategic intelligence and tactical intelligence differ primarily in level of application, but may also vary in terms of scope and detail. (JP 1-02) Also see *intelligence; operational intelligence; tactical intelligence.*

Sherman Kent defined *strategic intelligence* as “high-level foreign positive intelligence.”

Strategic Intelligence Interrogation. An intelligence interrogation of any person who is in the custody or under the effective control of the DoD or under detention in a DoD facility, conducted at a theater-level detention facility. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013) Also see *intelligence interrogation*.

Strategic Level of War. The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, and then develops and uses national resources to achieve these objectives. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see also *operational level of war; tactical level of war.*

Strategic Mission Assurance Data System (SMADS). A classified geospatially enabled Critical Infrastructure database with the capability to analyze potential national, strategic, and operational impacts resulting from the loss or disruption of Critical Infrastructure and Key Resources (CIKR).

> Strongly recommended that all DoD CI personnel providing CI support to DCIP obtain an SMADS account.
>
> SMADS is a restricted database accessible on SIPRNet at: <https://smads.stratcom.smil.mil> Access is only granted to end-users who have a valid user account (requires valid need-to-know). Permissions are granted based upon a user's mission and associated responsibilities.
>
> SMADS is managed and maintained by the U.S Strategic Command (USTRATCOM) Mission Assurance Division (MAD). It is the current Joint Staff program of record for Critical Infrastructure and Key Resources (CIKR).
>
> Refer to the *SMADS User Manual* which serves as a general reference for end-users; it provides a step-by-step guide to performing web-enabled database tasks, while incorporating some DCIP program information to help facilitate the completion of these tasks.
>
> For other DCIP tools see web site at: <http://dcip.dtic.mil/DCIPtools.html>

Strategy. A prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

-- *Military Strategy*. The art and science of employing the armed forces of a nation to secure the objectives of national policy by the application of force or the threat of force. (JP 1-02)

-- *National Military Strategy*. The art and science of distributing and applying military power to attain national objectives in peace and war; also called NMS. (JP 1-02)

-- *National Strategy*. The art and science of developing and using the diplomatic, economic, and informational powers of a nation, together with its armed forces, during peace and war to secure national objectives; also called national security strategy or grand strategy. (JP 1-02)

Structured Analysis. A distinct form of intelligence analysis methodology that provides a step-by-step process for analyzing the kinds of incomplete, ambiguous, and sometimes deceptive information that analysts must deal with.

> Structured analysis is a mechanism by which internal thought processes are externalized in a systematic and transparent manner so that they can be shared, built on, and easily critiqued by others. Structured analysis helps analysts ensure that their analytical framework—the foundation upon which they form their analytical judgments—is as solid as possible.
>
> For in-depth information on structured analysis see Richards J. Heuer, Jr. and Randolph H. Pherson, *Structured Analytical Techniques for Intelligence Analysis* (Washington, DC; CQ Press, 2011).

Subject. Person, place, or thing observed or under investigation. (AFOSI Manual 71-142, OFCO, 9 Jun 2000) Also see *suspect.*

-- Also, a person about whom probable cause exists to believe that the person committed a particular criminal offense. (AR 195-2, Criminal Investigation Activities, 15 May 2009)

Subject Interview. Interview with the subject of an investigation; it may be non-custodial or custodial.

> *Interviews of subjects of CI investigations are conducted to afford subjects the opportunity to refute, explain, clarify or mitigate allegations of espionage, terrorism, and other acts that may constitute threats to national security.*
> -- AR 381-20, *Army CI Program*, 25 May 2010

Subversion. Actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority. (JP 1-02 and JP 3-24, Counterinsurgency, 22 Nov 2013) Also see *subversive activity*.

-- Also, actions designed to undermine the military, economic, political, psychological, or moral strength of a nation or entity. It can also apply to an undermining of a person's loyalty to a government or entity. (Senate Report 95-755, Book I – Glossary, 26 Apr 1976)

-- Also, actively encouraging military or civilian personnel to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, or discipline of the US military forces. Lending aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of the U.S. Government. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, the crime of creating a revolt, disturbance, or violence against lawful civil authority with the intent to cause its overthrow or destruction. (Dictionary.com)

> Subversion refers to an attempt to overthrow structures of authority, including the state. It is an overturning or uprooting. Subversive activity is the lending of aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of incumbent governments by force and violence. All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage are placed in the category of subversive activity.
>
> ---
>
> *In the context of DoD investigative policy, subversion refers only to such conduct as is forbidden by the laws of the United States. Specifically, this is limited to information concerning the activities of individuals or groups that involve or will involve the violation of Federal law, for the purpose of:*
> *1) Overthrowing the Government of the United States or the government of a State; and*
> *2) Substantially impairing for the purpose of influencing U.S. Government policies or decisions.*
> -- DoD 5200.2-R, *Personnel Security Program*, Jan 1987 (w. chg 3), p.22

Subversion of Department of Defense Personnel. Actions designed to undermine the loyalty, morale, or discipline of DoD military and civilian personnel. (JP 1-02)

-- Also, [previously defined in DoDI 5240.06, 7 Aug 2004] an act or acts inciting military or civilian personnel of the DoD to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, [or] discipline, of the Military Forces of the United States.

> Criminal subversion of military forces is a violation of Title 18 USC, §§ 2384-2390.

Subversive Activity. Anyone lending aid, comfort, and moral support to individuals, groups or organizations that advocate the overthrow of incumbent governments by force and violence is subversive and is engaged in subversive activity. All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage will be placed in the category of subversive activity. (JP 1-02)

Suitability Investigation. An inquiry into a person's identifiable character traits and conduct sufficient to decide whether an individual's employment or continued employment would or would not protect the integrity or promote the efficiency of the service. (ONCIX, http://www.ncix.gov/SEA/reform/secvssuit.php; accessed 18 Sep 2012) Also see *security clearance investigation*.

> "*The Director of the Office of Personnel Management shall serve as the Suitability Executive Agent. As the Suitability Executive Agent, the Director of the Office of Personnel Management will be responsible for developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of suitability and eligibility for logical and physical access.*"
> -- EO 13467 (30 June 2008)

Superencryption. Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, on-line circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Supply Chain. The linked activities associated with providing materiel from a raw materiel stage to an end user as a finished product. (JP 1-02 and JP 4-09, Distribution Operations, 5 Feb 2010) Also see *adversarial supply chain operations, supply chain attack, supply chain risk, supply chain risk management*.

-- Also, the linked activities associated with providing materiel from a raw materiel stage to an end user as a finished product or system. Including design, manufacturing, production, packaging, handling, storage, transport, mission operation, maintenance, and disposal. (DoDI 4140.67, DoD Counterfeit Prevention Policy, 26 Apr 2013)

-- Also, organizations, people, technology, information and associated resources involved in moving a product or service from supplier to customer. (National Counterintelligence Strategy of the United States of America, 2012)

-- Also, a system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

> *Supply Chain: 1) Starting with unprocessed raw materials and ending with the final customer using the finished goods, the supply chain links many companies together; 2) the material and informational interchanges in the logistical process stretching from acquisition of raw materials to delivery of finished products to the end user. All vendors, service providers, and customers are links in the supply chain.*
> -- CSCMP Glossary, Feb 2010, p. 179
>
> See *Supply Chain Management Terms and Glossary*, Feb 2010. Available online at: <http://cscmp.org/sites/default/files/user_uploads/resources/downloads/glossary.pdf>

Supply Chain Attack. Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Supply Chain Risk. The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, otherwise degrade the function, use or operation of the item or system. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 w/ chg 1 and DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012) Also see *supply chain risk management; supply chain risk mitigation; supply chain vulnerabilities.*

-- Also, the risk that adversaries will insert malicious code into or otherwise subvert the design, manufacturing, production, distribution, installation, or maintenance of ICT components that may be used in DoD systems to gain unauthorized access to data, to alter data, to disrupt operations, or to interrupt communications. (DTM 09-016, SCRM to Improve the Integrity of Components Used in DoD Systems, 25 Mar 2010 w/ chg 3 dated 23 Mar 2012)

"*The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system.*"

-- The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, (Section 806)

The increased dependence of the United States on global inputs in the manufacturing and service sectors, especially relating to information technology, opens the door to greater supply-chain vulnerabilities. As international companies and foreign individuals play a greater role in the information-technology supply chain, the specter of persistent, stealthy subversion is raised—particularly by foreign intelligence and military services, as well as international terrorists and criminal groups.

– ONCIX website <http://www.ncix.gov/sections/carc/index.html>

Within DoD, see DoDI 52400.44 (Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012) which establishes policy to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components by foreign intelligence, terrorists, or other hostile elements.

DoD computing systems, are a constant target of foreign exploitation. A 2007 Defense Science Board report noted that the software industry has become increasingly and irrevocably global. Much of the code is now written outside the United States, some in countries that may have interests inimical to those of the United States. The combination of DoD's profound and growing dependence upon software and the expanding opportunity for adversaries to introduce malicious code into this software has led to a growing risk to the Nation's defense.

See report of the *Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software*, Sep 2007.

"A computer chip with a hidden, malicious flaw could sabotage a weapons system. And the compromised hardware is almost impossible to detect…. A chip might even be embedded with a 'kill switch,' allowing the weapon to be disabled by remote control. …only about 2 percent of the integrated circuits purchased every year by the military are manufactured in the United States."

-- David Wise, *Tiger Trap: America's Secret Spy War with China* (2011), p. 233

"The Defense supply chain is at risk: More than two-thirds of electronics in U.S. advanced fighter aircraft are fabricated in off-shore foundries."

-- Dr. Kaigham J. Gabriel, Acting Director DARPA, DoD
March 2012 – Testimony before the Senate Armed Services Committee hearing on Emerging Threats and Capabilities

---

"Interdependence of information technologies and integration of foreign technology in US information technology, telecommunications, and energy sectors will increase the potential scope and impact of foreign intelligence and security services' supply chain operations. The likely continued consolidation of infrastructure suppliers—which means that critical infrastructures and networks will be built from a more limited set of provider and equipment options—will also increase the scope and impact of potential supply chain subversions."

-- James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013

Counterfeit Electronic Parts in the DoD Supply Chain…

"In March 2001, the Senate Armed Services Committee initiated an investigation into counterfeit electronic parts in the Department of Defense (DOD) supply chain. The investigation uncovered overwhelming evidence of large numbers of counterfeit parts making their way into critical defense systems. … The investigation… found overwhelming evidence that companies in China are the primary source of counterfeit electronic parts in the defense supply chain."

-- Armed Services U.S. Senate Report 112-167, 21 May 2012; copy of full report at: <http://www.armed-services.senate.gov/Publications/Counterfeit%20Electronic%20Parts.pdf>

Supply Chain Risk Management (SCRM). The management of supply chain risk whether presented by the supplier, the supplied product and its sub-components, or the supply chain (e.g., packaging, handling, storage, and transport). (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013) Also see *adversarial supply chain operations*, *supply chain attack*, *supply chain risk; supply chain risk mitigation; supply chain vulnerabilities.*

-- Also, the systematic identification, assessment, and quantification of potential supply chain disruptions with the objective to control exposure to risk or reduce its negative impact on supply chain performance.(DoDI 4140.01, DoD Supply Chain Materiel Management Policy, 14 Dec 2011)

-- Also, a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal). (DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012)

-- Also, management of risk that an adversary may sabotage, malicious[ly] introduce unwanted functions, or otherwise subvert the design, manufacturing, production, distribution, installation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, otherwise degrade the function, use or operation of the item or system. (DoD FCIP Strategy FY 2013-2017)

-- Also, [within the Intelligence Community] the management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain. It addresses the activities of foreign intelligence entities and other adversarial attempts aimed at compromising the IC supply chain, which may include the introduction of counterfeit or malicious items into the IC supply chain. (ICD 731, Supply Chain Risk Management, 7 Dec 2013)

Supply chain risk management encompasses many disciplines and requires participation from subject matter experts in acquisition, counterintelligence, information assurance, logistics, program offices, analysis, security, and other relevant functions as necessary.

-- ICD 731, Supply Chain Risk Management, 7 Dec 2013

The President's Comprehensive National Cybersecurity Initiative (CNCI) 11 directs the implementation of SCRM in information and communications technology (ICT) acquisition.

Various SCRM References:

National Strategy for Global Supply Chain Security, White House, Jan 2012; copy available at www.whitehouse.gov

Committee on National Security Systems Directive (CNSSD) No. 505, *Supply Chain Risk Management* (U), 7 Mar 2012; available at www.cnss.gov

For SCRM policy within the IC see Intelligence Community Directive (ICD) 701, *Supply Chain Risk Management*, 7 Dec 2013.

"Supply Chain Risk Management Awareness" by J. Filsinger, B. Fast, D. Wolf, et al; copy available at: <http://www.afcea.org/committees/cyber/documents/Supplychain.pdf>

Supply Chain Risk Mitigation. A process to ensure software and hardware commodity items are not compromised by malicious actions that disrupt or endanger military operations or provided an entry point for gaining access or control of DoD systems. (DoD Strategy for Operating in Cyberspace, May 2011) Also see *supply chain risk; supply chain risk management; supply chain risk vulnerabilities.*

> ***Manage Supply Risk*** *– Identify, assess, and prioritize efforts to manage risk by utilizing layered defenses, and adapting our security posture according to the changing security and operational environment.*
>
> -- White House, *National Startegy for Global Supply Chain Security*, Jan 2012, p.1

Supply Chain Vulnerabilities. An assessment of the supply chain related to CPI [critical program information] to determine if an adversary has the capability and intent to affect it in a manner that compromises the military effectiveness of the given platform, weapon system, or network. (DoDI 5200.39, CPI within the DoD,16 Jul 2008 with change 1 dated 28 Dec 2010) Also see *supply chain risk; supply chain risk mitigation; supply chain risk management*.

Supplier Assurance. Evidence demonstrating the level of confidence that a supplier is free from vulnerabilities. (DoDI 5200.39, CPI within the DoD,16 Jul 2008 with change 1 dated 28 Dec 2010)

Support Agent. An agent recruited to do support work, such as finding and living in safehouses, serving as a courier, or any of the other activities required to support a spy in place. In many cases, this support agent is a local citizen of the country in which the CIA operates. (A Spy's Journey)

Support Asset. An asset who acquires, maintains, and/or provides services. (HDI Lexicon, April 2008)

Supported Commander. 1) The commander having primary responsibility for all aspects of a task assigned by the Joint Strategic Capabilities Plan or other joint operation planning authority. 2) In the context of joint operation planning, the commander who prepares operation plans or operation orders in response to requirements of the Chairman of the Joint Chiefs of Staff. 3) In the context of a support command relationship, the commander who receives assistance from another commander's force or capabilities, and who is responsible for ensuring that the supporting commander understands the assistance required. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *support; supporting commander*.

Supporting Commander. 1) A commander who provides augmentation forces or other support to a supported commander or who develops a supporting plan. Includes the designated combatant commands and Defense agencies as appropriate. 2) In the context of a support command relationship, the commander who aids, protects, complements, or sustains another commander's force, and who is responsible for providing the assistance required by the supported commander. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *support; supported commander*.

Suspect Counterfeit. Materiel, items, or products in which there is an indication by visual inspection, testing, or other information that it may meet the definition of counterfeit materiel provided herein. (DoDI 4140.67, DoD Counterfeit Prevention Policy, 26 Apr 2013) Also see *counterfeit material*.

Surreptitious Entry. Entry by stealth. (Spycraft)

-- Also, unauthorized entry in a manner which leaves no readily discernible evidence. (DSS Glossary and AR 381-14, Technical Counterintelligence, 30 Sep 2002)

-- Also, any entry into a guarded or locked area or container and a departure therefrom without leaving a trace that such entry was made. (FM 30-17, Counterintelligence Operations, Jan 1972)

Surreptitious Entry Unit. Unit in OTS [CIA's Office of Technical Service] whose specialty was opening locks and gaining access to enemy installations for the purpose of supporting bugging operations. (Spy Dust)

Surveillance. The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *counter surveillance*, *electronic surveillance*, *physical surveillance, surveillance detection*.

> ***"Surveillance is a valuable investigative tool [emphasis added]…."***
>
> *"Investigators always should assume that subjects engaged in operational, terrorist, or criminal activity will attempt to detect surveillance by employing a variety of methods and techniques…. During surveillances, participants must remain vigilant and alert to the possibility of countersurveillance techniques being employed against them."*
>
> -- John T. Nason, "Conducting Surveillance Operations" in *FBI Law Enforcement Bulletin*, May 2004

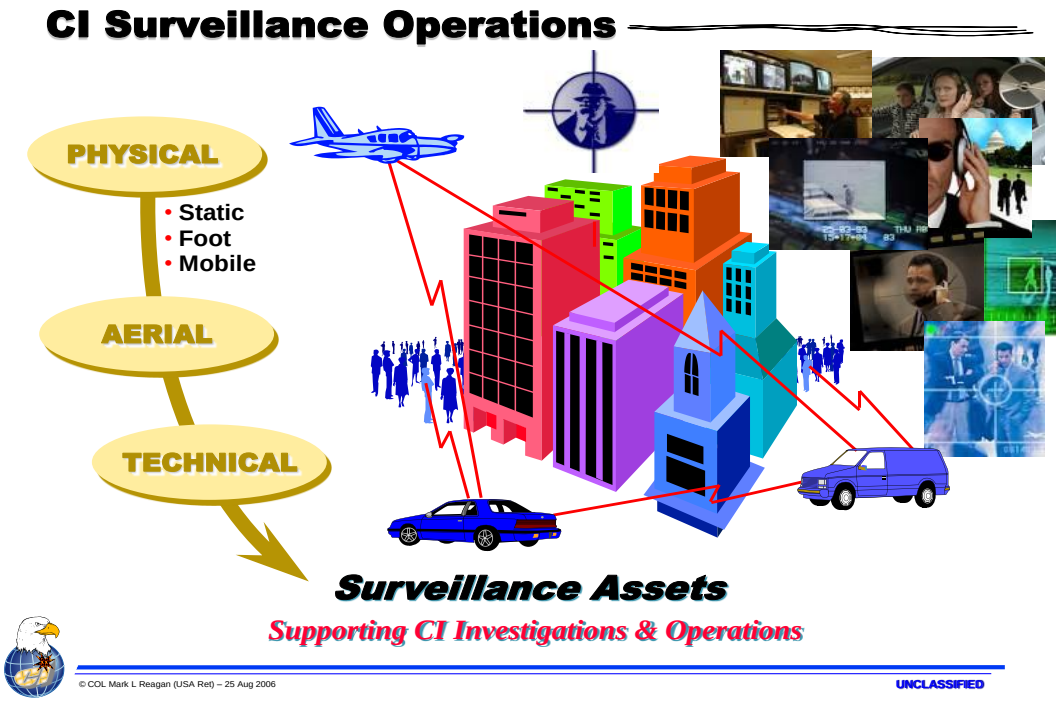
-- Also, systematic observation of a target. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, the continuous watching or listening (overtly or covertly) of people, vehicles, places, or objects to obtain information concerning the activities and identities of individuals. (Peter Jenkins, *Surveillance Tradecraft: The Professional's Guide to Covert Surveillance Training*, 2010)

-- Also, the tradecraft of undetected observation. Surveillance can be physical, electronic, or acoustic. It may include audio or photographic observation and includes mail opening. (A Spy's Journey)

-- Also, actively but unobtrusively observing a subject to gather information about their activities and whereabouts. (Webster's New World Law Dictionary, 2010)

-- Also [as used within DoD concerning force protection], monitoring the activity of DoD personnel, facilities, processes, or systems including showing unusual interest in a facility, infrastructure, or personnel (e.g., observations through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit. (DTM 08-007, DoD Force Protection Threat Information, 22 Jul 2008)



Surveillance, by definition, is intrusion into the affairs of other people.
-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

The word surveillance comes from the French *surveiller*, to watch over. The term is often used for all forms of observation or monitoring, not just visual observation.

In order to be effective, surveillance must go unnoticed and be undetected.

Surveillance can be used from a static point, on foot, from vehicle or by using technical devices. In most cases a combination of all four are used, with targets even often taking public transport and even attempting to detect or avoid surveillance.
-- Peter Jenkins in an introduction to *Surveillance Tradecraft* (2010)

Surveillance, physical: term for the universal tradecraft of undetected observation conducted by humans versus technical means.

Surveillance, technical: generic term for surveillance using various forms of visual, auditory and electronic aids in covering a designated target.

Surveillance, close: tradecraft jargon term for surveillance maintained where the prevention of loss of the subject is paramount.

Surveillance, discreet: tradecraft jargon term for surveillance maintained on a "loose" basis, the prevention of detection being paramount, even to the loss of the subject being tailed. Generally, the guiding rule is to discontinue surveillance rather than risk actions which make the subject aware of the surveillance.

Surveillance, fixed: tradecraft jargon term for a stationary or static surveillance. Also *stakeout*, tradecraft jargon for the static surveillance of a given target.

Surveillance, foot: tradecraft jargon term for, as the words imply, a surveillance conducted on foot.

Surveillance, mobile: tradecraft jargon term for surveillance conducted with the use of various mobile platforms, e.g., vehicles, aircraft, boats, etc.
-- Adapted from *The CIA's Insider's Dictionary* by Leo D. Carl (1996)

Surveillance… must be executed with maximum care lest its target become aware of it.
-- Allen W. Dulles, *The Craft of Intelligence* (2006), p. 124

Surveillance Detection. Measures taken to detect and/or verify whether an individual, vehicle, or location is under surveillance. (DoDI S-5240.15, FPRG, 20 Oct 2010 with change 1 dated 16 Oct 2013) Also see *counter surveillance*, *surveillance*.

-- Measures taken to determine if an individual is under surveillance. (HDI Lexicon, April 2008)

-- Also, self-initiated actions taken by a target/subject to identify surveillance. Conducted by taking advantage of screen and flow, couple with detailed route selection, and noting possible surveillance against time and distance relationships. (CI Community Lexicon)

Surveillance Detection Route (SDR). A carefully crafted route, of varying lengths and complexity depending on the operational environment, used by a case officer and/or agent to get to a meeting site, and after leaving the meeting site, [to] determine that the case officer and agent are not under surveillance before going to and after the ops meeting. (National HUMINT Glossary)

-- Also, a preplanned route used to determine if an individual is under surveillance. (HDI Lexicon, April 2008)

-- Also, a planned route taken by an agent or handler prior to conducting a clandestine act… designed to identify or elude surveillance. (Spycraft)

-- Also, *surveillance detection run*; a route designed to erode or flush out surveillance without alerting them to an operative's purpose. (CI Centre Glossary)

> *Professional case officers of all services, conduct lengthy SDRs before engaging in operational acts. A good SDR gives a case officer the opportunity to flush out surveillance if it is there and to make a determination of his or her surveillance status. The CIA jargon for completing an SDR and verifying without any doubt that surveillance is not there is "getting black."*
>
> -- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)
>
> ---
>
> *Case officers posted to Moscow station underwent rigorous training in "denied area tradecraft"… The primary discipline was the surveillance detection route (SDR). Case officers moved about on long and circuitous routes planned in advance while searching for KGB "tails." If they detected surveillance, they aborted their missions. If no surveillance was detected, they would "go black" for brief periods and perform operational acts.*
>
> -- Benjamin B. Fischer, "Spy Dust and Ghost Surveillance: How the KGB Spooked the CIA and Hid Aldrich Ames in Plain Sight," *International Journal of Intelligence and Counterintelligence*, Vol 24 No 2 (Summer 2011), p. 275
>
> ---
>
> See a brief discussion of "Surveillance Detection Runs" in an excellent article by Barry G. Royden, CIA, entitled "Tolkachev, A Worthy Successor to Penkovsky: An Exceptional Espionage Operation" originally classified SECRET and published in CIA's *Studies In Intelligence*, Vol. 41, No. 4. 1997. Later declassified and published in *Studies In Intelligence*, Vol 47, No. 3, 2003, Unclassified Edition; available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article02.html>

Surveillance Device. A piece of equipment or mechanism used to gain unauthorized access to and removal of information. (DoDI 5240.05, TSCM, 3 Apr 2014)

Suspect. A person about whom some credible information exists to believe that the person committed a particular criminal offense. (AR 195-2, Criminal Investigation Activities, 15 May 2009) Also see *subject*.

Susceptibility. The inherent capacity of an asset to be affected by one or more threats or Hazards. (DoDI 3020.45, DCIP Management, 21 Apr 2008)

Suspension of Access. The temporary withdrawal of a person's eligibility for access to classified information. Access is suspended when information becomes known that casts doubt on whether continued access is consistent with national security interests. (AR 380-67, Personnel Security Program, 24 Jan 2014)

Suspicious Activity. Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. (ISE-FS-200 v1.5 cited in DoDI 2000.26, SAR, 1 Nov 2011) See *suspicious activity report (SAR).*

Suspicious Activity Report (SAR). Official documentation of behavior that may be indicative of preoperational planning related to terrorism or criminal intentions. (DoDI 2000.12, DoD AT Program, 1 Mar 2013, w/ change 1 dated 9 Sep 2013)

-- Also, official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. (ISE-FS-200 v1.5 cited in DoDI 2000.26, SAR, 1 Nov 2011) See *suspicious activity*.

> **eGuardian** -- the FBI's law enforcement-centric threat reporting system -- rapidly disseminates SARs dealing with information regarding a potential threat or suspicious activity throughout the national law enforcement community to include DoD.

For DoD policy see DoDI 2000.26, *Suspicious Activity Reporting*, 1 Nov 2011.

Access to the eGuardian system is via Law Enforcement Online (LEO). Only DoD law enforcement personnel or analysts within DoD law enforcement organizations will enter SARs into the eGuardian system.

Categories of Suspicious Activity (see encl 4, DoDI 2000.26): Acquisition of Expertise; Breach or Attempted Intrusion; Eliciting Information; Expressed or Implied Threat; Flyover or Landing, Materials Acquisition or Storage; Misrepresentation; Recruiting; Sabotage, Tampering, or Vandalism; Surveillance; Testing of Security; Theft, Loss, or Diversion; Weapons Discovery; and Unexplained Absences of International Military Students.

Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting Version 1.5 (ISE-FS-200 v1.5) available on line at: <http://www.ise.gov/sites/default/files/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf>

Suspicious Contact. Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country. (DSS Glossary)

Swallow. A female operative who uses sex as a tool. (Spy Dust)

The swallow's mission is to engage in sexual activity with the targeted person and gather the intelligence either through pillow talk or blackmail. In order to be able to blackmail the targeted person into disclosing secrets, the sexual activity usually takes place in a prearranged room or residence equipped with hidden cameras and recording devices.

-- *Encyclopedia of the Central Intelligence Agency* (2003)

A male operative who uses sex as a tool is referred to as a "Raven."

For additional open source information see David Lewis, *Sexpionage: The Exploitation of Sex by Soviet Intelligence* (1976).

Sweep. [Jargon] To electronically and/or physically examine a room or area in order to detect any clandestine devices; a search for "bugs," i.e., concealed electronic listening devices at a specific location. (Words of Intelligence, 2nd Edition, 2011)

Synchronization. 1) The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2) In the intelligence context, application of intelligence sources and methods in concert with the operation plan to ensure intelligence requirements are answered in time to influence the decisions they support. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Synthesis. In intelligence usage, the examining and combining of processed information with other information and intelligence for final interpretation. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Systems Administrator (SA). Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

System Assurance. The justified measures of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008 with change 1 dated 28 Dec 2010)

T ==========

Tactical Control (TACON). Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. TACON is inherent in operational control. TACON may be delegated to, and exercised at any level at or below the level of combatant command. When forces are transferred between combatant commands, the command relationship the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. TACON provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. (JP 1, 25 Mar 2013 and JP 1-02) Also see *combatant command*; *combatant command (command authority)*; *operational control*.

Tactical Intelligence. Intelligence required for planning and conducting tactical operations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Tactical Intelligence and Related Activities (TIARA). Those activities outside the National Foreign Intelligence Program that accomplish the following: 1) respond to operational commanders' tasking for time-sensitive information on foreign entities; 2) respond to national intelligence community tasking of systems whose primary mission is support to operating forces; 3) train personnel for intelligence duties; 4) provide an intelligence reserve; or 5) are devoted to research and development of intelligence or related capabilities. Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data. (Previously in JP 1-02)

Tactical Level of War. The level of war at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *operational level of war; strategic level of war*.

Tactical Questioning (TQ). The field-expedient initial questioning for information of immediate tactical value of a captured or detained person at or near the point of capture and before the individual is placed in a detention facility. Tactical questioning is generally performed by members of patrols, but can be done by any appropriately trained DoD personnel. Tactical questioning is limited to direct questioning. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

> For DoD policy see DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, 11 Oct 2012

-- Also, direct questioning by any Department of Defense personnel of a captured or detained person to obtain time-sensitive tactical intelligence, at or near the point of capture or detention and consistent with applicable law. (JP 1-02 and JP 3-63, Detainee Operations, 30 May 2008)

-- Also, expedient initial questioning for information of immediate tactical value. (Army FM 2-22.3, Human Intelligence Collector Operations, Sep 2006)

Tag. Something that is attached to the item to be located and/or tracked, which increases its ability to be detected or its probability of identification by a surveillance system suitably tuned to the tag. (Defense Science Board 2004 Summer Study, *Transition to and from Hostilities*, Dec 2004)

> Tags can be either active (such as radio-emitting tags) or passive (such as radio frequency identification [RFID] tags). Passive tags can also be chemical (such as infrared fluorescent) or biological in nature.

Task. A clearly defined action or activity specifically assigned to an individual or organization that must be done as it is imposed by an appropriate authority. (JP 1, 25 Mar 2013)

Task Critical Asset. An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD Components or DISLA organizations to execute the task or mission-essential task it supports. Task critical assets are used to identify defense critical assets. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Target. 1) An entity or object considered for possible engagement or other action; 2) **in intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed…** [emphasis added] (JP 1-02 and JP 3-60)

-- Also, an individual, organization, or intelligence service against which intelligence operations are conducted. Also refers to documents or instruments which an intelligence service is trying to obtain, or the subject of a surveillance. (FBI FCI Terms)

Target Audience (TA). An individual or group selected for influence. (JP 1-02 and JP 3-13, Information Operations, 13 Feb 2006)

Target Folder. A folder, hardcopy or electronic, containing target intelligence and related materials prepared for planning and executing action against a specific target. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007)

Target Intelligence. Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (JP 3-60, Joint Targeting, 13 Apr 2007)

Targeted Violence: Pre-conceived violence focused on individuals, groups, or locations where perpetrators are engaged in behaviors that precede and are related to their attacks. These perpetrators consider, plan and prepare before engaging in acts of violence and are often detectable, providing an opportunity for disruption of the intended violence. (DSB Report, *Predicting Violent Behavior*, Aug 2012)

"There is no panacea for stopping all targeted violence."

-- DSB Report, *Predicting Violent Behavior*, August 2012

Copy of Defense Science Board Report (DSB), *Predicting Violent Behavior*, Aug 2012 available at: <http://www.acq.osd.mil/dsb/reports/PredictingViolentBehavior.pdf> (accessed 10 Oct 2012)

Targeting. The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0, Joint Operations, 11 Aug 2011)

-- Also, the act of focusing on a country, organization, non-state actor, installation, system, or person to identify an operational or intelligence goal. (National HUMINT Glossary)

-- Also, the process of selecting targets and matching the appropriate response to them, including operational requirements and capabilities. The purpose of targeting is to disrupt, delay, or limit threat interference with friendly COAs [courses of actions]. (FM 2-22.2, Counterintelligence, Oct 2009)

CI support to the targeting process include the development of CI targets list to identify those FISS and ITO persons, organizations, facilities, or installations that must be exploited through raid and capture to gain additional intelligence or neutralization to disable or destroy, negate, mitigate, or degrade the adversary's ability to collect on U.S. forces.

-- FM 2.22-2, *Counterintelligence*, October 2009, p. 5-7

See JP 3-60, *Joint Targeting*, for additional information.

Note: The doctrinal targeting process that has been adopted by the Army is denoted by the acronym "D3A," which stands for "Decide, Deliver, Detect, and Assess" and is covered in-depth in FM 6-20-10, *Tactics, Techniques, and Procedures for the Targeting Process*, 8 May 1996.

TARP. Acronym for *Threat Awareness and Reporting Program*; see Army Regulation 381-12, TARP, 4 Oct 2012.

Task Asset. [In critical infrastructure usage] an asset that is directly used to support execution of one or more operations, tasks, activities, or mission essential tasks (METs). (DoDI 3020.45, DCIP Management, 21 Apr 2008) Also see *asset, defense critical asset, defense critical infrastructure program (DCIP), task critical asset*.

Task Critical Asset (TCA). An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD Components or DISLA organizations to execute the task or mission-essential task it supports. Task critical assets are used to identify defense critical assets. (DoDD 3020.40, Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *asset, defense critical asset, defense critical infrastructure program (DCIP), task asset.*

Tier 1 - 3 Task Critical Assets

Tier 1 TCA. An asset the loss, incapacitation, or disruption of which could result in mission (or function) failure at the DoD, Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure sector level.

Tier 2 TCA. An asset the loss, incapacitation, or disruption of which could result in severe mission (or function) degradation at the DoD, Military Department, Combatant Command, subunified command, Defense Agency, or defense infrastructure sector level.

Tier 3 TCA. An asset the loss, incapacitation, or disruption of which could result in mission (or function) failure below the Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure sector level.

-- DoDM 3020.45-Vol 1, *Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP),* 24 Oct 2008

Task Force Counterintelligence Coordinating Authority (TFCICA). An individual that affects the overall coordination of counterintelligence activities (in a joint force intelligence directorate counterintelligence and human intelligence staff element, joint task force configuration), with other supporting CI organizations, and supporting agencies to ensure full CI coverage of the task force operational area. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Tasking. Directing or requesting a source to perform in a specific manner to achieve an objective or conduct an activity. (DoDI S-5200.42, Defense HUMINT and Related Activities (U), 8 Dec 2009)

-- Also, the process associated with acceptance of a validated collection requirement and assigning it to organic collection assets for action. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

Tear Line. A physical line on an intelligence message or document separating categories of information that have been approved for foreign disclosure and release. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *tearline reporting*.

The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with "need-to-know", need-to-release, and write-to-release principles and foreign disclosure guidelines of the information below the tear line.

-- Also, a physical line on an intelligence message or document separating categories of information that have been approved for foreign disclosure and release. Normally, the intelligence below the tear line is that which has been previously cleared for disclosure or release. (DoDI S-5240.17, CI Collection Activities, 14 Mar 2014)

Tearline Reporting. An automated or manual technique for separating an intelligence report into multiple portions separated by machine-or human-readable tearlines. A tearline section is the area in an intelligence report or finished intelligence product where the sanitized version of a more highly classified and/or controlled report is located. The sanitized information within the tearlines contains the substance of the more detailed information without identifying the sensitive sources and methods, allowing wider dissemination of substantive intelligence information to authorized users. (ICD 206, 17 Oct 2007) Also see *tear line*.

Also see ICD 209, *Tearline Production and Dissemination*, 6 Sep 2012

Technical Counterintelligence (TCI). A component of counterintelligence technical services. TCI includes Technical Surveillance Countermeasures (TSCM) and the investigation, study, and control of compromising emanations from information systems, known as TEMPEST. Also see *technical penetration, Technical Surveillance Countermeasures, TEMPEST.*

The essence of technical counterintelligence collection is learning through technical means what foreign intelligence services see, hear, and sense, what they know about one's own technical means, and how they are using this information.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 224

Technical Counterintelligence (TCI) Countermeasures. Any action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment or facility that electronically processes information to technical exploitation of classified and/or sensitive information. (AR 381-14, Technical Counterintelligence [U], 30 Sep 2002)

Technical Intelligence (TECHINT). Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, the identification, assessment, collection, exploitation, and evacuation of captured enemy materiel (CEM) in support of national and immediate technical intelligence requirements. TECHINT provides rapid performance and vulnerability assessments of enemy equipment, giving a critical edge to US forces in current and future operations. (Army FM 2-22.401, TECHINT, 9 Jun 2006)

Technical Hazard. An insecure condition that could permit the technical exploitation of an area with classified national security information, restricted data, and/or unclassified information requiring protection. (AR 381-14, Technical Counterintelligence, 30 Sep 2002)

Technical Penetration. The use of technological means to conduct an intentional, unauthorized interception of information-bearing energy. (DoDI 5240.05, TSCM Program, 22 Feb 2006)

-- Also, a deliberate, unauthorized, clandestine emplacement of a device or modification of existing government equipment, or the clandestine employment of a technique, which allows the technical monitoring within an area for the purpose of gaining information. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, *technical penetrations* include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. (Previously in JP 2-01.2, CI & HUMINT Support to Joint Operations, 13 Jun 2006)

> *"…[I]t had been my experience that the most up-to-snuff secret audio and other clandestine monitoring techniques always seemed to be a step ahead of the counter-surveillance teams."*
> -- Richard Helms with William Hood, *A Look Over My Shoulder* (2003), p. 449

Technical Security. A security discipline dedicated to detecting, neutralizing, and/or exploiting a wide variety of hostile and foreign penetration technologies. This discipline mandates training in various countermeasure techniques. (IC Standard 700-1, 4 Apr 2008)

Technical Services. The investigative use of video surveillance and interception of oral, electronic and wire communications. (AFPD 71-1, Criminal Investigations and Counterintelligence, 1 Jul 1999)

Technical Surveillance. The use of optical, audio, or electronic monitoring devices or systems to surreptitiously collect information. (DoDI 5240.05, TSCM, 3 Apr 2014)

-- Also, surveillance accomplished through the use of electronic listening devices, vehicle trackers, and signaling devices. (CI Community Lexicon)

Technical Surveillance Countermeasures (TSCM). Techniques to detect, neutralize, and exploit technical surveillance technologies and hazards that permit the unauthorized access to or removal of information. (DoDI 5240.05, TSCM Program, 3 Apr 2014)

-- Also, techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, physical, electronic, and visual techniques used to detect and counter technical security devices, technical security hazards, and related physical security deficiencies. (IC Standard 700-1, 4 Apr 2008)

Long history of adversary technical surveillance collection and exploitation of sensitive U.S. facilities and activities…

"*In 1944, the very first TSCM sweep uncovered 120 microphones in the Moscow Embassy* [U.S. Embassy in Moscow]."
-- Frederick L. Wettering, "Counterintelligence: The Broken Triad." *International Journal of Intelligence and Counterintelligence* 13 (Fall 2000), pp. 265-299.

TSCM identifies technically exploitable conditions and provides strategies to mitigate or remove them.

_____

TSCM represents the convergence of two distinct disciplines -- counterintelligence and security countermeasures. These techniques and countermeasures are designed to detect and nullify a wide variety of technologies used to gain unauthorized access to classified national security information, restricted data, or otherwise sensitive information.

-- ICD 702, *TSCM,* 18 Feb 2008

TSCM involves the search for technical surveillance devices or "bugs." …[T]he overwhelming number of technical attacks against US interests occur overseas. … Scare resources should be directed both to specific threat-driven inspections and to the maintenance of an R&D and training effort,

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, p. 61

The TSCM Program includes four separate functions: detection, nullification, isolation, and education.

-- FM 2-22.2, *Counterintelligence*, October 2009, p. 6-5;
also AR 381-14, *Technical Counterintelligence (TCI)* (U), 30 Sep 2002, p. 7

TSCM: the systematic physical and electronic examination of a designated area by properly trained, qualified and equipped persons in an attempt to discover electronic eavesdropping devices, security hazards or security weaknesses.

-- www.dbugman.com

PROJECT GUNMAN

A most spectacular case of electronic espionage occurred in the 1980s, at the height of the Cold War, when it was discovered that Soviet intelligence had successfully implanted very sophisticated bugs in a large number of electronic typewriters at the U.S. embassy in Moscow. On 25 March 1985, the story of the Soviet bug of U.S. typewriters in the Moscow Embassy broke on the CBS nightly news.

For detailed information see Sharon A. Maneki, *Learning From the Enemy: The GUNMAN Project*, NSA, 2012, 35 pages. Available on line at: http://www.nsa.gov/about/_files/cryptologic_heritage/center_crypt_history/ publications/Learning_From_the_Enemy_The_GUNMAN_Project.pdf

Technical Surveillance Device (TSD). A device covertly installed to monitor (visually, audibly, or electronically) sensitive activities and/or information processing within a target area. (ICS Glossary)

Technical Threat Analysis. A continual process of compiling and examining information on technical surveillance activities against personnel, information, operations, and resources. (DoDI 5240.05, TSCM Program, 3 Apr 2014)

Technology. The application of scientific and technical information and know-how to design, produce, manufacture, use, adapt, reconstruct, or reverse-engineer goods. This includes technical information and data in all forms, including electronic form. The term does not include the goods themselves, nor does it include scientific information in the public domain. (DoDI 2040.02, International Transfers of Technology, Articles, and Services, 10 Jul 2008) Also see *critical technology*.

Technology Readiness Level (TRL). A standard utilized in the scientific community to track the maturity of a technology. The readiness level is depicted on a numerical scale form one to nine, where one represents the initial idea stage and nine represents the final fielding and utilization of the technology. (DoD FCIP Strategy FY 2013-017)

Technology Targeting Risk Assessment (TTRA). A country-by-country assessment conducted by the Defense Intelligence Community that quantifies risks to CPI [critical program information] and related enabling technologies for weapons systems, advanced technologies or programs, and facilities such as laboratories, factories, research and development sites (test ranges, etc.), and military installations. The TTRA evaluates five independent risk factors, each of which contributes to an overall risk factor. The five areas evaluated are: Technology Competence, National Level of Interest, Risk of Technology Diversion, Ability to Assimilate, and Technology Protection Risk. (DoDI 5200.39, CPI within DoD, 16 Jul 2008 with change 1 dated 28 Dec 2010)

> The TTRA and CI Assessment provide laboratory/technical directors and Program Managers with information required to establish a comprehensive security program for the protection of identified critical program information (CPI).

Technology Transfer. The intentional communication (sharing) of knowledge, expertise, facilities, equipment, and other resources for application to military and nonmilitary systems. (DoDI 5535.8, DoD Technology Transfer Program, 14 May 1999)

-- Also, transferring, exporting, or disclosing defense articles, defense services, or defense technical data covered by the United States Munitions List (USML) to any foreign person or entity in the United States (U.S.) or abroad. (DSS Glossary)

Telecommunications and Information Systems Security. Protection afforded to telecommunications and information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security material and technical security information. (National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, 5 Jul 1990)

> Copy of NSD 42 available at: <http://www.fas.org/irp/offdocs/nsd/nsd42.pdf>

TEMPEST. An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security. (JP 1-02) Also see *compromising emanations; TEMPEST Test.*

-- Also, an unclassified term that refers to the investigation and study of compromising emanations. (IC Standard 700-1, 4 Apr 2008)

-- Also, a name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, Transient Electro Magnetic Pulse Emanation Standard (TEMPEST) the investigation, study, and control of compromising emanations from telecommunication and automated information systems equipment. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, the evaluation and control of compromising emanations from telecommunications and automated information systems. TEMPEST countermeasures are designed to prevent FISS and ITO [international terrorist organization] exploitation of compromising emanations by containing them within the space of the equipment or facility processing classified information. (Army FM 2-22.2, CI, Oct 2009)

-- An unclassified term referring to technical investigations for compromising emanations from electrically operated, information processing equipment; they are conducted in support of emanations and emission security. (ICS Glossary, Jun 1989)

TEMPEST – the problem of compromising radiation. Any time a machine is used to process classified information electrically… that machine may emit radio frequency or acoustic energy. These emissions, like tiny radio beacons, may radiate through free space for considerable distances…. Or they may be induced on nearby conductors like signal lines, power lines, telephones lines, or waste pipes and be conducted along those paths for some distance…. When these emissions can be intercepted and recorded, it is frequently possible to analyze them and recover the intelligence that was processed by the source equipment. The phenomenon affects not only cipher machines buy any information-processing equipment—teletypewriters, duplicating equipment, intercoms, facsimile, computers.…

-- Source: NSA, *TEMPEST: A Signal Problem*, undated [declassified/redacted version]
see <www.nsa.gov/public/crypt-spectrum.cfm>
also at: http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf

---

TEMPEST (an acronym for Transient Electromagnetic Pulse Emanation Standard) is both a specification for equipment and a term used to describe the process for preventing compromising emanations. The fact that electronic equipment such as computers, printers, and electronic typewriters give off electromagnetic emanations has long been a concern of the US Government. An attacker using off-the-shelf equipment can monitor and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring. …

Given the absence of a domestic threat, any use of TEMPEST countermeasures within the US should require strong justification.

[TEMPEST] *attacks require a high level of expertise, proximity to the target, and considerable collection time.* [emphasis added]

The commission recognizes the need for an active overseas TEMPEST program but believes the domestic threat is minimal.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, pp. 60-61

According to a declassified NSA publication: *"There is no special meaning in the word 'TEMPEST.' It was simply picked from a covername list by a NSA engineer in the early 1950s. However, TEMPEST has now become a generic word used throughout the US Government and industry to describe the unintentional emanation of classified information from an equipment."*

-- NSA, *Crypotolog*, Nov 1983 [declassified], p. 1

For a history of TEMPEST see declassified NSA publication, *A History of U.S. Communications Security (U),* [Vol I], revised July 1973, pp. 89-101; covers the timeframe through 1972.

This NSA report identified the main TEMPEST countermeasures as: "low-level keying, shielding, filtering, grounding, isolation, and physical protective measures." It also highlighted that shielded enclosures "provided not only the best means, but the only means we had come across to provide really complete TEMPEST protection in those environments where a large-scale intercept effort could be mounted at close range."

TEMPEST Test. A laboratory or on site (field) test to determine the nature and amplitude of conducted or radiated signals containing compromising information. (NSTISSI 7002, TEMPEST Glossary, 17 Mar 1995) Also see *compromising emanations; TEMPEST.*

Temporary Refuge. Protection afforded for humanitarian reasons to a foreign national in a DoD shore installation, facility, or military vessel within the territorial jurisdiction of a foreign nation or in international waters, under conditions of urgency in order to secure the life or safety of that person against imminent danger, such as pursuit by a mob. (DoDI 2000.11, Procedures for Handling Requests for Asylum and Temporary Refuge, 13 May 2010)

Terrorism. The unlawful use of violence or threat of unlawful violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010) Also see *homegrown terrorist, radicalization, violent extremism, violent radicalization.*

> ***There is no universally accepted definition of terrorism.***
> ***It remains the subject of continuing debate in international bodies.***
> -- Lord Carlile of Berriew Q.C. (March 2007)

-- Also, premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents (22 USC §2656f(d) and the National Strategy for Combating Terrorism, Feb 2003) [Definition used by Department of State, NCTC and CIA].

-- Also, the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (28 CFR §0.85) [Definition used by FBI, which reflects its mission, identifying a terrorist incident as a violation of the criminal laws of the United States and a suspected terrorist would, therefore, be subject to arrest and prosecution.]

-- Also, [the federal crime of terrorism] an offense that is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct. This includes terrorist acts committed within and outside U.S. national boundaries. (18 USC §2332b(g)(5)(A)).

-- Also, violent or illegal action taken on the basis of radical or extremist beliefs. (CRS Report R42553, Countering Violent Extremism in The United States, 19 Feb 2014)

> The Federal Bureau of Investigation (FBI) is the lead agency for investigating the federal crime of terrorism. If another federal agency identifies an individual who is engaged in terrorist activities or in acts in preparation of terrorist activities, the other agency is required to promptly notify the FBI. The extraterritorial jurisdiction for terrorism crimes is specified in 18 U.S.C. 2332b(e) and (f).
>
> Pursuant to 28 C.F.R. 0.85(1), the Attorney General has assigned responsibility to the Director of the FBI to "Exercise Lead Agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States. Within the United States, this would include the collection, coordination, analysis, management and dissemination of intelligence and criminal information as appropriate."
> -- Congressional Research Service (CRS) Report R41780, 27 Apr 2011
>
> ---
>
> For additional information on terrorism, see US Army TRADOC G2 Handbook No.1, *A Military Guide to Terrorism in the Twenty-First Century*, 15 Aug 2007.
> Copy available at: <http://www.fas.org/irp/threat/terrorism/>

Terrorism Threat Assessment. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat; [or] the product of a threat analysis for a particular unit, installation, or activity. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

Terrorist. One that engages in acts or an act of terrorism. (answer.com; accessed 27 October 2011)

> *Terrorists undertake criminal acts that involve the use or threat of violence against innocent persons. These acts are premeditated, intended to achieve a political objective through coercion or intimidation of an audience beyond the immediate victims.*
> – National Security Decision Directive 207, *The National Program for Combating Terrorism* (U), originally TOP SECRET, declassified

> Note: *Within DoD; None -- the term "terrorist" removed from JP 1-02.* Previously defined in JP 3-26, Counterterrorism (13 Nov 2009) as "those who commit acts of terrorism."

Terrorist Extremist. An extremist that uses terrorism -- the purposeful targeting of ordinary people -- to produce fear to coerce or intimidate governments or societies in the pursuit of political, religious, or ideological goals. Extremists use terrorism to impede and undermine political progress, economic prosperity, the security and stability of the international state system, and the future of civil society. (National Military Support Plan - War on Terrorism, 1 Feb 2006)

Terrorist Group. Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of terrorism.

> Current list of Foreign Terrorist Organizations (FTOs) at US Department of State web site: <http://www.state.gov/s/ct/rls/other/des/123085.htm>

Terrorist Identities Datamart Environment (TIDE). The U.S. Government's (USG) central repository of information on international terrorist identities. TIDE supports the USG's various terrorist screening systems or "watchlists" and the US Intelligence Community's overall counterterrorism mission. (NCTC)

> *The TIDE database includes, to the extent permitted by law, all information the USG possesses related to the identities of individuals known or appropriately suspected to be or to have been involved in activities constituting, in preparation for, in aid of, or related to terrorism (with the exception of purely domestic terrorism information). This information is available to counterterrorism professionals throughout the Intelligence Community, including the Department of Defense, via the web-based, read-only "TIDE Online."*
>
> -- NCTC Fact Sheet at <http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf>

Terrorism Screening Center (TSC). A multi-agency center administered by the FBI with support from the Department of Homeland Security, the Department of State, the Department of Justice, the Department of Defense, the Department of the Treasury, and the Office of the Director of National Intelligence. The TSC maintains the U.S. government's consolidated Terrorist Watchlist—a single database of identifying information about those known or reasonably suspected of being involved in terrorist activity. (fbi.gov)

> The TSC was created by HSPD-6 (16 Sep 2003) to consolidate the USG's approach to terrorist screening by creating a single comprehensive database of known or appropriately suspected terrorists (KSTs), and to make the information from this consolidated list available to foreign, federal, state, local, territorial, tribal, regulatory and private sector entities through the TSC's 24/7 Terrorist Screening Operations Center (TSOC).
>
> For additional information see FBI web site at: <http://www.fbi.gov/about-us/nsb/tsc>

Terrorist Screening Database (TSDB). Under Homeland Security Presidential Directive-6, the TSDB is the master terrorist watchlist, for both international and domestic terrorists, maintained by the Terrorist Screening Center (TSC) for the U.S. Government.

Terrorist Threat. An expression of intention, by an individual or group, to commit an act or acts of violence to inflict injury or damage in pursuit of political, religious, or ideological objectives. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012, w/ change 1 dated 9 Sep 2013)

> *Terrorist threats emanate from a diverse array of terrorist actors, ranging from formal groups to homegrown violent extremists (HVEs) and ad hoc, foreign-based actors.*
>
> *US-based extremists will likely continue to pose the most frequent threat to the US Homeland.*
>
> -- DNI, Worldwide Threat Assessment of the US Intelligence Community, SSCI, 29 January 2014, p. 4

Terrorists with Global Reach – Transnational Terrorists. Terrorist organizations with an operational and support network in multiple countries that possess the capability to recruit, plan, resource, and execute terrorist acts worldwide. (National Military Support Plan - War on Terrorism, 1 Feb 2006)

TFCICA. See *Task Force Counterintelligence Coordinating Authority*.

Theater. The geographical area for which a commander of a geographic combatant command has been assigned responsibility. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02)

Theater Clearance. Clearance for official travel within a geographic combatant command area of responsibility granted by the responsible geographic combatant commander or other delegated authority. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

Theater of War. Defined by the Secretary of Defense or the geographic combatant commander, the area of air, land, and water that is, or may become, directly involved in the conduct of the war. A theater of war does not normally encompass the geographic combatant commander's entire area of responsibility and may contain more than one theater of operations. (JP 1-02)

Theater Strategy. An overarching construct outlining a combatant commander's vision for integrating and synchronizing military activities and operations with the other instruments of national power in order to achieve national strategic objectives. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Thermal Imagery. Imagery produced by sensing and recording the thermal energy emitted or reflected from the objects which are imaged. (JP 1-02)

Third Agency Rule. An agreement among the US Government agencies participating in the exchange of intelligence data forbidding one agency to disseminate to another agency information which originated with a third agency. (National HUMINT Glossary)

-- Also, the tenet that information, usually classified or sensitive, originating in one U.S. agency not be disseminated by another agency to which the information has not been made available without the consent of the originating agency. (AR 381-20, Army CI Program, 25 May 2010)

Threat. The intention and capability of an adversary to undertake actions that would be detrimental to the interest of the U.S. (IC Standard 700-1, 4 Apr 2008)

-- Also, the sum of the potential strengths, capabilities, and strategic objectives of any adversary that can limit or negate U.S. mission accomplishment or reduce force, system, or equipment effectiveness. (DoDD 5200.1-M, Acquisition Systems Protection Program, March 1994)

-- Also, an adversary having the intent, capability, and opportunity to cause loss or damage. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, (1) A source of unacceptable risk; or (2) The capability of an adversary coupled with the adversary's intention to undertake actions that would be detrimental to the success of certain activities or operations. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, the capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations. (IOSS OPSEC Glossary of Terms, 27 Aug 2003)

-- Also, any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADRP 3-0, Unified Land Operations, May 2012)

-- Also see *threat to national security; transnational threat; foreign intelligence collection threat; insider threat.*

Threat Advisory. An advisory is a one-time product or produced on a recurring schedule – daily, weekly, or monthly. The advisory informs authorized recipients of an immediate or the potential for a foreign intelligence or terrorist threat. The advisory typically contains information of a perishable nature. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

> A threat advisory is distinguishable from an assessment and an analysis report in that it is prepared when there is an imminent or near-term intelligence or terrorist threat. A threat advisory often contains perishable information with only limited study or research conducted prior to publication.

Threat Analysis. a process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities. (DoDM 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, *terrorism threat analysis*, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target the DoD Components or DoD elements and personnel. A threat analysis shall review the factors of a terrorist group's operational capability, intentions, activity, and the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013; also JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

Threat Assessment. A resultant product of the defined process used to conduct a threat analysis and develop an evaluation of a potential threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, *DCIP Threat Assessment*: [in Defense Critical Infrastructure Protection usage] a compilation of strategic intelligence information incorporating multi-faceted threats facing DCAs [Defense Critical Assets] and Tier 1 TCAs [Task Critical Assets]. DCIP threat assessments address threats posed to DCAs [and Tier 1 TCAs] from domestic and transnational terrorist elements, foreign intelligence and security services, and weapons of mass destruction. (DoDI 5240.19, CI Support to the Defense Critical Infrastructure Program, 31 Jan 2014)

-- Also, an evaluation of the current or projected capability of a foreign intelligence service or international terrorist group to limit, neutralize, or negate the effectiveness of a friendly mission, organization, or material item through multidisciplined intelligence collection, espionage, or sabotage. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, in antiterrorism, examining the capabilities, intentions, and activities, past and present, of terrorist organizations as well as the security environment within which friendly forces operate to determine the level of threat. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, [in antiterrorism usage] the process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat; the product of a threat analysis for a particular unit, installation, or activity. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

Threat Finance. The covert movement of the profits of illicit acts or of funds that will support illicit acts. (*A Guide to Counter Threat Finance Intelligence* by Marilyn B. Peterson, 2009) Also see *counter threat finance (CTF).*

> ***The covert movement of money is the underlying facilitator of all threat activity.***
>
> Within DoD, see DoDD 5205.14, *DoD Counter Threat Finance Policy*, 19 Aug 2010 (w/ chg1 dated 16 Nov 2012)

Threat Indicator. Any observable action that displays violent behavior, abnormal disgruntlement, radicalization, or an extreme world view on religion or another type of ideology. (US Army, Asymmetric Warfare Group, Insider Threats in Partnering Environments: *A Guide for Military Leaders*, Jun 2011)

Copy of reference available at: <https://rdl.train.army.mil/catalog/go/100.ATSC/883A3A74-A803-4CD5-B693-0D59B108E7EC-1326399638300>

Reference also at: <http://www.wired.com/images_blogs/dangerroom/2012/10/awsc-pdf-CDR-72811.pdf>

Threat Warning. The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Threats to the National Security. International terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order. (FBI, Domestic Investigations and Operations Guide, 15 Oct 2011)

Time Bomb. Resident computer program that triggers an unauthorized act at a predefined time. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Time-Sensitive Collection Requirement (TSCR). A HUMINT collection requirement (HCR) needing immediate or time-specific action. Those organizations tasked with the time sensitive collection requirement should provide initial intelligence reports or a report stating an inability to collect on the requirement with 48 hours of issuance. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Tosses (hand, vehicular) [e.g., hand toss, car toss]. Tradecraft techniques for placing drops by tossing them while on the move. (CI Centre Glossary)

Traces. The product resulting from a name check. (AFOSI Instruction 71-101, 6 Jun 2000)

Tracking. Precise and continuous position-finding of targets by radar, optical, or other means. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

Tradecraft. Specialized methods and equipment used in the organization and activity of intelligence organizations, especially techniques and methods for handling communications with agents. Operational practices and skills used in the performance of intelligence related duties. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; DoDI S-5240.17, CI Collection Activities, 14 Mar 2014; and CI Community Lexicon)

Tradecraft

The methods of the clandestine operator…
Principles and techniques of clandestine operations

Successful espionage is impossible without good tradecraft

In general, tradecraft is the sum total of the skills the Case Officer or agent must master in order to securely operate in the field and preserve security of operational activity.

"Tradecraft is an art—a combination of common sense and imagination…. [T]he art of tradecraft, the methods employed to mange an intelligence operation. It is an art because of the nuances involved and it is not easy to learn. Some, lacking the personality traits, can never master it."

-- Richard L. Holm, The Craft We Chose (2011), pp 25 and 275

The techniques adopted by spies to conceal their activities are lumped together under the catch-all term "tradecraft." It refers to a vast range of protective measures devised to preserve the operational security of spying.

-- Frederick P. Hitz (Former CIA IG 1990-1998), *The Great Game* (2005)

Pillars of Tradecraft: *assessment; cover and disguise; concealments; clandestine surveillance; and covert communications*.

-- *Spycraft* (p. 363)

[T]he greatest danger… lay not in betrayal by a Soviet mole, as Angleton would have it, but by simple mistakes in tradecraft and a failure to maintain proper compartmentation of information.

-- Benjamin Weiser, *A Secret Life* (2004)

"The spy who does not take tradecraft seriously is unlikely to remain a spy for very long."

-- H.H.A. Cooper and Lawrence J. Redlinger, *Making Spies: A Talent Spotter's Handbook*

-- Also, the art, discipline and methodology of conducting secure clandestine operations and intelligence collection. (National HUMINT Glossary)

-- Also, the tactics, techniques, and procedures used in executing HUMINT, counterintelligence, or related activities to obscure, protect, or otherwise frustrate detection. (HDI Lexicon, April 2008)

-- Also, specialized techniques used in intelligence operations. (FBI FCI Terms)

-- Also, the techniques, technology, and methodologies used in covert intelligence operations. Tradecraft applies to both the procedures, such as surveillance detection routes, as well as the use of devices in covert audio and agent communications. (Spycraft)

-- Also, the art, methodology, and know-how of conducting clandestine operations and intelligence collection techniques. Includes such things as dead drops, covert communications, how to recruit agents, secret writing and photography, surveillance, and surveillance detection. (A Spy's Journey)

-- Also, the essential skills required to conduct successful clandestine operations. (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd edition, 2012)

-- Also, the techniques of the espionage trade, or the methods by which an agency involved in espionage conducts its business. Elements of tradecraft, in general terms, include the ways in which an intelligence officer arranges to make contact with an agent, the means by which the agent passes on information to the officer, the method for paying the agent, and the many precautions and tactics of deception applied along the way. (<http://www.espionageinfo.com/Te-Uk/Tradecraft.html>)

Tradecraft - Analytical. The term "tradecraft" usually applied to espionage techniques, but there is also *analytical tradecraft*: techniques, methods, and standards of the practice of analysis, e.g., framing questions, marshaling evidence, making concise arguments, identifying intelligence gaps, etc. Analytical tradecraft affords some criteria by which to judge analytical products and analysts.

Transmission Security. The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010) Also see *communications security*.

Transnational Threat. Any transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery for such weapons, and organized crime) that threatens the national security of the United States. (50 USC §401a)

-- Also, any activity, individual, or group not tied to a particular country or region that operates across international boundaries and threatens United States national security or interests. (JP 1-02 and JP 3-26, Counterterrorism, 13 Nov 2009)

> DoD further defines a *transnational threat* as any activity, individual, or group not tied to a particular country or region that operates across international boundaries and threatens US national security or interests. These threats also include extremists who enter into convenient relationships that exploit each others' capabilities and cloud the distinction between crime and terrorism (e.g., violent extremist organizations and opportunists, drug trafficking organizations, transnational criminal organizations [TCOs], and those trafficking in persons).
>
> Lawless and subversive organizations can take advantage of failed states, contested spaces, and ungoverned areas by forging alliances with corrupt government officials and some foreign intelligence services, further destabilizing political, financial, and security institutions in fragile states, undermining competition in world strategic markets, using cyberspace technologies and other methods to perpetrate sophisticated frauds, creating the potential for the transfer of WMD to terrorists, and expanding narco-trafficking and human and weapons smuggling networks.
>
> -- JP 3-27, Homeland Defense, 29 Jul 2013 (p. I-4)

Transnational Organized Crime (TOC). Self-perpetuating associations who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/ or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms. (White House, Strategy to Combat Transnational Organized Crime, Jul 2011)

> ***Transnational Criminal Organizations pose a National Security Threat***
>
> TOC represent a globally-networked national security threat and pose a real and present risk to the safety and security of Americans and our partners across the globe.
>
> *Countering TOC* is defined as the means to detect, counter, contain, disrupt, deter, or dismantle the transnational activities of state and non-state adversaries threatening U.S. and partner nation national security.
>
> Copy of the *Strategy to Combat Transnational Organized Crime* (July 2011) *at:* <https://www.hsdl.org/?view&did=682263>.
>
> Also see *The "New" Face of Transnational Crime Organizations (TCOs): A Geopolitical Perspective and Implications to U.S. National Security,* March 2013 (a compendium of white papers on TCOs).
>
> _____
>
> *"Transnational organized crime (TOC) networks erode good governance, cripple the rule of law through corruption, hinder economic competitiveness, steal vast amounts of money, and traffic millions of people around the globe. (Cybercrime, an expanding for-profit TOC enterprise….) TOC threatens US national interests in a number of ways: …drug activity, facilitating terrorist activity, money laundering, corruption, human trafficking, and environmental crime."*
>
> -- James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013

Trap. A hidden indicator to detect or confirm surreptitious tampering or search of items (e.g., documents, letters, packages, luggage, drawers, safes, rooms, film, equipment) by security or other personnel. (AFOSI Manual 71-119, CI Investigations, 27 Oct 2009)

Trap and Trace. A device which capture the incoming electronic or other impulses which identify the origination number of an instrument or device from which a wire or electronic communication was transmitted; see 18 USC §3127(4). (AR 381-10, US Army Intelligence Activities, 3 May 2007) Also see *pen register; trap and trace device*.

> A *trap and trace device* identifies all incoming phone numbers to a particular telephone.
> A *pen register* captures all outgoing phone numbers a particular telephone has called.

Trap and Trace Device. Captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011) Also see *pen register; trap and trace*.

Trash Cover. The intentional search of a specific person's trash (that is located at the place of collection), whether from a home or business, designed to find information relevant to an ongoing investigation when no reasonable expectation of privacy exists. A trash cover is a targeted effort to gather information regarding a particular person or entity by reviewing that person or entity's refuse. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Treason. -- Violation of the allegiance owed to one's sovereign or state; betrayal of one's country. (JP 1-02)

-- Also, [previously defined in DoDI 5240.06, *CI Awareness, Briefing, and Reporting Programs*, 7 Aug 2004) Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason [in war time, treason is a violation of Title 18 USC, § 2381].

"Treason is the ultimate mid-life crisis."

-- Dr. Marcus, CIA Psychiatrist in *Sira* by David Ignatius

Treason is the only crime specifically defined in the U.S. Constitution. Article III Section 3 delineates treason as follows: "Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court."

The crime is prohibited by legislation passed by Congress; 18 U.S.C. § 2381 states "whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than $10,000; and shall be incapable of holding any office under the United States." In the history of the United States there have been fewer than 40 federal prosecutions for treason and even fewer convictions.

"*Treason is the ultimate word of betrayal. Treason means stabbing your country on the back. But in legal terms, treason, the only crime that is defined in the U.S. Constitution has a narrow meaning… The founding fathers, well aware of the political use of treason charges by the kings of England, wanted to restrict the crime to one that could not be used as an excuse for the elimination of political rivals."*

-- Thomas B. Allen and Norman Polmar, *Merchants of Treason: America's Secrets for Sale* (1988), p. 176

"Treason is loved of many, but the traitor is hated of all."

-- Robert Greene

Triple Agent. An agent who serves three [intelligence] services in an agent capacity but who, like a double agent, wittingly or unwittingly withholds significant information from two services at the instigation of the third service. (FBI FCI Terms)

Trojan. A type of malware disguised or attached to legitimate or innocuous-seeming software, but that instead carries a malicious payload, most often opening a backdoor to unauthorized users. (Cybersecurity and cyberwar) Also see *Trojan Horse*.

Trojan Horse. A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *Trojan.*

-- Also, a computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security (for example, making a "blind copy" of a sensitive file for the creator of the Trojan horse). (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

-- Also, a malicious program that pretends to be a benign application; it purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but they can be just as destructive. (McAfee.com; accessed 15 Nov 2010)

True Name. A genuine and accurate representation of an individual or organization name, that may involve alterations of other identity information (e.g., address, telephone number, credit score, employer) when used under an approved cover in order to conceal true identity, purpose, or organizational affiliation. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

Trusted Foundry Program. DoD program that provides a cost-effective means to assure the integrity and confidentiality of integrated circuits during design and manufacturing while providing the US Government with access to leading edge microelectronics technologies for both Trusted and non-sensitive applications. (DMEA web site)

> Defense Microelectronics Activity (DMEA) is the program manager for the DoD Trusted Foundry program; see website at: <http://www.dmea.osd.mil/trustedic.html>
>
> Also see NSA's Trusted Access Program Office (TAPO) web site at: <http://www.nsa.gov/business/programs/tapo.shtml>

TSCM. See *Technical Surveillance Countermeasures*.

TSCM Practitioner. An individual trained and certified to conduct all TSCM activities within DoD. (DoDI 5240.05, TSCM, 3 Apr 2014) Also see *TSCM Technician*.

TSCM Technician. An individual trained to perform limited TSCM activities under the oversight of a TSCM practitioner. (DoDI 5240.05, TSCM, 3 Apr 2014) Also see *TSCM Practitioner*.

TSCM Equipment. Equipment or mechanisms used to identify the presence of surveillance devices. TSCM includes general purpose, specialized, or fabricated equipment to determine the existence and capability of surveillance devices. (DoDI 5240.05, TSCM, 3 Apr 2014)

Turnover. The official changing of an agent from one case officer to the other—i.e., turning him over to another. (A Spy's Journey)

Two-Person Control (TPC). the continuous surveillance and control of material at all times by a minimum of two authorized individuals, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and each familiar with established security requirements. (DoDI 5200.33, Defense Courier Operations, 30 Jun 2011) Also see *two-person integrity; two-person rule.*

-- Also, continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Two-Person Integrity. A provision that prohibits one person from working alone. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Two-Person Rule. A system designed to prohibit access by an individual to nuclear weapons and certain designated components by requiring the presence at all times of at least two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task to be performed. (JP 1-02)

U

Umbrella Special Access Program (SAP). An approved Department of Defense (DoD) Special Access Program (SAP) that contains compartments for specific projects within the overall program. While there is no formal requirement to obtain separate approval for each individual project under the umbrella SAP, each project must be consistent with the Special Access Program Oversight Committee (SAPOC)-approved scope of the umbrella SAP. The nickname, program description, and accomplishments of each significant project will be reported in the annual Special Access Program report. *Note: An individual participant's access can be afforded across-the-board at the umbrella level or specific individual project access can be granted on a limited or non-umbrella level.* (DSS Glossary)

Unacceptable Risk. Threat to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, privileged, proprietary, financial, or medical records; or to the privacy of data subjects, which will not be tolerated by the Government. (DoDI 5200.02, DoD Personnel Security Program, 21 Mar 2014)

Unacknowledged SAP. A SAP [Special Access Program] having protective controls ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information. (DoDD 5205.07, SAP Policy, 1 Jul 2010) Also see *acknowledged SAP*.

Unauthorized Access. Any access that violates the stated security policy. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient. (EO 13526, Classified National Security Information, 29 Dec 2009 and DoDD 5210.50, Unauthorized Disclosure of Classified Information to the Public, 22 Jul 2005)

> *Unauthorized disclosures of classified information, including media leaks, may compromise sources and methods and pose a threat to national security.*
> -- ICD 701 Security Policy for Unauthorized Disclosures of Classified Information, 14 Mar 2007

-- Also, a communication or physical transfer, usually of sensitive but unclassified information or classified information, to an unauthorized recipient. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, an event involving the exposure of information to entities not authorized access to the information. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, intentionally conveying classified documents, information, or material to any unauthorized person (one without the required clearance, access, and need to know). (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

> *Unauthorized disclosures of classified information put at risk the success of the most sensitive classified operations, plans, partnerships, and technologies of DoD and our mission partners.*
>
> *Personnel who disclose classified information without authorization, in addition to having potentially committed a crime, breach the trust that we, as leaders, have placed in them.*
> -- SECDEF memorandum, subj: Deterring and Preventing Unauthorized Disclosures of Classified Information, 18 Oct 2012*
>
> * Copy available at: <http://www.fas.org/sgp/othergov/dod/osd101812.pdf>

Unauthorized disclosure of classified information is an increasingly common occurrence.

The harm caused by… frequent unauthorized disclosures is manifold. Particular items of information appearing in the press provide valuable intelligence for our adversaries concerning the capabilities and plans of the United States for national defense and foreign relations…. Disclosures about US intelligence programs are particularly damaging, because they may cause sources to dry up. Lives of human agents are endangered and expensive technical systems become subject to countermeasures.

--*The Willard Report*, 31 March 1982

Leaking sensitive information is like giving the enemy our play book.

Each year, countless unauthorized leaks cause severe damage to our intelligence activities and expose our capabilities. The fact of the matter is, some of the worst damage done to our intelligence community has come not from penetration by spies, but from unauthorized leaks by those with access to classified information…. The threat leaks pose to our national security is alarming, and it is imperative we do more to protect our national secrets.

-- Congressman Rep. Pete Hoekstra at the Heritage Foundation, 25 July 2005.
See full remarks at <http://www.fas.org/sgp/news/2005/07/hoekstra072505.html>

Intelligence requires secrets. And secrecy is under assault…. When secrecy is breached, foreign targets of US intelligence—such as adversary countries and terrorists—learn about, and then often develop countermeasures to, US intelligence techniques and operations. As a result, the effectiveness of intelligence declines, to the detriment of the national security policymakers and warfighters, and the citizenry that it is meant to serve.

-- James B. Bruce, Former CIA Officer

See Bruce's excellent article, entitled "The Consequences of Permissive Neglect: Laws and Leaks of Classified Intelligence" in *Studies of Intelligence* (Vol 47 No 1), available online at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article04.html>

Leaks are a problem that has plagued intelligence agencies throughout modern history – they can undermine intelligence operations, jeopardize intelligence sources and methods, and have a terrible impact on the lives of covert agents who are publicly exposed.

-- Senator Ron Wyden, cited in Senate Report 112-12, 4 April 2011, p. 12

The unauthorized release of classified documents in 2010 by major newspapers and the Wikileaks website underscore the risks of widespread dissemination of sensitive information.

-- CRS Report RL33539, *Intelligence Issues for Congress*, 20 Jun 2011

In the secret operations canon it is axiomatic that the probability of leaks escalates exponentially each time a classified document is exposed to another person—be it an Agency employee, a member of Congress, a senior official, a typist, or a file clerk. Effective compartmentation is fundamental to all secret activity…. The potential leaks—deliberate or accidental—is vast.

-- Richard Helms with William Hood, *A Look Over My Shoulder* (2003), pp.184-185

Every once in a while, there are people in the United States government who decide that they want to break federal criminal law and release classified information, and they ought to be imprisoned. And if we find out who they are, they will be imprisoned. Why people do it, I do not know.

-- Defense Secretary Donald Rumsfeld

When information about our intelligence, our people, or our operations appears in the media, it does incredible damage to our nation's security and our ability to do our job of protecting the nation. More importantly, it could jeopardize lives. For this reason, such leaks cannot be tolerated."

-- CIA Director Leon Panetta, Nov 2010

Leaks of classified information regarding intelligence sources and methods can disrupt intelligence operations, threaten the lives of intelligence officers and assets, and make foreign partners less likely to work with us. The culture of leaks has to change.

-- Senator Dianne Feinstein, Chairman of the Senate Intelligence Committee, 25 July 2012

Uncertain Environment. Operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct, do not have totally effective control of the territory and population in the intended operational area. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Uncertainty. Doubt resulting from awareness of imperfect knowledge. This may arise from information absence, perceived error, deception, unpersuasive nature of evidence, complexity, etc. (*A Handbook of the Psychology of Intelligence Analysis*, Richard L. Rees, Ph.D., Editor; n.d. - circa 2007)

In analysis, uncertainty can derive from seeing plausible alternatives to the truth (the latter of which may be unknown or unknowable). Moreover, emotional and motivational factors attend cognitive uncertainty. Analysts can feel anxiety or discomfort if they lack confidence or self-esteem generally, feel an aversion to ambiguity, or have a need to please, or have a hypersensitivity to criticism. This affective element can exist even in the presence of sufficient evidence to make a reasonable judgment. Some analyst may well estimate the truth, but—in contrast to the inscription on the wall of the CIA lobby (*John* 8:32)—the truth.

-- *A Handbook of the Psychology of Intelligence Analysis*, Richard L. Rees, Ph.D., Editor; n.d., p. 375

Unconventional Warfare (UW). A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes, but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery. (DoDD 3000.07, Irregular Warfare, 1 Dec 2008)

-- Also, activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area. (JP 3-05, Special Operations, 18 Apr 2011)

Undeclared. An officer, asset, agent, or action whose agency affiliation is not formally identified to a foreign intelligence or security service, government or organization, or other US Government entity. (National HUMINT Glossary)

-- Also, an individual or action whose intelligence affiliation is not disclosed. (HDI Lexicon, April 2008)

Undercover Activity. Any investigative activity involving the use of an assumed identity by an undercover employee for an official purpose, investigative activity, or function. (FBI, Domestic Investigations and Operations Guide, 15 Oct 2011)

Undercover Employee. An employee of the FBI, another federal, state, or local law enforcement agency, another entity of the United States Intelligence Community (USIC), or another foreign intelligence agency working under the direction and control of the FBI whose relationship with the FBI is concealed from third parties by the maintenance of a cover or alias identity for an official purpose, investigative activity, or function. (FBI, Domestic Investigations and Operations Guide, 15 Oct 2011)

Undercover Operation. A phrase usually associated with the law enforcement community and which describes an operation that is so planned and executed as to conceal the identity of, or permit plausible denial by, the sponsor. (DSS Glossary)

Understand. The ability to individually and collectively comprehend the implications of the character, nature, or subtleties of information about the environment and situation to aid decision-making. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Unified Action. The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Unified Command Plan (UCP). The document, approved by the President, that sets forth basic guidance to all unified combatant commanders; establishes their missions, responsibilities, and force structure; delineates the general geographical area of responsibility for geographic combatant commanders; and specifies functional responsibilities for functional combatant commanders. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02) Also see *Combatant Command*.

Six Combatant Commands (COCOMs) have geographic area responsibilities:
-- U.S. Northern Command (NORTHCOM)
-- U.S. Central Command (CENTCOM)
-- U.S. European Command (EUCOM)
-- U.S. Pacific Command (PACOM)
-- U.S. Southern Command (SOUTHCOM)
-- U.S. Africa Command (AFRICOM)

Three COCOMs that have worldwide functional responsibilities not bounded by geography:
-- U.S. Special Operations Command (SOCOM)
-- U.S. Strategic Command (STRATCOM)
-- U.S. Transportation Command (TRANSCOM)

Note: U.S. Joint Forces Command (JFCOM) was disestablished in August 2011.

For additional information, see CRS Report, *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*, 3 Jan 2013, copy available at: <http://www.fas.org/sgp/crs/natsec/R42077.pdf>

Uniform Code of Military Justice (UCMJ). The criminal code governing the Armed Services of the United States. (CI Community Lexicon)

UCMJ (10 USC Chapter 47), is the foundation of military law in the United States. See UCMJ appendix in Manual for Courts-Martial (MCM): <http://www.au.af.mil/au/awc/awcgate/law/mcm.pdf>

Unilateral Operation. A clandestine activity conducted without the knowledge or assistance of a foreign intelligence or security service, host country, foreign organization, or non-state actor. (National HUMINT Glossary)

United States (US). Includes the land area, internal waters, territorial sea, and airspace of the United States, including the following: a) US territories, possessions, and commonwealths; and b) Other areas over which the US Government has complete jurisdiction and control or has exclusive authority or defense responsibility. (JP 1-02)

-- Also, when used in a geographic sense, means all areas under the territorial sovereignty of the United States. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Unity of Effort. Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization - the product of successful unified action. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02)

Unknown Subject (UNSUB). The subject of an investigation, whose identity has not been determined, commonly referred to as an "UNSUB." Also see *DoD Unknown Subject*.

Unknown Subject Lead. [Within DoD,] information indicating an unidentified current or former DoD-affiliated individual may have passed information or provided support to an FIE. (DoD Manual 5240.26, CI Insider Threat Program, *draft* 20 Nov 2013)

Unload Signal. A visual signal to indicate the departure of an individual or removal of an object from a given locale. (HDI Lexicon, April 2008)

Unsolicited Correspondence. Request for information from a person which may range from direct inquiries by phone, e-mail, fax, or letter in which the recipient is asked to provide seemingly innocuous data. (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

> Typical requests include solicitation of research papers, requests for additional information after a public presentation, suggestions for mutual research, requests for survey participation, and so forth; correspondence where the actual purpose may be to identify by name and position any individual who might be targeted later by a foreign intelligence service, and to elicit targeted information not readily obtainable by other means.

Unwitting. A person who is not aware of USG sponsorship of or affiliation with the cover. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013) Also see *witting.*

-- Also, not aware of US Government sponsorship or affiliation. (National HUMINT Glossary)

-- Also, unaware of the true nature of the activities being conducted or of the intelligence connections of persons involved. (HDI Lexicon, April 2008)

U.S. Coast Guard (USCG). A military, multi-function, maritime service that is the principal Federal agency responsible for safety, security, and stewardship with the maritime domain. It has diverse missions: national defense, homeland security, maritime safety, and environmental & natural resources stewardship. In March 2003, pursuant to the Homeland Security Act, the USCG was transferred from the Department of Transportation to the Department of Homeland Security (DHS).

> The CI component of the USCG is the Coast Guard Counterintelligence Service (CGCIS).

U.S. Homeland. The physical territory of the United States: the 50 states, District of Columbia, US territories and territorial waters; significant infrastructure linked to the United States; and major commercial air, land and sea corridors into the country. Also see *homeland*.

U.S. National. US citizen and US permanent and temporary legal resident aliens. (JP 1-02)

U.S. Person (USPERS; also USP). For intelligence purposes, a US person is defined as one of the following: 1) a US citizen; 2) an alien known by the intelligence agency concerned to be a permanent resident alien; 3) an unincorporated association substantially composed of US citizens or permanent resident aliens; or 4) a corporation incorporated in the United States, except for those directed and controlled by a foreign government or governments. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> Note: A person or organization outside the United States shall be presumed not to be a USP unless specific information to the contrary is obtained.

U.S. Secret Service (USSS). A federal law enforcement agency mandated by Congress to carry out dual missions: protection of national and visiting foreign leaders, and criminal investigations. (www.secretservice.gov)

> The Secret Service was established in 1865, solely to suppress the counterfeiting of U.S. currency. Headquarters in Washington, D.C. and more than 150 offices throughout the United States and abroad. Congress transferred USSS to the Department of Homeland Security (DHS) in 2002.
>
> Criminal investigation activities encompass financial crimes, identity theft, counterfeiting, computer fraud, and computer-based attacks on the nation's financial, banking, and telecommunications infrastructure.
>
> Protection mission is the most prominent of the two, covering the President, Vice President, their families, former Presidents, and major candidates for those offices, along with the White House and the Vice President's residence (through the Service's Uniformed Division). Protective duties of the Service also extend to foreign missions in the District of Columbia and to designated individuals, such as the Homeland Security Secretary and visiting foreign dignitaries.
>
> Separate from these specific mandated assignments, USSS is responsible for certain security activities such as National Special Security Events (NSSEs), which include the major party quadrennial national conventions as well as international conferences and events held in the United States.
>
> -- See CRS Report RL34603, *The U.S. Secret Service: An Examination and Analysis of Its Evolving Missions*, 31 July 2008

U.S.A. Patriot Act. USA Patriot Act of 2011 (Public Law 107-56); see *Patriot Act*.

V ==========

Validation. [In intelligence usage], a process associated with the collection and production of intelligence that confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Vault. A room(s) used for the storing, handling, discussing, and/or processing of Special Access Program (SAP) information and constructed to afford maximum protection against unauthorized entry. (DSS Glossary)

Vehicle-Borne Improvised Explosive Device (VBIED). A device placed or fabricated in an improvised manner on a vehicle incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. Otherwise known as a car bomb. (JP 1-02 and JP 3-10, Joint Security Operations in Theater, 3 Feb 2010)

VENONA. Highly classified U.S. SIGINT (cryptanalysis) effort during World War II to decipher encoded Soviet intelligence messages transmitted to Moscow on espionage activity in the United States. VENOA traffic indicated that the Soviets had over 300 assets of various kinds inside numerous U.S. Government agencies.

-- Also, code name for the U.S. codebreaking project that deciphered portions of the texts of Soviet intelligence messages between Moscow and other cities in the 1940s. Most messages concerned spy activities in the United States. (Spy Book)

I stood in the vestibule of the enemy's house, having entered by stealth.
I held in my hand a set of keys… and we were determined to use them.
-- FBI Agent Robert J. Lamphere

VENONA decryptions of Soviet intelligence messages in the 1940s, majority during WWII, identified numerous agents with access to the White House, Congress, and political parties, as well as agents in the media and in high-tech defense industries, however 178 Russian code names have yet to be linked to the true names of the American spies.

Research in Soviet Archives has added to the corroboration of some VENONA material, including the identities of many codenamed individuals

For additional information:
<www.nsa.gov/public_info/declass/venona/index.shtml>
<http://web.archive.org/web/20060614231955/http://www.nsa.gov/publications/publi00039.cfm>

Also see "In the Enemy's House: Venona and the Maturation of American Counterintelligence" at:
<http://web.archive.org/web/20061115021025/http://www.fbi.gov/libref/historic/history/foxpaper.htm>

Also see *The FBI-KGB War: A Special Agent's Story* by Robert J. Lamphere and Tom Shachtman.

Vetting. A generic term to describe the full spectrum of asset evaluation for authenticity, reliability and hostile control. It includes ops testing, caser officer and psychological assessment, polygraph, security, counterintelligence interview, production review and personal record questionnaires. (National HUMINT Glossary) Also see *asset validation, source validation* and *counterintelligence flags*.

-- Also, as related to *source validation*, an ongoing process the purpose of which is to continually determine, by means of specific operational acts and analytical assessments, the motivation, veracity, and control of a reporting source. (DoDI S-3325.07, Guidance for the Conduct of DoD Human Source Validation (U), 22 Jun 2009)

-- Also, the complete process of investigating and testing a potential source or information to determine its ability and suitability for clandestine activities. (AFOSI Instruction 71-101, 6 Jun 2000)

-- Also, a process of examination and evaluation, generally referring to performing a background check on someone before offering him or her employment, conferring an award, etc. In addition, in intelligence gathering, assets are vetted to determine their usefulness. (en.wikipedia.org/wiki/Vetting)

"Vetting" literally means getting a sick animal examined by a veterinarian; it has evolved into a term meaning to test or scrutinize.

-- Spy Book

Vetting is used in agent/source authentication. The vetting process is one of testing and examining the agent to determine the degree of the agent's/source's reliability and truthfulness in reporting information. It is designed to weed out fabricators and double agents.

Violent Behavior. The intentional use of physical force or power, threatened or actual, against a person or group that either results in or has a high likelihood of injury, death, or psychological harm to self or others. (DoDI 1438.06, DoD Workplace Violence Prevention and Response Policy 16 Jan 2014)

Violent Extremism. Individuals who openly express their religious, political, or ideological views through violence or a call for violence. (US Army Tactical Reference Guide, Radicalization into Violent Extremism: *A Guide for Military Leaders*, Aug 2011) Also see *radicalization*, *terrorism*, *violent radicalization.*

--Also, any ideology that encourages, endorses, condones, justifies, or supports the commission of a violent act or crime… to achieve political, social, or economic changes…. (FBI Counterterrorism Analytical Lexicon)

-- Also, the process of adopting or promoting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change. (House Bill 1955, 110th Congress, 24 Oct 2007)

Copy of Army reference cited above available at: <https://rdl.train.army.mil/catalog/go/100.ATSC/883A3A74-A803-4CD5-B693-0D59B108E7EC-1326399638300> Reference also at: <http://www.wired.com/images_blogs/dangerroom/2012/10/awsc-pdf-CDR-72811.pdf>

The Complexity of Violent Extremism

The threat posed by violent extremism is neither constrained by international borders nor limited to any single ideology. Groups and individuals inspired by a range of religious, political, or other ideological beliefs have promoted and used violence against the homeland.

Increasingly sophisticated use of the Internet, mainstream and social media, and information technology by violent extremists adds an additional layer of complexity.

-- Department of Homeland Security
See <http://www.dhs.gov/topic/countering-violent-extremism. (accessed 16 Jul 2013)

"Violent extremism presents one of the greatest threats to the citizenry of the United States and its allies."

-- *Edges of Radicalization*, Combating Terrorism Center, Feb 2012, p. 6

Violent Jihadist. The term characterizes jihadists who have made the jump to illegally supporting, plotting, or directly engaging in violent terrorist activity. (CRS Report R41416, 23 Jan 2013)

> American Jihadist Terrorism: Combating a Complex Threat, CRS Report R41416, 23 Jan 2013 available online at: <http://www.fas.org/sgp/crs/terror/R41416.pdf>

Violent Radicalization. The process of adopting or promoting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change. (House Bill 1955, 24 Oct 2007) Also see *radicalization, terrorism, violent extremism*.

Virus. Malicious software; a form of Trojan horse that reproduces itself in other executable code. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995) Also see *computer virus*.

-- Also, a computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. (US Army TRADOC DCSINT Handbook 1.02, 15 Aug 2007)

> *A virus is a computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates the files. Some viruses display symptoms, and others damage files and computer systems, but neither is essential in the definition of a virus; a non-damaging virus is still a virus.*
>
> – McAfee.com; accessed 15 Nov 2010

Volunteer. A person who initiates contact with a government, and who volunteers operational or intelligence information and/or request political asylum; includes call-ins, walk-ins, virtual walk-ins, and write-ins. (National HUMINT Glossary)

Vulnerability. 1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished; 2). The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment; and 3) In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007)

-- Also, a situation or circumstance, which left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, a weakness or susceptibility of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (DHS, National Infrastructure Protection Plan - 2009)

Vulnerability Analysis. A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Vulnerability Assessment (VA). A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, [regarding infrastructure] a systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the comprehensive evaluation of an installation, facility, or activity to determine preparedness to deter, withstand, and /or recover from the full range of adversarial capabilities based on the threat assessment, compliance with protection standards, and risk management. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, the process of identifying weaknesses in the protection of friendly operations and activities which, if successfully exploited by foreign intelligence, could compromise current or future plans, capabilities, or activities, including RDA [research, development and acquisition]. (AR 381-20, Army CI Program, 25 May 2010)

Vulnerability Study. An analysis of the capabilities and limitations of a force in a specific situation to determine vulnerabilities capable of exploitation by an opposing force. (JP 1-02)

W ==========

Waived Special Access Program. A SAP [Special Access Program] for which the Secretary of Defense has waived applicable reporting in accordance with [Section 119 of Title 10 US Code] following a determination of adverse effect to national security. An unacknowledged SAP that has more restrictive reporting and access controls. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

-- Also, an unacknowledged Special Access Program (SAP) to which access is extremely limited in accordance with the statutory authority of Section 119e of 10 United States Code (U.S.C), Reference b. The unacknowledged SAP protections also apply to Waived SAPs. Only the Chairman, Senior Minority member, and, by agreement, their Staff Directors of the four Congressional Defense Committees normally have access to program material.

Waiver. An exemption from a specific requirement. (DSS Glossary)

Walk-in. An unsolicited contact who provides information. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; DoDI S-5240.17, CI Collection Activities, 14 Mar 2014; and DHE-M 3301.002, Vol II Collections Operations, 23 Nov 2010) Also see *volunteer*.

-- Also, an individual who voluntarily offers his services or information to a foreign government. (FBI FCI Terms)

-- Also, an individual who offer his/her services to an intelligence service without being solicited. (CIA, D&D Lexicon, 1 May 2002)

-- Also, someone who has something to offer or sell to the intelligence service he is approaching: a volunteer spy. (A Spy's Journey)

Individuals who walk-in and provide information or offer to assist are motivated by a wide range of factors, including a sincere desire to help, pure greed, desire for revenge against some real or perceived grievance, etc. Each walk-in interview is unique.

In the real world of secret operations volunteers have produced some of the greatest coups. "It's the walk-in trade that keeps the shop open" is one of the first bits of operational wisdom impressed on newcomers to the business.

-- William Hood, *Mole: The True Story of the First Russian Intelligence Officer Recruited by the CIA* (1982)

As always with a "walk-in," as we irreverently referred to volunteer agents, the first consideration is the possibility of provocation.

-- Richard Helms with William Hood, *A Look Over My Shoulder: A Life in the Central Intelligence Agency* (2003), p. 219

[Walk-in] applies universally to agents who volunteer their services to a hostile intelligence agency by making an approach to an adversary at its premises. The KGB recognized that some of its best sources including John Walker, Aldrich Ames, and Robert Hanssen, acted in this way, but did not use the same term, preferring "self-recruited agents.

-- *Historical Dictionary of Cold War Counterintelligence* (2007)

For the story of a walk-in, see Barry G. Royden, "Tolkachev, A Worthy Successor to Penkovsky," *Studies in Intelligence*, v 47, n 3: pp. 5-33. Full article available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article02.html>

…it should be emphasized once more that work with "walk-ins" is an important part of agent operations for strategic intelligence and when properly planned and conducted can be very fruitful.

-- Ivan A. Serov, GRU General (1962)

See Ivan A. Serov, "Work with Walk-Ins,"* *Studies in Intelligence*, Vol 8, No, 1. This article, originally published in 1962, is adapted from one of several on Soviet intelligence doctrine written by high-ranking officers of the GRU (Soviet Military Intelligence). The article shows that Soviet/Russian problems in assessing and handling the walk-in are not unlike our own. The full article available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol8no1/html/v08i1a02p_0001.htm >

* Note: Russian term *dobrozhelatel* ("well-wisher") is virtually the same as our "walk-in."

Warning. 1) A communication and acknowledgment of dangers implicit in a wide spectrum of activities by potential opponents ranging from routine defense measures to substantial increases in readiness and force preparedness and to acts of terrorism or political, economic, or military provocation; and 2) operating procedures, practices, or conditions that may result in injury or death if not carefully observed or followed. (JP 1-02) Also see *warning intelligence*.

-- Also, a communication and acknowledgment of dangers implicit in a wide spectrum of activities by potential opponents ranging from routine defense measures to substantive increases in readiness and force preparedness and to acts of terrorism or political, economic, or military provocation. (DoDD 3115.16, The Defense Warning Network,5 Dec 2013)

-- Also, to issue an advance notification of possible harm or victimization following the receipt of information or intelligence concerning the possibility of a crime or terrorist attack. (ODNI, U.S. National Intelligence – An Overview 2011)

Warning Intelligence. Those intelligence activities intended to detect and report time sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Watch List. A list of words -- such as names, entities, or phrases -- which can be employed by a computer to select out required information from a mass of data. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Weapon System. A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012)

Weapons of Mass Destruction (WMD). Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. (JP 1-02 and JP 3-40, Combating WMD, 10 Jun 2009)

Specifically defined in US Code as: (1) any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or missile having an explosive or incendiary charge of more than one-quarter ounce, or mine or similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. (18 USC 18 §2332a)

White List. The identities and locations of individuals who have been identified as being of intelligence or counterintelligence interest and are expected to be able to provide information or assistance in existing or new intelligence areas of interest. (CI Community Lexicon) Also see *Black List*; *Gray List.*

> *White lists contain the identities and locations of individuals in enemy controlled areas. These individuals are of intelligence or CI interest. They are expected to be able to provide information or assistance in the accumulation of intelligence data or in the exploitation of existing or new intelligence areas of interest. They are usually in accord with or favorably inclined toward U.S. policies. Their contributions are based on a voluntary and cooperative attitude. Decisions to place individuals on the white list may be affected by the combat situation, critical need for specialists in scientific fields, and such intelligence needs as indicated from time to time.*
> *Examples of individuals included in this category are:*
> 1) *Deposed political leaders of a hostile state.*
> 2) *Intelligence agents employed by U.S. or allied intelligence agencies.*
> 3) *Key civilians in areas of scientific research, including faculty members of universities and staffs of industrial or national research facilities whose credibility have been established.*
>
> -- USMC, MCWP 2-6 (previously 2-14), Counterintelligence, 5 Sep 2000

Wilderness of Mirrors. The organizational culture of the secret services. In it deceptions are false, lies are truth, the reflections are illuminating and confusing. The phrase centers on the problem of the reliability of the secret information about espionage and the identity of spies. The mirrors comprise information from defectors, disinformation from the opposing sides in the Cold War, deviously covered false trails, and facts thought to be valid but incomplete (and later established as totally untrue). (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd edition, 2012)

-- Also, expression to sgnify the confusion of the world of intelligence and espionage. James Jesus Angleton, long-time head of counterespionage for the CIA, is generally credited with coining the term, having written that the Wilderness of Mirrors "is that… myriad of strategms, deceptions, artifices and all other devices of disinformation which the Soviet bloc and its coordinated intelligence services use to confuse and split the West," thus producing "an ever-fluid landscape where fact and illusion merge…." (Spy Book)

> *"Wilderness of Mirrors"* a description of counterintelligence attributed to James J. Angleton. It comes from T.S. Eliot's poem "Gerontion" (1920); also the title of a 1980 book authored by David C. Martin about CIA counterintelligence (New York: HarperCollins, First Edition, 1980).
>
> Angleton was CIA's Chief of the Counterintelligence from 1954 until his retirement in 1974. In December 1974, Angleton was basically forced into retirement by the Director of CIA (William Colby), who became convinced that Angleton's "labyrinthine" approach to counterintelligence severely hampered the Agency's primary mission -- clandestine HUMINT collection.

Window Dressing. [Tradecraft jargon] Ancillary materials that are included in a cover story or deception operation to help convince the opposition or casual observers that what they are observing is genuine. (CI Centre Glossary)

Witting. A term of intelligence art that indicates that one is not only aware of a fact or piece of information but also aware of its connection to intelligence activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *unwitting*.

-- Also, a person is aware of USG sponsorship or affiliation. (National HUMINT Glossary)

-- Also, aware of the true nature of the activities being conducted or of the intelligence connections of persons involved. (HDI Lexicon, April 2008)

-- Also, knowledgeable as to certain aspects of a clandestine organization and its activities. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Workplace Violence. Any act of violent behavior, threats of physical violence, harassment, intimidation, bullying, verbal or non-verbal threat, or other threatening, disruptive behavior that occurs at or outside the work site. (DoDI 1438.06, DoD Workplace Violence Prevention and Response Policy 16 Jan 2014)

Worm. A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) See *worms*.

-- Also, a type of malware that spreads automatically over a network, installing and replicating itself. The network traffic from rapid replication and spread can cripple networks even when the malware does not have a malicious payload. (Cybersecurity and Cyberwar)

> A worm is an unwanted software program secretly planted on a computer that enables (among other things) someone other than the owner to control it.
>
> In 2009, cyber security analysts worldwide reported that a "worm" called Stuxnet had penetrated and, in all likelihood, damaged an Iranian nuclear facility. The attack was apparently prosecuted through the facility's industrial control system.
>
> -- RAND Report, *A Cyberworm that Knows No Boundaries*, 2011* (see Appendix B - Worms)
>
> * Copy at: <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.pdf>

Worms. Parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread via Internet Relay Chat (IRC). (McAfee.com; accessed 15 Nov 2010) See *worm*.

Write for Maximum Utility (WMU). An approach that guides the way that intelligence organizations conceive, format, produce, and disseminate intelligence products in order to increase their usability for the intended customers. (ICD 208, 17 Dec 2008) Also see *write-to-release*.

> *Utility is maximized when customers receive or are able to expeditiously discover and pull or request intelligence, information, and analysis in a form they are able to easily use and able to share with their colleagues, subordinates, and superiors. WMU ensures intelligence, information, and analysis are produced in a manner to facilitate reuse—either in its entirety or in coherent portions—thereby enabling wider dissemination and enhancing its usability.*
>
> *WMU shares certain goals as well as techniques with previous and ongoing IC WTR [write-to-release] efforts. WMU goes further than WTR in linking knowledge of the customer's operating environment to the intelligence production effort. The resulting effort is not "one size fits all" or production of all intelligence products at the lowest classification, but products tailored to best meet a customer's requirements. This may mean producing the definitive assessment on a given topic area based on all available intelligence, regardless of classification.*
>
> -- ICD 208, *Write for Maximum Utility*, 17 Dec 2008

Write-to-Release (WTR). A general approach whereby intelligence reports are written in such a way that sources and methods are protected so that the report can be distributed to customers or intelligence partners at lower security levels. In essence, write-to-release is proactive sanitization that makes intelligence more readily usable by a more diverse set of customers. The term encompasses a number of specific implementation approaches, including sanitized leads and tearline reporting. (ICD 208, 17 Dec 2008) Also see *tearline reporting* and *write for maximum utility*.

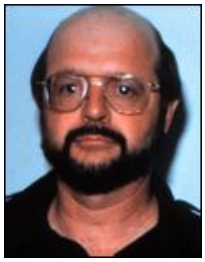
Written Statement. Permanently record of pretrial testimony of accused persons, suspects, victims, complaints, and witnesses. (FM 19-20, Law Enforcement Investigations, Nov 1985)

> *Written statements may be used in courts as evidence attesting to what was told investigators. They also are used to refresh the memory of the persons making the statements.*
>
> -- FM19-20, Law Enforcement Investigations, Nov 1985, p. 53

Y ==========

Year of the Spy. The year 1985 was labeled "The Year of the Spy" by the media because of the number of espionage-related incidents that came to light that year. Unbeknownst to the media and the CIA at the time, several other significant spying ventures started during this same year and would not come to light until years later. (Spy Dust)

-- Also, the phrase, coined late in 1985, to summarize the activities among notable spies and defectors in the Cold War. (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd edition, 2012)


John A. Walker, Jr.

Sharon M. Scranage

Jonathan J. Pollard

Larry Wu-tai Chin

Ronald W. Pelton

"The Year of the Spy" -- 1985

Spring 1985, the John Walker Spy Ring—John A. Walker, Jerry Whitworth, Arthur Walker, and Michael Walker—arrested for passing classified material to the Soviet Union.

July 1985, CIA employee Sharon Marie Scranage and boyfriend Michael Soussoudis arrested for passing material to Ghanian intelligence.

November 21, Navy intelligence analyst Jonathan Jay Pollard arrested for spying for Israel.

November 23, former CIA analyst Larry Wu-Tai Chin arrested on charges of spying for the People's Republic of China since 1952.

November 25, former National Security Agency employee Ronald William Pelton arrested for selling military secrets to the Soviets.

-- FBI at <http://www.fbi.gov/about-us/investigate/counterintelligence/cases>

For general background on these cases see Thomas B. Allen and Norman Polmar, *Merchants of Treason: America's Secrets for Sale,* New York: Delacorte Press, 1988.

For additional background see –
Walker Spy Ring: Hunter, Robert W., with Lynn Dean Hunter, eds. *Spy Hunter: Inside the FBI Investigation of the Walker Espionage Case*. Annapolis, MD: Naval Institute Press, 1999.

Other works on the Walker Espionage Ring:
-- Barron, John. *Breaking the Ring: The Bizarre Case of the Walker Family Spy Ring*. Boston: Houghton Mifflin, 1987.
-- Blitzer, Wolf. *Territory of Lies: The Exclusive Story of the Walker Family Spy Ring*. New York: Houghton Mifflin, 1987.
-- Blum, Howard. *I Pledge Allegiance: The True Story of the Walkers: An American Spy Family*. Simon & Schuster Books, 1987.
-- Earley, Pete. *Family of Spies: Inside the John Walker Spy Ring*. Bantam Books, 1988.
-- Kneece, Jack. *Family Treason: The Walker Spy Case*. New York: Stein & Day, 1986.
-- Walker, John Anthony. *My Life as a Spy*. Amherst, New York: Prometheus, 2008.

Pollard: Olive, Ronald J. *Capturing Jonathan Pollard: How One of the Most Notorious Spies in America History Was Brought to Justice.* Annapolis, MD: Naval Institute Press, 2006.

Chin: Hoffman, Tod. *The Spy Within: Lary Chin and China's Penetration of the CIA.* Hanover, NH: Steerforth Press, 2008.

Z ==========

Zero Day. [In computer usage] an attack that exploits a previously unknown vulnerability; taken from the notion that the attacks takes places on the zeroth day of awareness. Knowledge about zero-day exploits are valuable to both defenders and attackers. (Cybersecurity and Cyberwar)

Zombie. [In computer usage] a computer that is infected with a virus or Trojan horse that puts it under the remote control of an online hijacker. The hijacker uses a zombie to generate spam or launch denial of service attacks. (McAfee Labs – Threat Glossary)

-- Also, a computer that has been compromised by an outside party, for the purpose of exploiting its computational and network resources; frequently, lined into a botnet. (Cybersecurity and Cyberwar)

Zoning. A method of surveillance in which the surveillance area is divided into zones, and surveillants are assigned to cover a specific area. (Words of Intelligence, 2nd Edition, 2011)

Counterintelligence
A variety of views...

Counterintelligence (CI) is probably the most misunderstood secret intelligence function. The work itself has suffered as many definitions as there are intelligence services.

-- Richard Helms, Former DCI and Director CIA

Richard Helms with William Hood, *A Look Over My shoulder: A Life in the Central Intelligence Agency* (New York: Random House 2003), pp. 34-35

"…[C]ountering the intelligence efforts of an adversary is the central function of counterintelligence."
-- Roy Godson, Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence (Washington: Brassey's 1995), pp. xii, 15 & 304

"[Counterintelligence is]…intelligence of a special kind, plus something else…. Counterintelligence collects, stores, analyzes and disseminates information about certain foreign threats to U.S. security and then acts to destroy or neutralize them…. Its end purpose is not the mere collection and analysis of information, but action, and successful action, against those who threaten the security of the United States."
-- Francis McNamara, U.S. Counterintelligence Today, (Washington: The Nathan Hale Institute1985), p. 18

"[Counterintelligence] …must strive to know everything possible about an adversary's intelligence capabilities, including his sources, and methods of collection, his covert actions at influencing and managing our actions and perceptions, and even his culture and thought processes."
-- S. Eugene Poteat, "Counterintelligence Spy vs. Spy, Traitor vs. Traitor," *American Intelligence Journal* (Winter 2000-2001), p. 62

"[Counterintelligence is] …information about an adversary's intelligence operations, capabilities, agents, collection technology, and so on. It is *not* security. It is intelligence on which security policies should be based. Nor is it intelligence about an adversary's policy making or military operations or other nonintelligence capabilities and activities."
-- William E. Odom, Fixing Intelligence For a More Secure America (New Haven: Yale University Press 2003), p. xxix

"…[E]fforts taken to protect one's own intelligence operations from penetration and disruption by hostile nations or their intelligence services. It is both analytical and operational. …not a separate step in the intelligence process but an important function throughout the process."
-- Mark M. Lowenthal, Intelligence: From Secrets to Policy (Washington: CQ Press 2000), p. 98

"…[N]ational effort to prevent foreign intelligence services… from infiltrating our institutions and establishing the potential to engage in espionage, subversion, terrorism, and sabotage."
-- Newton Miller, "Counterintelligence at the Crossroads," Intelligence Requirements for the 1980's: Elements of Intelligence, ed. Roy Godson (Washington: National Strategy Information Center, Inc., 1983), p. 50

"[Counterintelligence] …involves the use of both offensive and defensive measures to: protect sensitive US information and operations from compromise and penetration by foreign intelligence services and other hostile entities; ensure the security and integrity of ongoing US diplomatic, military and intelligence operations; and penetrate, compromise and neutralize hostile operations mounted by foreign intelligence services, terrorist organizations and drug cartels."
-- "Richard L. Haver, "The Ames Case: Catalyst for a National Counterintelligence Strategy," *Defense Intelligence Journal*, Vol. 4 No. 1 (Spring 1995), p. 12

"[Counterintelligence] …includes all information gathered and activities conducted by the government aimed at detecting, analyzing, and countering threat. …the term refers to active operations conducted to counter--through detection, assessment, neutralization, and manipulation--the intelligence operations of foreign countries and groups. …it includes recruitment of foreign intelligence officers, disruption of activities, prosecution of criminal espionage, and manipulation and deception. …it involves the use of surveillance, double agents, and other clandestine techniques."
-- Kenneth E, deGraffenreid, "Countering Hostile Intelligence Activities as a Strategic Threat," National Strategy Information Center, Inc., Sep 1989, p. 3

"Counterintelligence is a term often associated with catching spies. …[It is also] information gathered and activities conducted with the purpose of disrupting and neutralizing the activities of hostile intelligence services."
-- Jeffery Richelson, The US Intelligence Community, 2d ed. (Ballinger Publishing Co., Cambridge MA, 1989), pp. 317 - 330

"Counterintelligence is a critical part of nearly all intelligence activities. When performed properly, the CI function is integral to the intelligence activity itself and part of the overall security of the organization."
-- Aspin-Brown Commission Report, Preparing for the 21st Century: An Appraisal of U.S. Intelligence, 1 March 1996

"[Counterintelligence is] …the most arcane and organizationally fragmented, the least doctrinally clarified, and legally, and thus politically, the most sensitive intelligence activity."
-- William E. Odom, Fixing Intelligence For a More Secure America (New Haven: Yale University Press 2003), p. 167

"CI, the quality-control of intelligence, is the key to the struggle between states and armies for a favorable disparity of knowledge. …CI concerns all other aspects of intelligence; that it must use all of the elements of intelligence as part of itself, while at the same time CI as a whole must be part of the analysis, collection, and covert action practiced by intelligence services. In its inward-looking perspective, CI is a double-check on one's own intelligence operations. In its outward-looking perspective, it is the sharpest weapon in the intelligence arsenal."
-- Angelo Codevilla, Informing Statecraft: Intelligence for a New Century (1992), pp. 325-326

"Counterintelligence… is a strategic instrument available to states to protect themselves and advance their interests in the struggle for power, wealth, and influence. …the end product, the mission of counterintelligence, is action—action to protect against foreigners and action to manipulate foreigners in the service of national goals."
-- Roy Godson, Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence (Washington: Brassey's 1995), pp. 238-239

Across the profession, there are vast differences in understanding of what counterintelligence means, and how it is done, and even the basic terminology it employs.

-- Hon. Michelle VanCleave (former NCIX 2003-2006)

The NCIX and the National Counterintelligence Mission: what has worked, what has not, and why,
Case Study Prepared for the Project on National Security Reform, May 2008

Miscellaneous Thoughts…

"CI… the most secret of secret intelligence activities…."

-- Senate Report 94-755, Church Committee Report, 26 April 1976

"There are far too many in the Intelligence Community who either do not understand counterintelligence or, who understanding its concepts, have climbed to the top of their career ladders by opposing it."

-- Senator Malcolm Wallop, Senate Intelligence Committee (1985)

"…[T]he counterintelligence community is performing its wartime mission every day as agents counter foreign intelligence threats – that's why we call it the silent war."

-- Colonel Stuart A. Herrington, USA (Ret)
Former Commander, US Army Foreign Counterintelligence Activity

"In the spy game, when you're penetrated – when someone is working for the other side inside your security world – they own you."

-- Richard Haver, Former Executive Director for IC Affairs and Former Special Asst to USD(I)

"…I became convinced that no intelligence service can be more effective than its counterintelligence component for very long."

-- Richard Helms, Former DCI and Director CIA
Richard Helms with William Hood, *A Look Over My shoulder: A Life in the Central Intelligence Agency* (2003), pp. 34-35

"In short, there appears to be no abatement in espionage either now or on the horizon."

-- Eli Jacobs, Chairman, Jacobs Panel
SSCI, S. Hrg. 101-1293, "S. 2726 to Improve U.S. Counterintelligence Measures," 101st Congress 2nd session, 1991, p. 9
(Testimony before the Senate Select Committee on Intelligence, 23 May 1980)

"No one can realistically expect that espionage will ever be totally eradicated. But we can take steps to minimize its occurrence and lessen its impact."

-- Senator David L. Boren, Chairman Senate Select Committee on Intelligence, 23 May 1990
SSCI, S. Hrg. 101-1293, "S. 2726 to Improve U.S. Counterintelligence Measures," 101st Congress 2nd session, 1991, p. 9

CI... A Never-Ending Necessity

*The Ten Commandments of Counterintelligence**

- I -- Be Offensive
- II -- Honor Your Professionals
- III -- Own the Street
- IV -- Know Your History
- V -- Do Not Ignore Analysis
- VI -- Do Not Be Parochial
- VII -- Train Your People
- VIII -- Do Not Be Shoved Aside
- IX -- Do Not Stay Too Long
- X -- Never Give Up

-- James M. Olson, Former Chief of CIA Counterintelligence
(served 31 years in the CIA)

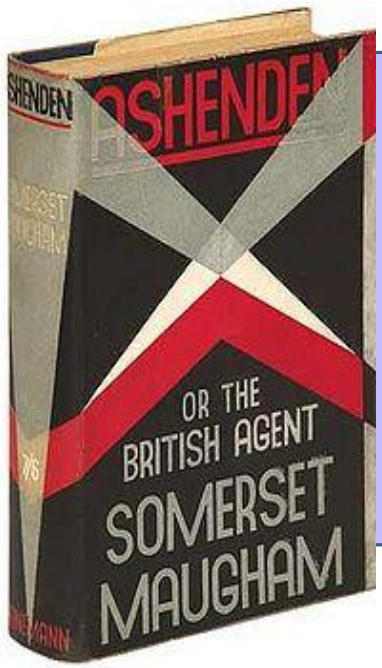
---

* James M. Olson, "The Ten Commandments of Counterintelligence," Center for the Study of Intelligence, CIA, *Studies in Intelligence*, Volume. 45 ,No. 5, Fall-Winter 2001, pp. 81-87; available online at <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article08.html>
Also available online at: <http://www.dtic.mil/dtic/tr/fulltext/u2/a529667.pdf>

To advance its interests, the United States will need to do what prudent statesmen have done in different ways for centuries: ensure that counterintelligence is adequate to the task.

-- Roy Godson, Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence (Washington: Brassey's 1995), pp. 238-239

Need for Counterintelligence…



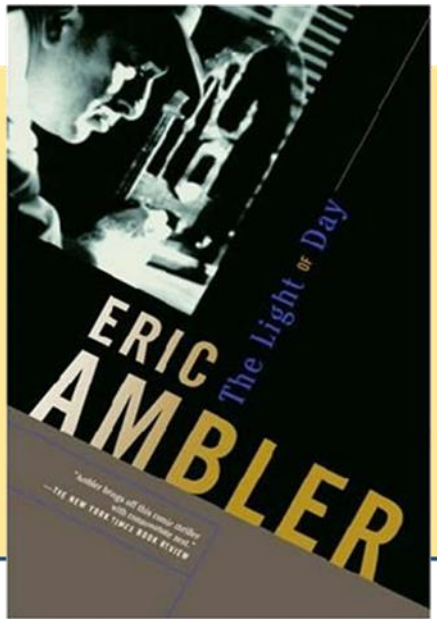
But there will always be espionage and there will always be counter-espionage. Though conditions may have altered, though difficulties may be greater…, there will always be secrets which one side jealously guards and which the other will use every means to discover; there will always be men who from malice or for money will betray their kith and kin and there will always be men who, from love of adventure or a sense of duty, will risk a shameful death to secure information valuable to their country.

W. Somerset Maugham, *Ashenden: or the British Agent* (1928)

Inescapable Truth… there will always be Spies

We must develop effective espionage and counterespionage services and must learn to subvert, sabotage and destroy our enemies by more clever, more sophisticated and more effective methods than those used against us.

-- Doolittle Report (1954)*



I think if I were asked to single out one specific group of men, one category as being the most suspicious, unbelieving, unreasonable, petty, inhuman, sadistic, double-crossing set of bastards in any language, I would say without hesitation the people who run counterespionage departments.

-- Eric Ambler, *Light of Day* (1962)

---

* *Report on the Covert Activities of the Central Intelligence Agency* (aka Doolittle Report), 30 Sep 1954, redacted copy (originally classified TOP SECRET). Lt Gen James H. Doolittle was the Chairman of this Presidential directed Special Study Group. One result of the report was the creation of a counterintelligence staff within CIA which was run by James J. Angleton from 1954 to 1974. Redacted copy available online at: <http://www.foia.cia.gov/helms/pdf/doolittle_report.pdf>

COUNTERINTELLIGENCE—*THE WILDERNESS OF MIRRORS*

Counterintelligence officers—people who specialize in catching spies—work in a part of the profession so labyrinthine that it is often referred to as a "wilderness of mirrors"…

-- H. Keith Melton and Robert Wallace, *The Official CIA Manual of Trickery and Deception* (2009)

One final perspective…

Counterintelligence… a wilderness of mirrors

"A wilderness of mirrors" -- a description of counterintelligence attributed to James J. Angleton. It comes from T.S. Eliot's poem "Gerontion" (1920); also the title of a 1980 book authored by David C. Martin about CIA counterintelligence.

Angleton was CIA's Chief of the Counterintelligence from 1954 until his retirement in 1974. In December 1974, Angleton was basically forced into retirement by the Director of CIA (William Colby), who became convinced that Angleton's "labyrinthine" approach to counterintelligence severely hampered the Agency's primary mission -- clandestine HUMINT collection.

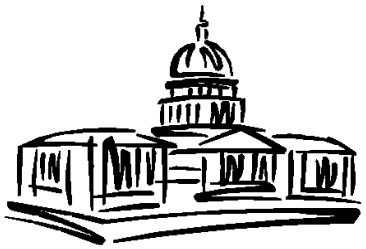
THE CHALLENGE: *THINKING THE UNTHINKABLE*

Most fundamental to counterintelligence–as true today as ever–is the need to "think the unthinkable." Yet this is one of the most difficult attitudes to instill and maintain because it runs contrary to human nature, especially in open societies like the United States. …

Today, thinking the unthinkable is not easier, but it is just as critical to our national security.

As we proceed to face the counterintelligence threat of the 21st century, we are faced with a host of challenges: some new, others ancient and deeply rooted in human weakness, and some not yet even invented.

-- Honorable Richard Shelby, Chairman of the U.S. Senate Select Committee on Intelligence (2001)*



To all Counterintelligence professionals --

Combating adversarial intelligence threats is a demanding and challenging profession… CI is a strategic instrument of national security underappreciated by most. A sincere thank you for all you do!!!!!!

-- COL Mark L. Reagan (USA Ret)
Editor, *Terms & Definitions of Interest for Counterintelligence Professionals*

CI a strategic enabler and a national asset…
Critical to U.S. National Security

---

* Quote from "Intelligence and Espionage in the 21st Century," Heritage Lectures - No. 705, The Heritage Foundation, 18 May 2001

Key Sources

A Spy's Journey: A CIA Memoir by Floyd L. Paseman. Minneapolis, MN: Zenith Press, 2004 (Glossary pp. 290-296) – cited as A Spy's Journey.

Consumer's Guide to Intelligence (PAS 95-00010), CIA, Public Affairs Staff, July 1995; updated, 2d ed. 1996; replaced with ***National Intelligence: A Consumer's Guide - 2009***, Office of Director National Intelligence (ODNI). Copy available online at: <www.dni.gov/reports/IC_Consumers_Guide_2009.pdf>

Counterintelligence Community Lexicon (CI Community Lexicon), National Counterintelligence Center, NACIC 2000-10004, June 2000 – cited as CI Community Lexicon.

Cyber Threats to National Security, Symposium Five: Keeping the Nation's Industrial Base Safe From Cyber Threats, co-sponsored by USNI, CACI and Center for Security Policy, 2011 -- cited as Cyber Threats to National Security, Symposium Five, 2011. Copy available online at: <http://asymetricthreat.net>

Cybersecurity and Cyberwar: What Everyone Needs to Know by P.W. Singer and Allan Friedman. New York, NY: Oxford University Press, 2014 – cited as Cybersecurity and Cyberwar.

DoD Dictionary of Military and Associated Terms, Joint Publication 1-02. Copy available online at: <http://www.dtic.mil/doctrine/dod_dictionary/> (also available at <https://jdeis.js.mil>) – cited as JP 1-02.

Domestic Investigations and Operations Guide [Redacted Version], Federal Bureau of Investigation, 15 Oct 2011. Copy available on line at: <http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version>

Encyclopedia of the Central Intelligence Agency by W. Thomas Smith, Jr. New York, NY: Checkmark Books, 2003 – cited as Encyclopedia of the CIA.

FBI Foreign Counterintelligence Terms in *Spy vs. Spy* by Ronald Kessler (1988) – cited as FBI FCI Terms.

Fair Play: The Moral Dilemmas of Spying by James M. Olson. Washington, DC: Potomac Books, Inc., 2006.

Glossary of Intelligence Terms and Definitions, The Intelligence Community Staff (ICS), Office of the Director of Central Intelligence, 1978; updated June 1989 – cited as ICS Glossary.

Glossary of Key Information Security Terms, NISTIR 7298 Revision 2, May 2013. Copy available at: <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>

Glossary of Security Terms, Definitions, and Acronyms, Intelligence Community Standard - Number 700-1 (previously numbered ICS 2008- 700-1), 4 April 2008 – cited as IC Standard 700-1 (33 pages). Available on line at: <http://www.ncix.gov/publications/policy/docs/ICS_700-01_Glossary_of_Security_Terms_Definitions_and_Acronyms.pdf>

Glossary of Security Terms, Definitions, and Acronyms, Defense Security Service, November 2012 – cited as DSS Glossary (337 pages). Copy available <http://www.cdse.edu/documents/cdse/Glossary_Handbook.pdf>

Glossary of Spy Terms, CI Centre – cited as CI Centre Glossary. Originally available online at <http://cicentre.com/LINKS_Reference_Material.htm> -- site now requires membership to access, see <http://www.cicentre.com/>

Historical Dictionary of Cold War Counterintelligence by Nigel West, Maryland: Scarecrow Press, Inc., 2007.

Human Derived Information Lexicon Terms and Definitions for HUMINT, Counterintelligence, and related Activities, April 2008 – cited as HDI Lexicon.

Intelligence Essentials for Everyone, by Lisa Krizen, Occasional Paper Number Six, Washington DC: DIA Joint Military Intelligence College, June 1999. Copy available online at: <http://www.dia.mil/college/pubs/8342.htm>

McAfee Labs - Threat Glossary**,** undated. Copy available online at: <http://www.mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx >

National Information Assurance (IA) Glossary, Committee on National Security Systems Instruction (CNSSI) No. 4009, 26 Apr 2010. Copy available on line at: <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf> Also at <http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf>

National Intelligence: A Consumer's Guide – 2009. Copy available online at: <http://www.dni.gov/reports/IC_Consumer's_Guide_2009.pdf>

National HUMINT Glossary, unclassified, 15 pages, undated. Copy available on JWICS at: <http://jwc-nhb-nhc03.idiss.cia.ic.gov/intelink/NationalHUMINTGlossary.pdf>

OPSEC Glossary of Terms. Interagency OPSEC Support Staff. Copy available online at: <http://www.ioss.gov/docs/definitions.html>

Spy Book – The Encyclopedia of Espionage by Norman Polmar and Thomas B. Allen, New York: Random House, revised edition, 2002 – cited as Spy Book.

Spy Dust: Two Masters of Disguise Reveal the Tools and Operations that Helped Win the Cold War by Antonio and Jonna Mendez, with Bruce Henderson, New York: Atria Books, 2002; Glossary pp. 283-298 (copy of glossary available on line at: <http://www.themasterofdisguise.com/glossary.html>) – cited as Spy Dust.

Spycraft: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda by Robert Wallace and H. Keith Melton, New York: Penguin Group, 2008 – cited as Spycraft.

U.S. National Intelligence – An Overview 2011, Office of the Director of National Intelligence. Copy available online at: <http://www.odni.gov/IC_Consumers_Guide_2011.pdf>

Words of Intelligence: An Intelligence Professional's Lexicon for Domestic and Foreign Threats, 2nd Edition, by Jan Goldman. Lanham, MD: Scarecrow Press, Inc., 2011 – cited as Words of Intelligence.

Notes:

DoD issuances (e.g., directives, instructions, DTMs) approved for public release available on the Internet from the DoD Issuances Website at: <http://www.dtic.mil/whs/directives/>. Also see <http://www.dtic.mil/doctrine/doctrine/doctrine.htm>.

Department of the Army publications at <https://www.apd.army.mil/> Also Army Field Manuals (FMs) are available online at: <http://armypubs.army.mil/doctrine/active_fm.html> (requires an AKO account). Selected Army publications are also at: <http://www.fas.org/irp/doddir/army/index.html>

Air Force doctrine at <http://www.cadre.maxwell.af.mil>

Navy doctrine at <https://ndls.nwdc.navy.mil>

Intelligence Community Intelligence Directives (ICDs), unclassified ICDs available online at: <http://www.dni.gov/electronic_reading_room.htm>
Also see <http://www.dni.gov/index.php/intelligence-community/ic-policies-reports/intelligence-community-directives>

United States law at <http://uscode.house.gov/lawrevisioncounsel.shtml>. United States Code (USC) also available online from the Government Printing Office online data base at: <http://www.gpoacess.gov/uscode/index.html>

Key DoD Counterintelligence Policy References

DoD Regulations

- *DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 Dec 1982; supplemented by DTM 08-11, Intelligence Oversight Policy Guidance, 26 Mar 2008 (w/ change 3 dated 27 Jul 2012)**

DoD Directives

- DoDD 5240.01, DoD Intelligence Activities, 27 Aug 2007 (with change 1 dated 29 Jan 2013)
- *DoDD O-5240.02, Counterintelligence, 20 Dec 2007 (with change 1 dated 30 Dec 2010)**
- DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR), 17 May 2011 (with change 1 dated 30 May 2013)
- *DoDD 5210.48, Polygraph and Credibility Assessment Program, 25 Jan 2007 (with change 2 dated 15 Nov 2013)**
- DoDD S-3325.09, (U) Oversight Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013 (with change 1 dated 13 Jun 2013)

DoD Instructions

- *DoDI 5240.04, Counterintelligence Investigations, 2 Feb 2009 (with change 1 dated 15 Oct 2013)**
- DoDI 5240.05, Technical Surveillance Countermeasures (TSCM) Program, 3 Apr 2014
- DoDI C-5240.08, Counterintelligence Security Classification Guide (U), 28 Nov 2011
- *DoDI S-5240.09, Offensive Counterintelligence Operations (OFCO) (U), 29 Oct 2008**
- DoDI 5240.10, Counterintelligence in the Combatant Commands and Other DoD Components, 5 Oct 2011 (with change 1 dated 15 Oct 2013)
- DoDI S-5240.15, Force Protection Response Group (FPRG) (U), 20 Oct 2010 (with change 1)
- DoDI 5240.16, DoD Counterintelligence Functional Services (CIFS), 27 Aug 2012 (with change 1)
- DoDI S-5240.17, (U) Counterintelligence Collection Acclivities (CCA), 14 Mar 2014
- DoDI 5240.18, Counterintelligence Analysis and Production, 17 Nov 2009 (with change 1)
- DoDI 5240.19, Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP), 31 Jan 2014
- DoDI O-5240.21, Counterintelligence Inquires, 14 May 2009 (with change 2 dated 15 Oct 2013)
- DoDI 5240.22, Counterintelligence Support to Force Protection, 24 Sep 2009 (with change 1)
- DoDI S-5240.23, Counterintelligence Activities in Cyberspace (U), 13 Dec 2010 (with change 1)
- DoDI O-5240.24, Counterintelligence Activities Supporting Research, Development, and Acquisition (RDA), 8 Jun 2011 (with change 1 dated 15 Oct 2013)
- DoDI 5240.25, Counterintelligence Badge and Credentials, 30 March 2012 (with change 1)
- DoDI 5240.26, Countering Espionage, International Terrorism, and the Counterintelligence Insider Threat, 4 May 2012 (with change 1 dated 15 Oct 2013)
- DoDI 5240.27, Joint Counterintelligence Training Academy (JCITA), 13 Nov 2013
- DoDI 3305.11, DoD Counterintelligence Training, 19 Mar 2007 (with change 2 dated 15 Oct 2013)
- DoDI 3305.12, Intelligence and Counterintelligence Training of Non-U.S. Persons, 25 Oct 2007 (with change 2 dated 15 Oct 2013)
- DoDI 5210.91, Polygraph and Credibility Assessment (PCA) Procedures, 12 Aug 2010 (with chg 1)
- *DoDI 5200.39, Critical Program Information (CPI) Protection within DoD, 16 Jul 2008 (with chg1)**

DoD Manuals

- DoD Manual S-5240.09-M, OFCO Procedures and Security Classification Guide (U), 13 Jan 2011

Under Development

- *DoD Manual S-5240.26-M, (U) DoD Counterintelligence Insider Threat Program (CIITP)**

**** under revision / under development***

Intelligence Community & Misc. Government Websites

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI): www.dni.gov
NATIONAL COUNTERINTELLIGENCE EXECUTIVE (NCIX): www.ncix.gov
NATIONAL COUNTERTERRORISM CENTER (NCTC): www.nctc.gov
DEPARTMENT OF DEFENSE (DoD): www.defense.gov (also see: www.defenselink.mil)
- Defense Intelligence Agency (DIA): www.dia.mil
- Defense Security Service (DSS): www.dss.mil
- Army: www.army.mil
  -- Intelligence & Security Command (INSCOM): www.inscom.army.mil
  -- 902d Military Intelligence Group: www.inscom.army.mil/MSC/902MIG.aspx
  -- Intelligence Knowledge Network (IKN): https://www.ikn.army.mil/
- Air Force: www.af.mil
  -- Air Force Office of Special Investigations (AFOSI): www.osi.andrews.af.mil
  -- Air Force ISR Agency: www.afisr.af.mil
- Navy: www.navy.mil
  -- Naval Criminal Investigative Service (NCIS): www.ncis.navy.mil
  -- Office of Naval Intelligence (ONI): www.nmic.navy.mil
- Marine Corp: www.marines.mil
  -- USMC Intelligence: www.hqinet001.hqmc.usmc.mil/DirInt/default.html

NATIONAL SECURITY AGENCY (NSA): www.nsa.gov
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA): www.nga.mil
NATIONAL RECONNAISSANCE OFFICE (NRO): www.nro.gov
CENTRAL INTELLIGENCE AGENCY (CIA): www.cia.gov
DEPARTMENT OF JUSTICE (DoJ): www.usdoj.gov
- Federal Bureau of Investigation (FBI): www.fbi.gov
- Drug Enforcement Agency (DEA): www.dea.gov
- DoJ Office of Legal Counsel (OLC): www.usdoj.gov/olc
- DoJ National Security Division (NSD): www.usdoj.gov/nsd

DEPARTMENT OF HOMELAND SECURITY (DHS): www.dhs.gov
- U.S. Coast Guard (USCG): www.uscg.mil
- Customs and Border Protection (CBP): http://cbp.gov/
- Immigrations and Customs Enforcement (ICE): www.ice.gov
- Transportation Security Administration (TSA): www.tsa.gov
- U.S. Secret Service (USSS): www.secretservice.gov
- DHS Office of Intelligence & Analysis: www.dhs.gov/xabout/structure/gc_1220886590914.shtm

DEPARTMENT OF STATE: www.state.gov
- Bureau of Diplomatic Security: www.state.gov/m/ds

DEPARTMENT OF TREASURY: www.ustreas.gov
- Office of Terrorism and Financial Intelligence: www.ustreas.gov/offices/enforcement/
- Financial Crimes Enforcement Network (FinCEN): www.fincen.gov

DEPARTMENT OF ENERGY: www.energy.gov
INTERAGENCY OPSEC SUPPORT STAFF (IOSS): www.ioss.gov
WHITE HOUSE: www.whitehouse.gov
U.S. SENATE: www.senate.gov
- Senate Select Committee on Intelligence (SSCI): www.intelligence.senate.gov

U.S. HOUSE OF REPRESENTATIVES: www.house.gov
- House Permanent Select Committee on Intelligence (HPSCI): www.intelligence.house.gov

LIBRARY OF CONGRESS: www.loc.gov
- Federal legislative information available at: www.thomas.loc.gov

NSTISSI No. 4009
September 2000

NATIONAL INFORMATION SYSTEMS SECURITY (INFOSEC) GLOSSARY

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

Page 3877 of 3957

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 SEP 2000	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
National Information Systems Security (INFOSEC) Glossary	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Security Agency, 9800 Savage Road, STE 6716, Ft. Meade, MD 20755-6716**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
National Security Agency, (410) 854-6805, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**80**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

National Security Telecommunications and Information Systems Security Committee

National Manager

FOREWORD

1. The NSTISSC Glossary Working Group recently convened to review terms submitted by the NSTISSC membership since the Glossary was last published in 1999. This edition incorporates those terms.

2. We recognize that, to remain useful, a glossary must be in a continuous state of coordination, and we encourage your review and welcome your comments. The goal of the Glossary Working Group is to keep pace with changes in information systems security terminology and meet regularly to consider comments.

3. The Working Group would like your help in keeping up to date as new terms come into being and old terms fall into disuse or change meaning. Some terms from the previous version were deleted, others updated or added, and some are identified as candidates for deletion (C.F.D.). If a term you still find valuable and need in your environment has been deleted, please resubmit the term with a definition based on the following criteria: (a) specific relevance to the security of information systems; (b) economy of words; (c) accuracy; and (d) clarity. Use these same criteria to recommend any changes to existing definitions or suggest new terms. In all cases, send your suggestions to the NSTISSC Secretariat via mail or fax (410) 854-6814.

4. Representatives of the NSTISSC may obtain additional copies of this instruction at the address listed below.

MICHAEL V. HAYDEN
Lieutenant General, USAF

NSTISSC Secretariat (I42). National Security Agency.9800 Savage Road STE 6716. Ft Meade MD 20755-6716
(410) 854-6805.UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

Page 3879 of 3957

SECTION I

TERMS AND DEFINITIONS

A

A1	Highest level of trust defined in the Orange Book (Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD).
access	Opportunity to make use of an information system (IS) resource.
access control	Limiting access to information system resources only to authorized users, programs, processes, or other systems.
access control list (ACL)	Mechanism implementing discretionary and/or mandatory access control between subjects and objects.
access control mechanism	Security safeguard designed to detect and deny unauthorized access and permit authorized access in an IS.
access control officer (ACO)	Designated individual responsible for limiting access to information systems resources.
access level	Hierarchical portion of the security level used to identify the sensitivity of IS data and the clearance or authorization of users. Access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. See category.
access list	(IS) Compilation of users, programs, or processes and the access levels and types to which each is authorized. (COMSEC) Roster of persons authorized admittance to a controlled area.
access period	Segment of time, generally expressed in days or weeks, during which access rights prevail.

access profile	Associates each user with a list of protected objects the user may access.
access type	Privilege to perform action on an object. Read, write, execute, append, modify, delete, and create are examples of access types.
accountability	(IS) Process of tracing IS activities to a responsible source. (COMSEC) Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.
accounting legend code (ALC)	Numeric code used to indicate the minimum accounting controls required for items of accountable COMSEC material within the COMSEC Material Control System.
accounting number	Number assigned to an item of COMSEC material to facilitate its control.
accreditation	Formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.
accreditation package	Product comprised of a System Security Plan (SSP) and a report documenting the basis for the accreditation decision.
accrediting authority	Synonymous with Designated Approving Authority (DAA).
add-on security	Incorporation of new hardware, software, or firmware safeguards in an operational IS.
advisory	Notification of significant new trends or developments regarding the threat to the IS of an organization. This notification may include analytical insights into trends, intentions,

	technologies, or tactics of an adversary targeting ISs.
alert	Notification that a specific attack has been directed at the IS of an organization.
alternate COMSEC custodian	Person designated by proper authority to perform the duties of the COMSEC custodian during the temporary absence of the COMSEC custodian.
anti-jam	Measures ensuring that transmitted information can be received despite deliberate jamming attempts.
anti-spoof	Measures preventing an opponent's participation in an IS.
assembly	Group of parts, elements, subassemblies, or circuits that are removable items of COMSEC equipment.
assurance	See information assurance.
attack	Type of incident involving the intentional act of attempting to bypass one or more security controls (see Information Assurance) of an IS.
attention character	In Trusted Computing Base (TCB) design, a character entered from a terminal that tells the TCB the user wants a secure communications path from the terminal to some trusted code to provide a secure service for the user.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
audit trail	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. Audit trail may apply to information in an IS, to message routing in a communications system, or to the transfer of COMSEC material.

UNCLASSIFIED

authenticate	To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IS, or to establish the validity of a transmission.
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
authentication system	Cryptosystem or process used for authentication.
authenticator	Means used to confirm the identity of a station, originator, or individual.
authorization	Access privileges granted to a user, program, or process.
authorized vendor	Manufacturer of INFOSEC equipment authorized to produce quantities in excess of contractual requirements for direct sale to eligible buyers. Eligible buyers are typically U.S. Government organizations or U.S. Government contractors.
Authorized Vendor Program (AVP)	Program in which a vendor, producing an INFOSEC product under contract to NSA, is authorized to produce that product in numbers exceeding the contracted requirements for direct marketing and sale to eligible buyers. Eligible buyers are typically U.S. Government organizations or U.S. Government contractors. Products approved for marketing and sale through the AVP are placed on the Endorsed Cryptographic Products List (ECPL).
automated security monitoring	Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the IS.
automatic remote rekeying	Procedure to rekey a distant crypto-equipment electronically without specific actions by the receiving terminal operator.
availability	Timely, reliable access to data and information services for authorized users.

B

back door	Hidden software or hardware mechanism used to circumvent security controls. Synonymous with trap door.
backup	Copy of files and programs made to facilitate recovery, if necessary.
banner	Display on an IS that sets parameters for system or data use.
Bell-La Padula security model	Formal-state transition model of a computer security policy that describes a formal set of access controls based on information sensitivity and subject authorizations. See star (*) property and simple security property.
benign	Condition of cryptographic data that cannot be compromised by human access.
benign environment	Nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures.
beyond A1	Level of trust defined by the DoD Trusted Computer System Evaluation Criteria (TCSEC) to be beyond the state-of-the-art technology. It includes all the Al-level features plus additional ones not required at the Al-level.
binding	Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information.
biometrics	Automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic.
bit error rate	Ratio between the number of bits incorrectly received and the total number of bits transmitted in a telecommunications system.
BLACK	Designation applied to information systems, and to associated areas, circuits, components, and

	equipment, in which national security information is encrypted or is not processed.
boundary	Software, hardware, or physical barrier that limits access to a system or part of a system.
brevity list	List containing words and phrases used to shorten messages.
browsing	Act of searching through IS storage to locate or acquire information, without necessarily knowing the existence or format of information being sought.
bulk encryption	Simultaneous encryption of all channels of a multichannel telecommunications link.

C

call back	Procedure for identifying and authenticating a remote IS terminal, whereby the host system disconnects the terminal and reestablishes contact. Synonymous with dial back.
canister	Type of protective package used to contain and dispense key in punched or printed tape form.
capability	Protected identifier that both identifies the object and specifies the access rights to be allowed to the subject who possesses the capability. In a capability-based system, access to protected objects such as files is granted if the would-be subject possesses a capability for the object.
cascading	Downward flow of information through a range of security levels greater than the accreditation range of a system network or component.
category	Restrictive label applied to classified or unclassified information to limit access.
CCI assembly	Device embodying a cryptographic logic or other COMSEC design that NSA has approved as a Controlled Cryptographic Item (CCI). It performs

	the entire COMSEC function, but depends upon the host equipment to operate.
CCI component	Part of a Controlled Cryptographic Item (CCI) that does not perform the entire COMSEC function but depends upon the host equipment, or assembly, to complete and operate the COMSEC function.
CCI equipment	Telecommunications or information handling equipment that embodies a Controlled Cryptographic Item (CCI) component or CCI assembly and performs the entire COMSEC function without dependence on host equipment to operate.
central office of record (COR)	Office of a federal department or agency that keeps records of accountable COMSEC material held by elements subject to its oversight.
certificate	Record holding security information about an IS user and vouches to the truth and accuracy of the information it contains.
certificate management	Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.
certificate revocation list (CRL)	List of invalid certificates (as defined above) that have been revoked by the issuer.
certification	Comprehensive evaluation of the technical and nontechnical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.
certification authority (CA)	Third level of the Public Key Infrastructure (PKI) Certification Management Authority responsible for issuing and revoking user certificates, and exacting compliance to the PKI policy as defined by the parent Policy Creation Authority (PCA).
certification authority workstation (CAW)	Commercial-off-the-shelf (COTS) workstation with a trusted operating system and special purpose application software that is used to issue certificates.

certification package	Product of the certification effort documenting the detailed results of the certification activities.
certification test and evaluation (CT&E)	Software and hardware security tests conducted during development of an IS.
certified TEMPEST technical authority (CTTA)	An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with NSTISSC-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.
certifier	Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.
challenge and reply authentication	Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply.
checksum	Value computed on data to detect error or manipulation during transmission. See hash total.
check word	Cipher text generated by cryptographic logic to detect failures in cryptography.
cipher	Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both.
cipher text	Enciphered information.
cipher text auto-key (CTAK)	Cryptographic logic that uses previous cipher text to generate a key stream.
ciphony	Process of enciphering audio information, resulting in encrypted speech.
classified information	Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended,

	to require protection against unauthorized disclosure and is marked to indicate its classified status.
clearing	Removal of data from an IS, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., keyboard strokes); however, the data may be reconstructed using laboratory methods. Cleared media may be reused at the same classification level or at a higher level. Overwriting is one method of clearing.
closed security environment	Environment providing sufficient assurance that applications and equipment are protected against the introduction of malicious logic during an IS life cycle. Closed security is based upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control.
code	(COMSEC) System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.
code book	Document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique.
code group	Group of letters, numbers, or both in a code system used to represent a plain text word, phrase, or sentence.
code vocabulary	Set of plain text words, numerals, phrases, or sentences for which code equivalents are assigned in a code system.
cold start	Procedure for initially keying crypto-equipment.
command authority	Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

Commercial COMSEC Endorsement Program (CCEP)	Relationship between NSA and industry in which NSA provides the COMSEC expertise (i.e., standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products developed under the CCEP may include modules, subsystems, equipment, systems, and ancillary devices.
common criteria	Provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (Information Technology Security Evaluation Criteria [ITSEC])
common fill device	One of a family of devices developed to read-in, transfer, or store key.
communications cover	Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.
communications deception	Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications. See imitative communications deception and manipulative communications deception.
communications profile	Analytic model of communications associated with an organization or activity. The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the communications security measures applied.
communications security (COMSEC)	Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.
compartmentalization	A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone.

compartmented mode	INFOSEC mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following: (a) valid security clearance for the most restricted information processed in the system; (b) formal access approval and signed nondisclosure agreements for that information which a user is to have access; and (c) valid need-to-know for information which a user is to have access.
compromise	Type of incident where information is disclosed to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
compromising emanations	Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information systems equipment. See TEMPEST.
computer abuse	Intentional or reckless misuse, alteration, disruption, or destruction of information processing resources.
computer cryptography	Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information.
computer security	Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated.
computer security incident	See incident.
computer security subsystem	Hardware/software designed to provide computer security features in a larger system environment.
COMSEC account	Administrative entity, identified by an account number, used to maintain accountability, custody, and control of COMSEC material.
COMSEC account audit	Examination of the holdings, records, and procedures of a COMSEC account ensuring all

	accountable COMSEC material is properly handled and safeguarded.
COMSEC aid	COMSEC material that assists in securing telecommunications and is required in the production, operation, or maintenance of COMSEC systems and their components. COMSEC keying material, callsign/frequency systems, and supporting documentation, such as operating and maintenance manuals, are examples of COMSEC aids.
COMSEC boundary	Definable perimeter encompassing all hardware, firmware, and software components performing critical COMSEC functions, such as key generation and key handling and storage.
COMSEC chip set	Collection of NSA approved microchips.
COMSEC control program	Computer instructions or routines controlling or affecting the externally performed functions of key generation, key distribution, message encryption/decryption, or authentication.
COMSEC custodian	Person designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding, and destruction of COMSEC material assigned to a COMSEC account.
COMSEC end-item	Equipment or combination of components ready for use in a COMSEC application.
COMSEC equipment	Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes crypto-equipment, crypto-ancillary equipment, cryptoproduction equipment, and authentication equipment.
COMSEC facility	Space used for generating, storing, repairing, or using COMSEC material.

COMSEC incident	See incident.
COMSEC insecurity	COMSEC incident that has been investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information.
COMSEC manager	Person who manages the COMSEC resources of an organization.
COMSEC material	Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.
COMSEC Material Control System (CMCS)	Logistics and accounting system through which COMSEC material marked "CRYPTO" is distributed, controlled, and safeguarded. Included are the COMSEC central offices of record, cryptologistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the CMCS.
COMSEC modification	See information systems security equipment modification.
COMSEC module	Removable component that performs COMSEC functions in a telecommunications equipment or system.
COMSEC monitoring	Act of listening to, copying, or recording transmissions of one's own official telecommunications to analyze the degree of security.
COMSEC profile	Statement of COMSEC measures and materials used to protect a given operation, system, or organization.
COMSEC survey	Organized collection of COMSEC and communications information relative to a given operation, system, or organization.

COMSEC system data	Information required by a COMSEC equipment or system to enable it to properly handle and control key.
COMSEC training	Teaching of skills relating to COMSEC accounting, use of COMSEC aids, or installation, use, maintenance, and repair of COMSEC equipment.
concept of operations (CONOP)	Document detailing the method, act, process, or effect of using an IS.
confidentiality	Assurance that information is not disclosed to unauthorized persons, processes, or devices.
configuration control	Process of controlling modifications to hardware, firmware, software, and documentation to ensure the IS is protected against improper modifications prior to, during, and after system implementation.
configuration management	Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IS.
confinement channel	See covert channel.
confinement property	Synonymous with star (*) property.
contamination	Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category.
contingency key	Key held for use under specific operational conditions or in support of specific contingency plans.
contingency plan	Plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.
controlled access protection	The C2 level of protection described in the Trusted Computer System Evaluation Criteria (Orange Book). Its major characteristics are: individual

	accountability, audit, access control, and object reuse.
controlled cryptographic item (CCI)	Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. Such items are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI."
controlled security mode	See multilevel security.
controlled sharing	Condition existing when access control is applied to all users and components of an IS.
controlled space	Three-dimensional space surrounding IS equipment, within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance.
controlling authority	Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet.
cooperative key generation	Electronically exchanging functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit.
cooperative remote rekeying	Synonymous with manual remote rekeying.
correctness proof	A mathematical proof of consistency between a specification and its implementation.
countermeasure	Action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.
covert channel	Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an IS security policy. See overt channel and exploitable channel.
covert channel analysis	Determination of the extent to which the security policy model and subsequent lower-level program

	descriptions may allow unauthorized access to information.
covert storage channel	Covert channel involving the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.
covert timing channel	Covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process.
credentials	Information, passed from one entity to another, used to establish the sending entity's access rights.
critical infrastructures	Those physical and cyber-based systems essential to the minimum operations of the economy and government.
cryptanalysis	Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.
CRYPTO	Marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information.
crypto-alarm	Circuit or device that detects failures or aberrations in the logic or operation of crypto-equipment. Crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm.
crypto-algorithm	Well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as

	encryption/decryption, key generation, authentication, signatures, etc.
crypto-ancillary equipment	Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, without performing cryptographic functions itself.
crypto-equipment	Equipment that embodies a cryptographic logic.
cryptographic	Pertaining to, or concerned with, cryptography.
cryptographic component	Hardware or firmware embodiment of the cryptographic logic. A cryptographic component may be a modular assembly, a printed wiring assembly, a microcircuit, or a combination of these items.
cryptographic equipment room (CER)	Controlled-access room in which cryptosystems are located.
cryptographic initialization	Function used to set the state of a cryptographic logic prior to key generation, encryption, or other operating mode.
cryptographic logic	The embodiment of one (or more) crypto-algorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic process(es).
cryptographic randomization	Function that randomly determines the transmit state of a cryptographic logic.
cryptography	Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.
crypto-ignition key (CIK)	Device or electronic key used to unlock the secure mode of crypto-equipment.
cryptology	Field encompassing both cryptography and cryptanalysis.
cryptonet	Stations holding a common key.
cryptoperiod	Time span during which each key setting remains in effect.

cryptosecurity	Component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.
cryptosynchronization	Process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic.
cryptosystem	Associated INFOSEC items interacting to provide a single means of encryption or decryption.
cryptosystem analysis	Process of establishing the exploitability of a cryptosystem, normally by reviewing transmitted traffic protected or secured by the system under study.
cryptosystem evaluation	Process of determining vulnerabilities of a cryptosystem.
cryptosystem review	Examination of a cryptosystem by the controlling authority ensuring its adequacy of design and content, continued need, and proper distribution.
cryptosystem survey	Management technique in which actual holders of a cryptosystem express opinions on the system's suitability and provide usage information for technical evaluations.
cyclic redundancy check	Error checking mechanism that checks data integrity by computing a polynomial algorithm based checksum.

D

dangling threat	Set of properties about the external environment for which there is no corresponding vulnerability and therefore no implied risk.
dangling vulnerability	Set of properties about the internal environment for which there is no corresponding threat and, therefore, no implied risk.

data aggregation	The compilation of unclassified individual data systems and data elements resulting in the totality of the information being classified.
data encryption standard (DES)	Cryptographic algorithm, designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46.
data flow control	Synonymous with information flow control.
data integrity	Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
data origin authentication	Corroborating the source of data is as claimed.
data security	Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.
data transfer device (DTD)	Fill device designed to securely store, transport, and transfer electronically both COMSEC and TRANSEC key, designed to be backward compatible with the previous generation of COMSEC common fill devices, and programmable to support modern mission systems.
decertification	Revocation of the certification of an IS item or equipment for cause.
decipher	Convert enciphered text to plain text by means of a cryptographic system.
decode	Convert encoded text to plain text by means of a code.
decrypt	Generic term encompassing decode and decipher.
dedicated mode	IS security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following: a. valid security clearance for all information within the system; b. formal access approval and signed nondisclosure agreements for all the information stored and/or

Page 3898 of 3957

	processed (including all compartments, subcompartments, and/or special access programs); and c. valid need-to-know for all information contained within the IS. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.
default classification	Temporary classification reflecting the highest classification being processed in an IS. Default classification is included in the caution statement affixed to an object.
degaussing	Procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing.
delegated development program	INFOSEC program in which the Director, NSA, delegates, on a case by case basis, the development and/or production of an entire telecommunications product, including the INFOSEC portion, to a lead department or agency.
denial of service	Type of incident resulting from any action or series of actions that prevents any part of an IS from functioning.
depot maintenance	See full maintenance.
descriptive top-level specification	Top-level specification written in a natural language (e.g., English), an informal design notation, or a combination of the two. Descriptive top-level specification, required for a class B2 and B3 (as defined in the Orange Book, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD) information system, completely and accurately describes a trusted computing base. See formal top-level specification.
design controlled spare part (DCSP) (C.F.D.)	Part or subassembly for a COMSEC equipment or device with an NSA controlled design.
design documentation	Set of documents, required for Trusted Computer System Evaluation Criteria (TCSEC) classes C1

	and above (as defined in the Orange Book, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD), whose primary purpose is to define and describe the properties of a system. As it relates to TCSEC, design documentation provides an explanation of how the security policy of a system is translated into a technical solution via the Trusted Computing Base (TCB) hardware, software, and firmware.
designated approving authority (DAA)	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.
dial back	Synonymous with call back.
digital signature	Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation.
digital signature algorithm	Procedure that appends data to, or performs a cryptographic transformation of, a data unit. The appended data or cryptographic transformation allows reception of the data unit and protects against forgery, e.g., by the recipient.
direct shipment	Shipment of COMSEC material directly from NSA to user COMSEC accounts.
discretionary access control (DAC)	Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject. See mandatory access control.
distinguished name	Globally unique identifier representing an individual's identity.
DoD Trusted Computer System Evaluation Criteria (TCSEC)	Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and software security

	controls built into an IS. This document, DoD 5200.28 STD, is frequently referred to as the Orange Book.
domain	Unique context (e.g., access control parameters) in which a program is operating; in effect, the set of objects a subject has the privilege to access.
dominate	Term used to compare IS security levels. Security level S1 is said to dominate security level S2, if the hierarchical classification of S1 is greater than, or equal to, that of S2 and the non-hierarchical categories of S1 include all those of S2 as a subset.
drop accountability	Procedure under which a COMSEC account custodian initially receipts for COMSEC material, and then provides no further accounting for it to its central office of record. Local accountability of the COMSEC material may continue to be required. See accounting legend code.

E

electronically generated key	Key generated in a COMSEC device by introducing (either mechanically or electronically) a seed key into the device and then using the seed, together with a software algorithm stored in the device, to produce the desired key.
Electronic Key Management System (EKMS)	Interoperable collection of systems being developed by services and agencies of the U.S. Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.
electronic messaging services	Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business-quality electronic mail service suitable for the conduct of official government business.

electronic security (ELSEC)	Protection resulting from measures designed to deny unauthorized persons information derived from the interception and analysis of noncommunications electromagnetic radiations.
element	Removable item of COMSEC equipment, assembly, or subassembly; normally consisting of a single piece or group of replaceable parts.
embedded computer	Computer system that is an integral part of a larger system.
embedded cryptography	Cryptography engineered into an equipment or system whose basic function is not cryptographic.
embedded cryptographic system	Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem.
emissions security (EMSEC)	Protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from crypto-equipment or an IS.
encipher	Convert plain text to cipher text by means of a cryptographic system.
encode	Convert plain text to cipher text by means of a code.
encrypt	Generic term encompassing encipher and encode.
encryption algorithm	Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.
end-item accounting	Accounting for all the accountable components of a COMSEC equipment configuration by a single short title.
end-to-end encryption	Encryption of information at its origin and decryption at its intended destination without intermediate decryption.
end-to-end security	Safeguarding information in an IS from point of origin to point of destination.

endorsed for unclassified cryptographic item (EUCI)	Unclassified cryptographic equipment that embodies a U.S. Government classified cryptographic logic and is endorsed by NSA for the protection of national security information. See type 2 product.
endorsement	NSA approval of a commercially developed product for safeguarding national security information.
entrapment	Deliberate planting of apparent flaws in an IS for the purpose of detecting attempted penetrations.
environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an IS.
erasure	Process intended to render magnetically stored information irretrievable by normal means.
Evaluated Products List (EPL)	Equipment, hardware, software, and/or firmware evaluated by the National Computer Security Center (NCSC) in accordance with DoD TCSEC and found to be technically compliant at a particular level of trust. The EPL is included in the NSA Information Systems Security Products and Services Catalogue.
event	Occurrence, not yet assessed, that may effect the performance of an IS.
executive state	One of several states in which an IS may operate, and the only one in which certain privileged instructions may be executed. Such privileged instructions cannot be executed when the system is operating in other states. Synonymous with supervisor state.
exercise key	Key used exclusively to safeguard communications transmitted over-the-air during military or organized civil training exercises.
exploitable channel	Channel that allows the violation of the security policy governing an IS and is usable or detectable by subjects external to the trusted computing base. See covert channel.

extraction resistance	Capability of crypto-equipment or secure telecommunications equipment to resist efforts to extract key.

F

fail safe	Automatic protection of programs and/or processing systems when hardware or software failure is detected.
fail soft	Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent.
failure access	Type of incident in which unauthorized access to data results from hardware or software failure.
failure control	Methodology used to detect imminent hardware or software failure and provide fail safe or fail soft recovery.
fetch protection	IS hardware provided restriction to prevent a program from accessing data in another user's segment of storage.
file protection	Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents.
file security	Means by which access to computer files is limited to authorized users only.
fill device	COMSEC item used to transfer or store key in electronic form or to insert key into a crypto-equipment.
FIREFLY	Key management protocol based on public key cryptography.
firewall	System designed to defend against unauthorized access to or from a private network.
firmware	Program recorded in permanent or semipermanent computer memory.

fixed COMSEC facility	COMSEC facility located in an immobile structure or aboard a ship.
flaw	Error of commission, omission, or oversight in an IS that may allow protection mechanisms to be bypassed.
flaw hypothesis methodology	System analysis and penetration technique in which the specification and documentation for an IS are analyzed to produce a list of hypothetical flaws. This list is prioritized on the basis of the estimated probability that a flaw exists on the ease of exploiting it, and on the extent of control or compromise it would provide. The prioritized list is used to perform penetration testing of a system.
flooding	Type of incident involving insertion of a large volume of data resulting in denial of service.
formal access approval	Documented approval by a data owner allowing access to a particular category of information.
formal development methodology	Software development strategy that proves security design specifications.
formal proof	Complete and convincing mathematical argument presenting the full logical justification for each proof step and for the truth of a theorem or set of theorems.
formal security policy model	Mathematically precise statement of a security policy. Such a model must define a secure state, an initial state, and how the model represents changes in state. The model must be shown to be secure by proving the initial state is secure and all possible subsequent states remain secure.
formal top-level specification	Top-level specification written in a formal mathematical language to allow theorems, showing the correspondence of the system specification to its formal requirements, to be hypothesized and formally proven.
formal verification	Process of using formal proofs to demonstrate the consistency between formal specification of a system and formal security policy model (design

	verification) or between formal specification and its high-level program implementation (implementation verification).
frequency hopping	Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications.
front-end security filter	Security filter logically separated from the remainder of an IS to protect system integrity. Synonymous with firewall.
full maintenance	Complete diagnostic repair, modification, and overhaul of INFOSEC equipment, including repair of defective assemblies by piece part replacement. Also known as depot maintenance. See limited maintenance.
functional proponent	See network sponsor.
functional testing	Segment of security testing in which advertised security mechanisms of an IS are tested under operational conditions.

G

gateway	Interface providing a compatibility between networks by converting transmission speeds, protocols, codes, or security measures.
granularity	Relative fineness to which an access control mechanism can be adjusted.
guard	Process limiting the exchange of information between systems.
Gypsy verification environment	Integrated set of software tools for specifying, coding, and verifying programs written in the Gypsy language.

H

hacker	Unauthorized user who attempts to or gains access to an IS.
handshaking procedures	Dialogue between two IS's for synchronizing, identifying, and authenticating themselves to one another.
hard copy key	Physical keying material, such as printed key lists, punched or printed key tapes, or programmable, read-only memories (PROM).
hardwired key	Permanently installed key.
hash total	Value computed on data to detect error or manipulation. See checksum.
hashing	Computation of a hash total.
hashword	Memory address containing hash total.

I

identification	Process an IS uses to recognize an entity.
identity token	Smart card, metal key, or other physical object used to authenticate identity.
identity validation	Tests enabling an IS to authenticate users or resources.
imitative communications deception	Introduction of deceptive messages or signals into an adversary's telecommunications signals. See communications deception and manipulative communications deception.
impersonating	Form of spoofing.
implant	Electronic device or electronic equipment modification designed to gain unauthorized interception of information-bearing emanations.

UNCLASSIFIED

inadvertent disclosure	Type of incident involving accidental exposure of information to a person not authorized access.
incident	(IS) Assessed occurrence having actual or potentially adverse effects on an IS. (COMSEC) Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information or information governed by 10 U.S.C. Section 2315.
incomplete parameter checking	System flaw that exists when the operating system does not check all parameters fully for accuracy and consistency, thus making the system vulnerable to penetration.
indicator	A recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.
individual accountability	Ability to associate positively the identity of a user with the time, method, and degree of access to an IS.
information assurance (IA)	Information operations that (IO) protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
information environment	Aggregate of individuals, organizations, or systems that collect, process, or disseminate information, also included is the information itself.
information flow control	Procedure to ensure that information transfers within an IS are not made from a higher security level object to an object of a lower security level.
information operations (IO)	Actions taken to affect adversary information and ISs while defending one's own information and ISs.
information system (IS)	The entire infrastructure, organization, personnel, and components for the collection, processing,

	storage, transmission, display, dissemination, and disposition of information.
information systems security (INFOSEC and/or ISS)	Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.
information systems security engineering (ISSE)	Effort to achieve and maintain optimal security and survivability of a system throughout its life cycle.
information systems security equipment modification	Modification of any fielded hardware, firmware, software, or portion thereof, under NSA configuration control. There are three classes of modifications: mandatory (to include human safety); optional/special mission modifications; and repair actions. These classes apply to elements, subassemblies, equipment, systems, and software packages performing functions such as key generation, key distribution, message encryption, decryption, authentication, or those mechanisms necessary to satisfy security policy, labeling, identification, or accountability.
information systems security manager (ISSM)	Principal advisor on computer security matters.
information systems security officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer.
information systems security product	Item (chip, module, assembly, or equipment), technique, or service that performs or relates to information systems security.
initialize	Setting the state of a cryptographic logic prior to key generation, encryption, or other operating mode.

inspectable space	Three dimensional space surrounding equipment that process classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists. Synonymous with zone of control.
integrity	Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.
integrity check value	Checksum capable of detecting modification of an IS.
interface	Common boundary between independent systems or modules where interactions take place.
interface control document	Technical document describing interface controls and identifying the authorities and responsibilities for ensuring the operation of such controls. This document is baselined during the preliminary design review and is maintained throughout the IS lifecycle.
interim approval	Temporary authorization granted by a DAA for an IS to process information based on preliminary results of a security evaluation of the system.
internal security controls	Hardware, firmware, or software features within an IS that restrict access to resources only to authorized subjects.
internetwork private line interface	Network cryptographic unit that provides secure connections, singularly or in simultaneous multiple connections, between a host and a predetermined set of corresponding hosts.
internet protocol (IP)	Standard protocol for transmission of data from source to destinations in packet-switched

	communications networks and interconnected systems of such networks.
intrusion	Unauthorized act of bypassing the security mechanisms of a system.

K

key	Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, or for determining electronic counter-countermeasures patterns, or for producing other key.
key-auto-key (KAK)	Cryptographic logic using previous key to produce key.
key card (C.F.D.)	Paper card, containing a pattern of punched holes, that establishes key for a specific cryptonet at a specific time.
key distribution center (KDC)	COMSEC facility generating and distributing key in electrical form.
key-encryption-key (KEK)	Key that encrypts or decrypts other key for transmission or storage.
key list	Printed series of key settings for a specific cryptonet. Key lists may be produced in list, pad, or printed tape format.
key management	Supervision and control of the process whereby key is generated, stored, protected, transferred, loaded, used, and destroyed.
key pair	Public key and its corresponding private key as used in public key cryptography.
key production key (KPK)	Key used to initialize a keystream generator for the production of other electronically generated key.

key recovery	Mechanisms and processes that allow authorized parties to retrieve the cryptographic key used for data confidentiality.
key stream	Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce key.
key tag	Identification information associated with certain types of electronic key.
key tape	Punched or magnetic tape containing key. Printed key in tape form is referred to as a key list.
key updating	Irreversible cryptographic process for modifying key.
keying material	Key, code, or authentication information in physical or magnetic form.

L

label	See security label.
labeled security protections	Elementary-level mandatory access control protection features and intermediate-level discretionary access control features in a TCB that uses sensitivity labels to make access control decisions.
laboratory attack	Use of sophisticated signal recovery equipment in a laboratory environment to recover information from data storage media.
least privilege	Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IS.
level of protection	Extent to which protective measures, techniques, and procedures must be applied to ISs and

	networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. Levels of protection are: 1. Basic: IS and networks requiring implementation of standard minimum security countermeasures. 2. Medium: IS and networks requiring layering of additional safeguards above the standard minimum security countermeasures. 3. High: IS and networks requiring the most stringent protection and rigorous security countermeasures.
limited maintenance	COMSEC maintenance restricted to fault isolation, removal, and replacement of plug-in assemblies. Soldering or unsoldering usually is prohibited in limited maintenance. See full maintenance.
line conditioning	Elimination of unintentional signals or noise induced or conducted on a telecommunications or IS signal, power, control, indicator, or other external interface line.
line conduction	Unintentional signals or noise induced or conducted on a telecommunications or IS signal, power, control, indicator, or other external interface line.
link encryption	Encryption of information between nodes of a communications system.
list-oriented	IS protection in which each protected object has a list of all subjects authorized to access it. See also ticket-oriented.
local authority	Organization responsible for generating and signing user certificates.
Local Management Device/ Key Processor (LMD/KP)	An EKMS platform providing automated management of COMSEC material and generating key for designated users.
lock and key protection system	Protection system that involves matching a key or password with a specific access requirement.

logic bomb	Resident computer program triggering an unauthorized act when particular states of an IS are realized.
logical completeness measure	Means for assessing the effectiveness and degree to which a set of security and access control mechanisms meets security specifications.
long title	Descriptive title of a COMSEC item.
low probability of detection	Result of measures used to hide or disguise intentional electromagnetic transmissions.
low probability of intercept	Result of measures to prevent the intercept of intentional electromagnetic transmissions.

M

magnetic remanence	Magnetic representation of residual information remaining on a magnetic medium after the medium has been cleared. See clearing.
maintenance hook	Special instructions (trapdoors) in software allowing easy maintenance and additional feature development. Since maintenance hooks frequently allow entry into the code without the usual checks, they are a serious security risk if they are not removed prior to live implementation.
maintenance key	Key intended only for in-shop use.
malicious applets	Small application programs automatically downloaded and executed that perform an unauthorized function on an IS.
malicious code	Software or firmware capable of performing an unauthorized process on an IS.
malicious logic	Hardware, software, or firmware capable of performing an unauthorized function on an IS.
mandatory access control (MAC)	Means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access

	approvals, and need-to-know) of subjects to access information of such sensitivity. See discretionary access control.
mandatory modification	Change to a COMSEC end-item that NSA requires to be completed and reported by a specified date. See optional modification.
manipulative communications deception	Alteration or simulation of friendly telecommunications for the purpose of deception. See communications deception and imitative communications deception.
manual cryptosystem	Cryptosystem in which the cryptographic processes are performed without the use of crypto-equipment or auto-manual devices.
manual remote rekeying	Procedure by which a distant crypto-equipment is rekeyed electrically, with specific actions required by the receiving terminal operator.
masquerading	Form of spoofing.
master crypto-ignition key	A key device with electronic logic and circuits providing the capability for adding more operational CIKs to a keyset (maximum of seven) any time after fill procedure is completed. The master CIK can only be made during the fill procedure as the first CIK.
material symbol (MATSYM) (C.F.D.)	Communications circuit identifier used for key card resupply purposes.
memory scavenging	The collection of residual information from data storage.
message authentication code	Data associated with an authenticated message allowing a receiver to verify the integrity of the message.
message externals	Information outside of the message text, such as the header, trailer, etc.
message indicator	Sequence of bits transmitted over a communications system for synchronizing crypto-equipment. Some off-line cryptosystems, such as the KL-51 and one-time pad systems, employ

	message indicators to establish decryption starting points.
mimicking	Form of spoofing.
mode of operation	Description of the conditions under which an IS operates based on the sensitivity of information processed and the clearance levels, formal access approvals, and need-to-know of its users. Four modes of operation are authorized for processing or transmitting information: dedicated mode, system-high mode, compartmented/partitioned mode, and multilevel mode.
multilevel device	Equipment trusted to properly maintain and separate data of different security categories.
multilevel mode	INFOSEC mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts: a. some users do not have a valid security clearance for all the information processed in the IS; b. all users have the proper security clearance and appropriate formal access approval for that information to which they have access; and c. all users have a valid need-to-know only for information to which they have access.
multilevel security (MLS)	Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.
mutual suspicion	Condition in which two IS's need to rely upon each other to perform a service, yet neither trusts the other to properly protect shared data.

UNCLASSIFIED

N

national security information (NSI)	Information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure.
national security system	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 40 U.S.C. Section1452, Information Technology Management Reform Act of 1996.)
need-to-know	The necessity for access to, or knowledge or possession of, specific information required to carry out official duties.
network	IS implemented with a collection of interconnected nodes.
network front-end	Device implementing protocols that allow attachment of a computer system to a network.
network reference monitor	See reference monitor.
network security	See information systems security.
network security architecture	Subset of network architecture specifically addressing security-relevant issues.
network security officer	See information systems security officer.
network sponsor	Individual or organization responsible for stating the security policy enforced by the network, designing the network security architecture to properly enforce that policy, and ensuring the

	network is implemented in such a way that the policy is enforced.
network system	System implemented with a collection of interconnected components. A network system is based on a coherent security architecture and design.
network trusted computing base (NTCB)	Totality of protection mechanisms within a network, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. See trusted computing base.
network trusted computing base (NTCB) partition	Totality of mechanisms within a single network component for enforcing the network policy, as allocated to that component; the part of the NTCB within a single network component.
network weaving	Penetration technique in which different communication networks are linked to access an IS to avoid detection and trace-back.
no-lone zone	Area, room, or space that, when staffed, must be occupied by two or more appropriately cleared individuals who remain within sight of each other. See two-person integrity.
nonrepudiation	Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.
null	Dummy letter, letter symbol, or code group inserted into an encrypted message to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes.

O

object	Passive entity containing or receiving information. Access to an object implies access to the information it contains.
object reuse	Reassignment and re-use of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium.
off-line cryptosystem	Cryptosystem in which encryption and decryption are performed independently of the transmission and reception functions.
one-part code	Code in which plain text elements and their accompanying code groups are arranged in alphabetical, numerical, or other systematic order, so one listing serves for both encoding and decoding. One-part codes are normally small codes used to pass small volumes of low-sensitivity information.
one-time cryptosystem	Cryptosystem employing key used only once.
one-time pad	Manual one-time cryptosystem produced in pad form.
one-time tape	Punched paper tape used to provide key streams on a one-time basis in certain machine cryptosystems.
on-line cryptosystem	Cryptosystem in which encryption and decryption are performed in association with the transmitting and receiving functions.
open storage	Storage of classified information within an accredited facility, but not in General Services Administration approved secure containers, while the facility is unoccupied by authorized personnel.
operational data security (C.F.D)	Protection of data from either accidental or unauthorized intentional modification, destruction, or disclosure during input, processing, storage, transmission, or output operations.

UNCLASSIFIED

operational key	Key intended for use over-the-air for protection of operational information or for the production or secure electrical transmission of key streams.
operational waiver	Authority for continued use of unmodified COMSEC end-items pending the completion of a mandatory modification.
operations code	Code composed largely of words and phrases suitable for general communications use.
operations security (OPSEC)	Process denying information to potential adversaries about capabilities and/or intentions by identifying, controlling, and protecting unclassified generic activities.
optional modification	NSA-approved modification not required for universal implementation by all holders of a COMSEC end-item. This class of modification requires all of the engineering/doctrinal control of mandatory modification but is usually not related to security, safety, TEMPEST, or reliability.
Orange Book (C.F.D)	The DoD Trusted Computer System Evaluation Criteria (DoD 5200.28-STD).
organizational maintenance	Limited maintenance performed by a user organization.
organizational registration authority (ORA)	Entity within the PKI that authenticates the identity and the organizational affiliation of the users.
over-the-air key distribution	Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation.
over-the-air key transfer	Electronically distributing key without changing traffic encryption key used on the secured communications path over which the transfer is accomplished.
over-the-air rekeying (OTAR)	Changing traffic encryption key or transmission security key in remote crypto-equipment by sending new key directly to the remote crypto-

	equipment over the communications path it secures.
overt channel	Communications path within a computer system or network designed for the authorized transfer of data. See covert channel.
overwrite procedure	Process of writing patterns of data on top of the data stored on a magnetic medium.

P

parity	Bit(s) used to determine whether a block of data has been altered.
partitioned security mode	IS security mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by an IS.
password	Protected/private alphanumeric string used to authenticate an identity or to authorize access to data.
penetration	See intrusion.
penetration testing	Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.
per-call key	Unique traffic encryption key generated automatically by certain secure telecommunications systems to secure single voice or data transmissions. See cooperative key generation.
periods processing	Processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be purged of all information from one processing period before transitioning to the next.

permuter	Device used in crypto-equipment to change the order in which the contents of a shift register are used in various nonlinear combining circuits.
plain text	Unencrypted information.
policy approving authority (PAA)	First level of the PKI Certification Management Authority that approves the security policy of each PCA.
policy certification authority (PCA)	Second level of the PKI Certification Management Authority that formulates the security policy under which it and its subordinate CAs will issue public key certificates.
positive control material	Generic term referring to a sealed authenticator system, permissive action link, coded switch system, positive enable system, or nuclear command and control documents, material, or devices.
preproduction model	Version of INFOSEC equipment employing standard parts and suitable for complete evaluation of form, design, and performance. Preproduction models are often referred to as beta models.
print suppression	Eliminating the display of characters in order to preserve their secrecy.
privacy system	Commercial encryption system that affords telecommunications limited protection to deter a casual listener, but cannot withstand a technically competent cryptanalytic attack.
privileged access	Explicitly authorized access of a specific user, process, or computer to a computer resource(s).
probe	Type of incident involving an attempt to gather information about an IS for the apparent purpose of circumventing its security controls.
production model	INFOSEC equipment in its final mechanical and electrical form.
proprietary information	Material and information relating to or associated with a company's products, business, or activities,

	including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that have been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.
protected communications (C.F.D.)	Telecommunications deriving their protection through use of type 2 products or data encryption standard equipment. See type 2 product.
protected distribution systems (PDS)	Wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control.
protection philosophy	Informal description of the overall design of an IS delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy.
protection ring	One of a hierarchy of privileged modes of an IS that gives certain access rights to user programs and processes that are authorized to operate in a given mode.
protective packaging	Packaging techniques for COMSEC material that discourage penetration, reveal a penetration has occurred or was attempted, or inhibit viewing or copying of keying material prior to the time it is exposed for use.
protective technologies	Special tamper-evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.

protective technology/ package incident (C.F.D.)	Any penetration of INFOSEC protective technology or packaging, such as a crack, cut, or tear.
protocol	Set of rules and formats, semantic and syntactic, permiting IS's to exchange information.
proxy	Software agent that performs a function or operation on behalf of another application or system while hiding the details involved.
public key certificate	Contains the name of a user, the public key component of the user, and the name of the issuer who vouches that the public key component is bound to the named user.
public cryptography (C.F.D.)	Body of cryptographic and related knowledge, study, techniques, and applications that is, or is intended to be, in the public domain.
public key cryptography (PKC)	Encryption system using a linked pair of keys. What one key encrypts, the other key decrypts.
public key infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software.
purging	Rendering stored information unrecoverable. See sanitize.

Q

QUADRANT	Short name referring to technology that provides tamper-resistant protection to crypto-equipment.

R

rainbow series (C.F.D.)	Set of publications that interpret Orange Book requirements for trusted systems.

randomizer	Analog or digital source of unpredictable, unbiased, and usually independent bits. Randomizers can be used for several different functions, including key generation or to provide a starting state for a key generator.
read	Fundamental operation in an IS that results only in the flow of information from an object to a subject.
read access	Permission to read information in an IS.
real time reaction	Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.
recovery procedures	Actions necessary to restore data files of an IS and computational capability after a system failure.
RED	Designation applied to an IS, and associated areas, circuits, components, and equipment in which unencrypted national security information is being processed.
RED/BLACK concept	Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those that handle non-national security information (BLACK) in the same form.
Red team	Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of ISs.
RED signal	Any electronic emission (e.g., plain text, key, key stream, subkey stream, initial fill, or control signal) that would divulge national security information if recovered.
reference monitor	Access control concept referring to an abstract machine that mediates all accesses to objects by subjects.
reference validation mechanism	Portion of a trusted computing base whose normal function is to control access between subjects and

	objects and whose correct operation is essential to the protection of data in the system.
release prefix	Prefix appended to the short title of U.S.-produced keying material to indicate its foreign releasability. "A" designates material that is releasable to specific allied nations and "U.S." designates material intended exclusively for U. S. use.
remanence	Residual information remaining on storage media after clearing. See magnetic remanence and clearing.
remote rekeying	Procedure by which a distant crypto-equipment is rekeyed electrically. See automatic remote rekeying and manual remote rekeying.
repair action	NSA-approved change to a COMSEC end-item that does not affect the original characteristics of the end-item and is provided for optional application by holders. Repair actions are limited to minor electrical and/or mechanical improvements to enhance operation, maintenance, or reliability. They do not require an identification label, marking, or control but must be fully documented by changes to the maintenance manual.
reserve keying material	Key held to satisfy unplanned needs. See contingency key.
residual risk	Portion of risk remaining after security measures have been applied.
residue	Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place.
resource encapsulation	Method by which the reference monitor mediates accesses to an IS resource. Resource is protected and not directly accessible by a subject. Satisfies requirement for accurate auditing of resource usage.
risk	Possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability.

UNCLASSIFIED

risk analysis	Examination of information to identify the risk to an IS.
risk assessment	Formal description and evaluation of risk to an IS.
risk index	Difference between the minimum clearance or authorization of IS users and the maximum sensitivity (e.g., classification and categories) of data processed by the system.
risk management	Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.

S

safeguarding statement	Statement affixed to a computer output or printout that states the highest classification being processed at the time the product was produced and requires control of the product, at that level, until determination of the true classification by an authorized person. Synonymous with banner.
sanitize	Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs. See purging.
scavenging	Searching through object residue to acquire data.
scratch pad store (SPS) (C.F.D.)	Temporary key storage in crypto-equipment.
secure communications	Telecommunications deriving security through use of type 1 products and/or PDSs.
secure hash standard	Specification for a secure hash algorithm that can generate a condensed message representation called a message digest.
secure operating system (C.F.D.)	Resident software controlling hardware and other software functions in an IS to provide a level of protection or security appropriate to the

	classification, sensitivity, and/or criticality of the data and resources it manages.
secure state	Condition in which no subject can access any object in an unauthorized manner.
secure subsystem	Subsystem containing its own implementation of the reference monitor concept for those resources it controls. Secure subsystem must depend on other controls and the base operating system for the control of subjects and the more primitive system objects.
security fault analysis (SFA)	Assessment, usually performed on IS hardware, to determine the security properties of a device when hardware fault is encountered.
security features users guide (SFUG)	Guide or manual explaining how the security mechanisms in a specific system work.
security filter	IS trusted subsystem that enforces security policy on the data passing through it.
security flaw (C.F.D.)	Error of commission or omission in an IS that may allow protection mechanisms to be bypassed. See vulnerability.
security inspection	Examination of an IS to determine compliance with security policy, procedures, and practices.
security kernel	Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct.
security label	Information representing the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).
security net control station	Management system overseeing and controlling implementation of network security policy.

UNCLASSIFIED

security perimeter	All components/devices of an IS to be accredited. Separately accredited components generally are not included within the perimeter.
security policy	See information systems security policy.
security range	Highest and lowest security levels that are permitted in or on an IS, system component, subsystem, or network.
security requirements	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet IS security policy.
security requirements baseline	Description of the minimum requirements necessary for an IS to maintain an acceptable level of security.
security safeguards	Protective measures and controls prescribed to meet the security requirements specified for an IS. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. See accreditation.
security specification	Detailed description of the safeguards required to protect an IS.
security test and evaluation (ST&E)	Examination and analysis of the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of that system.
security testing	Process to determine that an IS protects data and maintains functionality as intended.
seed key	Initial key used to start an updating or key generation process.
sensitive information	Information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the

	interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235).)
sensitivity label	Information representing elements of the security label(s) of a subject and an object. Sensitivity labels are used by the trusted computing base (TCB) as the basis for mandatory access control decisions.
shielded enclosure	Room or container designed to attenuate electromagnetic radiation.
short title	Identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and controlling.
simple security property	Bell-La Padula security model rule allowing a subject read access to an object, only if the security level of the subject dominates the security level of the object.
single-level device (C.F.D.)	IS device not trusted to properly maintain and separate data to different security levels.
single point keying	Means of distributing key to multiple, local crypto-equipment or devices from a single fill point.
sniffer	Software tool for auditing and identifying network traffic packets.
software system test and evaluation process	Process that plans, develops, and documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational, and interface requirements.
special mission modification (C.F.D.)	Mandatory or optional modification that applies only to a specific mission, purpose, operational, or environmental need.
speech privacy (C.F.D.)	Techniques using fixed sequence permutations or voice/speech inversion to render speech unintelligible to the casual listener.

UNCLASSIFIED

split knowledge	Separation of data or information into two or more parts, each part constantly kept under control of separate authorized individuals or teams so that no one individual or team will know the whole data.
spoofing	Unauthorized use of legitimate Indentification and Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.
spread spectrum	Telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. Frequency hopping, direct sequence spreading, time scrambling, and combinations of these techniques are forms of spread spectrum.
star (*) property	Bell-La Padula security model rule allowing a subject write access to an object only if the security level of the object dominates the security level of the subject.
start-up KEK	Key-encryption-key held in common by a group of potential communicating entities and used to establish ad hoc tactical networks.
state variable	Variable representing either the state of an IS or the state of some system resource.
storage object	An object supporting both read and write accesses to an IS.
subassembly	Major subdivision of an assembly consisting of a package of parts, elements, and circuits that perform a specific function.
subject	Generally a person, process, or device causing information to flow among objects or change to the system state.
subject security level	Sensitivity label(s) of the objects to which the subject has both read and write access. Security level of a subject must always be dominated by the clearance level of the user associated with the subject.

sub-registration authority (SRA) (C.F.D.)	Individual with primary responsibility for managing the distinguished name process.
superencryption	Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, on-line circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted.
supersession	Scheduled or unscheduled replacement of a COMSEC aid with a different edition.
superuser (C.F.D.)	Special user who can perform control of processes, devices, networks, and file systems.
supervisor state	Synonymous with executive state of an operating system.
suppression measure	Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in an IS.
surrogate access	See discretionary access control.
syllabary	List of individual letters, combination of letters, or syllables, with their equivalent code groups, used for spelling out words or proper names not present in the vocabulary of a code. A syllabary may also be a spelling table.
symmetric key	Encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret.
synchronous crypto-operation	Method of on-line crypto-operation in which crypto-equipment and associated terminals have timing systems to keep them in step.
system administrator (SA)	Individual responsible for the installation and maintenance of an IS, providing effective IS utilization, adequate security parameters, and sound implementation of established INFOSEC policy and procedures.

system assets	Any software, hardware, data, administrative, physical, communications, or personnel resource within an IS.
system development methodologies	Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.
system high	Highest security level supported by an IS.
system high mode	IS security mode of operation wherein each user, with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts, has all of the following: a. valid security clearance for all information within an IS; b. formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs); and c. valid need-to- know for some of the information contained within the IS.
system indicator	Symbol or group of symbols in an off-line encrypted message identifying the specific cryptosystem or key used in the encryption.
system integrity	Attribute of an IS when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
system low	Lowest security level supported by an IS.
system profile	Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IS.
system security	See information systems security.
system security engineering	See information systems security.
system security evaluation (C.F.D.)	Risk assessment of a system, considering its vulnerabilities and perceived security threat.

UNCLASSIFIED

system security management plan (C.F.D.)	Formal document fully describing the responsibilities for security tasks planned to meet system security requirements.
system security officer	See information system security officer.
system security plan (C.F.D.)	Formal document fully describing the planned security tasks required to meet system security requirements.

T

tampering	Unauthorized modification altering the proper functioning of INFOSEC equipment.
telecommunications	Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.
telecommunications and automated information systems security (C.F.D.)	Superseded by information systems security.
telecommunications security (TSEC)	See information systems security.
TEMPEST	Short name referring to investigation, study, and control of compromising emanations from IS equipment.
TEMPEST test	Laboratory or on-site test to determine the nature of compromising emanations associated with an IS.
TEMPEST zone	Designated area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated.
test key	Key intended for testing of COMSEC equipment or systems.
threat	Any circumstance or event with the potential to adversely impact an IS through unauthorized

	access, destruction, disclosure, modification of data, and/or denial of service.
threat analysis	Examination of information to identify the elements comprising a threat.
threat assessment	Formal description and evaluation of threat to an IS.
threat monitoring	Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.
ticket-oriented	IS protection system in which each subject maintains a list of unforgeable bit patterns called tickets, one for each object a subject is authorized to access. See list-oriented.
time bomb	Resident computer program that triggers an unauthorized act at a predefined time.
time-compliance date	Date by which a mandatory modification to a COMSEC end-item must be incorporated if the item is to remain approved for operational use.
time-dependent password	Password that is valid only at a certain time of day or during a specified interval of time.
traditional COMSEC program	Program in which NSA acts as the central procurement agency for the development and, in some cases, the production of INFOSEC items. This includes the Authorized Vendor Program. Modifications to the INFOSEC end-items used in products developed and/or produced under these programs must be approved by NSA.
traffic analysis (TA)	Study of communications patterns.
traffic encryption key (TEK)	Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.
traffic-flow security (TFS)	Measure used to conceal the presence of valid messages in an on-line cryptosystem or secure communications system.

traffic padding	Generation of spurious communications or data units to disguise the amount of real data units being sent.
training key (C.F.D.)	Cryptographic key for training.
tranquility	Property whereby the security level of an object cannot change while the object is being processed by an IS.
transmission security (TRANSEC)	Component of COMSEC resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.
trap door	Synonymous with back door.
trojan horse	Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. See malicious code.
trusted computer system	IS employing sufficient hardware and software assurance measures to allow simultaneous processing of a range of classified or sensitive information.
trusted computing base (TCB)	Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.
trusted distribution	Method for distributing trusted computing base (TCB) hardware, software, and firmware components that protects the TCB from modification during distribution.
trusted facility manual	Document containing the operational requirements; security environment; hardware and software configurations and interfaces; and all security procedures, measures, and contingency plans.
trusted identification forwarding	Identification method used in IS networks whereby the sending host can verify an authorized user on its system is attempting a connection to another

	host. The sending host transmits the required user authentication information to the receiving host.
trusted path	Mechanism by which a person using a terminal can communicate directly with the trusted computing base (TCB). Trusted path can only be activated by the person or the TCB and cannot be imitated by untrusted software.
trusted process	Process that has privileges to circumvent the system security policy and has been tested and verified to operate only as intended.
trusted recovery	Ability to ensure recovery without compromise after a system failure.
trusted software	Software portion of a trusted computing base (TCB).
TSEC nomenclature	System for identifying the type and purpose of certain items of COMSEC material.
tunneling	Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.
two-part code	Code consisting of an encoding section, in which the vocabulary items (with their associated code groups) are arranged in alphabetical or other systematic order, and a decoding section, in which the code groups (with their associated meanings) are arranged in a separate alphabetical or numeric order.
two-person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.
two-person integrity (TPI)	System of storage and handling designed to prohibit individual access to certain COMSEC

	keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. See no-lone zone.
type 1 product	Classified or controlled cryptographic item endorsed by the NSA for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products, and not to information, key, services, or controls. Type 1 products contain classified NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.
type 2 product	Unclassified cryptographic equipment, assembly, or component, endorsed by the NSA, for use in national security systems as defined in Title 40 U.S.C. Section 1452.
type 3 algorithm	Cryptographic algorithm registered by the National Institute of Standards and Technology (NIST) and published as a Federal Information Processing Standard (FIPS) for use in protecting unclassified sensitive information or commercial information.
type 4 algorithm	Unclassified cryptographic algorithm that has been registered by the National Institute of Standards and Technology (NIST), but not published as a Federal Information Processing Standard (FIPS).

U

unauthorized disclosure	Type of event involving exposure of information to individuals not authorized to receive it.
unclassified	Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified.

untrusted process	Process that has not been evaluated or examined for adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.
updating	Automatic or manual cryptographic process that irreversibly modifies the state of a COMSEC key, equipment, device, or system.
user	Person or process authorized to access an IS. (PKI) Individual defined, registered, and bound to a public key structure by a certification authority (CA).
user ID	Unique symbol or character string used by an IS to identify a specific user.
User Partnership Program (UPP)	Partnership between the NSA and a U.S. Government agency to facilitate development of secure IS equipment incorporating NSA-approved cryptography. The result of this program is the authorization of the product or system to safeguard national security information in the user's specific application.
user profile	Patterns of a user's activity that can show changes from normal behavior.
user representative	Person authorized by an organization to order COMSEC keying material and interface with the keying system, provide information to key users, and ensure the correct type of key is ordered.
U.S.-controlled facility	Base or building to which access is physically controlled by U.S. persons who are authorized U.S. Government or U.S. Government contractor employees.
U.S.-controlled space	Room or floor within a facility that is not a U.S.-controlled facility, access to which is physically controlled by U.S. persons who are authorized U.S. Government or U.S. Government contractor employees. Keys or combinations to locks controlling entrance to U.S.-controlled spaces must be under the exclusive control of U.S. persons who

	are U.S. Government or U.S. Government contractor employees.
U.S. person	U.S. citizen or a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in U.S., except for a corporation directed and controlled by a foreign government or governments.

V

validation	Process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an IS by one or more departments or agencies and their contractors.
variant	One of two or more code symbols having the same plain text equivalent.
verification	Process of comparing two levels of an IS specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code).
verified design (C.F.D.)	Computer protection class in which formal security verification methods are used to assure mandatory and discretionary security controls can effectively protect classified and sensitive information stored in, or processed by, the system. Class A1 system is verified design.
virtual password (C.F.D.)	IS password computed from a passphrase meeting the requirements of password storage (e.g., 64 bits).
virtual private network (VPN)	Protected IS link utilizing tunneling, security controls (see information assurance), and end-point address translation giving the impression of a dedicated line.

virus	Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.
vulnerability	Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.
vulnerability analysis	Examination of information to identify the elements comprising a vulnerability.
vulnerability assessment	Formal description and evaluation of vulnerabilities of an IS.

W

work factor	Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure.
worm	See malicious code.
write	Fundamental operation in an IS that results only in the flow of information from a subject to an object. See access type.
write access	Permission to write to an object in an IS.

Z

zero fill	To fill unused storage locations in an IS with the representation of the character denoting "0."
zeroize	To remove or eliminate the key from a crypto-equipment or fill device.
zone of control	Synonymous with inspectable space.

SECTION II

COMMONLY USED ABBREVIATIONS AND ACRONYMS

ACL	Access Control List
ACO	Access Control Officer
ADM (C.F.D.)	Advanced Development Model
AE (C.F.D.)	Application Entity
AIG	Address Indicator Group
AIN	Advanced Intelligence Network
AIRK (C.F.D.)	Area Interswitch Rekeying Key
AJ (C.F.D.)	Anti-Jamming
AK	Automatic Remote Rekeying
AKDC (C.F.D.)	Automatic Key Distribution Center
AKD/RCU	Automatic Key Distribution/Rekeying Control Unit
AKMC (C.F.D.)	Automated Key Management Center
AKMS (C.F.D.)	Automated Key Management System
ALC	Accounting Legend Code
AMS	1. Auto-Manual System 2. Autonomous Message Switch
ANDVT	Advanced Narrowband Digital Voice Terminal
ANSI	American National Standards Institute
AOSS (C.F.D.)	Automated Office Support Systems
APC	Adaptive Predictive Coding
APU	Auxiliary Power Unit
ARPANET (C.F.D.)	Advanced Research Projects Agency Network

ASCII	American Standard Code for Information Interchange
ASPJ (C.F.D.)	Advanced Self-Protection Jammer
ASSIST Program	Automated Information System Security Incident Support Team
ASU (C.F.D.)	Approval for Service Use
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
AV (C.F.D.)	Auxiliary Vector
AVP	Authorized Vendor Program
C2	1. Command and Control 2. Controlled Access Protection (C.F.D.)
C3	Command, Control, and Communications
C3I	Command, Control, Communications and Intelligence
C4	Command, Control, Communications and Computers
CA	1. Controlling Authority 2. Cryptanalysis 3. COMSEC Account 4. Command Authority 5. Certification Authority
C&A	Certification and Accreditation
CAW	Certificate Authority Workstation
CCEP	Commercial COMSEC Endorsement Program
CCI	Controlled Cryptographic Item
CCO	Circuit Control Officer
CDS (C.F.D.)	Cryptographic Device Services
CEOI	Communications Electronics Operating Instruction

CEPR	Compromising Emanation Performance Requirement
CER	1. Cryptographic Equipment Room 2. Communication Equipment Room
CERT	Computer Security Emergency Response Team
CFD	Common Fill Device
CIAC	Computer Incident Assessment Capability
CIK	Crypto-Ignition Key
CIP (C.F.D.)	Crypto-Ignition Plug
CIRK (C.F.D.)	Common Interswitch Rekeying Key
CIRT	Computer Security Incident Response Team
CK (C.F.D.)	Compartment Key
CKG	Cooperative Key Generation
CMCS	COMSEC Material Control System
CNA	Computer Network Attack
CNCS (C.F.D.)	Cryptonet Control Station
CND	Computer Network Defense
CNK (C.F.D.)	Cryptonet Key
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOP	Concept of Operations
COR	1. Central Office of Record (COMSEC) 2. Contracting Officer Representative
COTS	Commercial-off-the-shelf
CPS (C.F.D.)	COMSEC Parent Switch
CPU	Central Processing Unit

CRL	Certificate Revocation List
CRP (C.F.D.)	COMSEC Resources Program (Budget)
Crypt/Crypto	Cryptographic-related
CSE	Communications Security Element
CSS	1. COMSEC Subordinate Switch 2. Constant Surveillance Service (Courier) 3. Continuous Signature Service (Courier) 4. Coded Switch System
CSSO	Contractor Special Security Officer
CSTVRP	Computer Security Technical Vulnerability Report Program
CTAK	Cipher Text Auto-Key
CT&E	Certification Test and Evaluation
CTTA	Certified TEMPEST Technical Authority
CUP	COMSEC Utility Program
DAA	1. Designated Approving Authority 2. Designated Accrediting Authority 3. Delegated Accrediting Authority
DAC	Discretionary Access Control
DAMA	Demand Assigned Multiple Access
DCID	Director Central Intelligence Directive
DCS	1. Defense Communications System 2. Defense Courier Service
DCSP (C.F.D.)	Design Controlled Spare Part(s)
DDS	Dual Driver Service (courier)
DES	Data Encryption Standard
DIB (C.F.D.)	Directory Information Base
DISN	Defense Information System Network

DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD TCSEC (C.F.D.)	Department of Defense Trusted Computer System Evaluation Criteria
DLED (C.F.D.)	Dedicated Loop Encryption Device
DMA	Direct Memory Access
DMS	Defense Message System
DPL (C.F.D.)	Degausser Products List (a section in the INFOSEC Products and Services Catalogue)
DSA	Digital Signature Algorithm
DSN	Defense Switched Network
DSVT	Digital Subscriber Voice Terminal
DTLS	Descriptive Top-Level Specification
DTD	Data Transfer Device
DTS	Diplomatic Telecommunications Service
DUA	Directory User Agent
EAM	Emergency Action Message
ECCM	Electronic Counter-Countermeasures
ECM	Electronic Countermeasures
ECPL	Endorsed Cryptographic Products List (a section in the Information Systems Security Products and Services Catalogue)
EDAC	Error Detection and Correction
EDESPL (C.F.D.)	Endorsed Data Encryption Standard Products List
EDM (C.F.D.)	Engineering Development Model
EFD	Electronic Fill Device
EFTO	Encrypt For Transmission Only

EGADS (C.F.D.)	Electronic Generation, Accounting, and Distribution System
EKMS	Electronic Key Management System
ELINT	Electronic Intelligence
ELSEC (C.F.D.)	Electronic Security
E Model	Engineering Development Model
EMSEC (C.F.D.)	Emissions Security
EPL	Evaluated Products List (a section in the INFOSEC Products and Services Catalogue)
ERTZ	Equipment Radiation TEMPEST Zone
ETL (C.F.D.)	Endorsed Tools List
ETPL	Endorsed TEMPEST Products List
EUCI (C.F.D.)	Endorsed for Unclassified Cryptographic Information
EV (C.F.D.)	Enforcement Vector
FDDI (C.F.D.)	Fiber Distributed Data Interface
FDIU	Fill Device Interface Unit
FIPS	Federal Information Processing Standard
FOCI	Foreign Owned, Controlled or Influenced
FOUO	For Official Use Only
FSRS	Functional Security Requirements Specification
FSTS	Federal Secure Telephone Service
FTS	Federal Telecommunications System
FTAM	File Transfer Access Management
FTLS	Formal Top-Level Specification
GCCS	Global Command and Control System

GETS	Government Emergency Telecommunications Service
GPS	Global Positioning System
GTS	Global Telecommunications Service
GWEN	Ground Wave Emergency Network
HDM (C.F.D.)	Hierarchical Development Methodology
HUS (C.F.D.)	Hardened Unique Storage
HUSK (C.F.D.)	Hardened Unique Storage Key
IA	Information Assurance
I&A	Identification and Authentication
IBAC	Identity Based Access Control
ICU	Interface Control Unit
IDS	Intrusion Detection System
IEMATS	Improved Emergency Message Automatic Transmission System
IFF	Identification, Friend or Foe
IFFN	Identification, Friend, Foe, or Neutral
IIRK (C.F.D.)	Interarea Interswitch Rekeying Key
ILS	Integrated Logistics Support
INFOSEC	Information Systems Security
IO	Information Operations
IP	Internet Protocol
IPM	Interpersonal Messaging
IPSO	Internet Protocol Security Option
IR (C.F.D.)	Information Ratio
IRK (C.F.D.)	Interswitch Rekeying Key

IS	Information System
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISS (C.F.D.)	Information Systems Security
ISSE	Information Systems Security Engineering
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITAR	International Traffic in Arms Regulation
ITSEC	Information Technology Security Evaluation Criteria
KAK	Key-Auto-Key
KDC	Key Distribution Center
KEK	Key Encryption Key
KG	Key Generator
KMASE (C.F.D.)	Key Management Application Service Element
KMC	Key Management Center
KMID	Key Management Identification Number
KMODC	Key Management Ordering and Distribution Center
KMP	Key Management Protocol
KMPDU (C.F.D.)	Key Management Protocol Data Unit
KMS	Key Management System
KMSA (C.F.D.)	Key Management System Agent
KMUA (C.F.D.)	Key Management User Agent
KP	Key Processor

KPK	Key Production Key
KSD	Key Storage Device
KSOS (C.F.D.)	Kernelized Secure Operating System
KVG (C.F.D.)	Key Variable Generator
LEAD	Low-Cost Encryption/Authentication Device
LEAF (C.F.D.)	Law Enforcement Access Field
LKG (C.F.D.)	Loop Key Generator
LMD	Local Management Device
LMD/KP	Local Management Device/Key Processor
LME (C.F.D.)	Layer Management Entry
LMI (C.F.D.)	Layer Management Interface
LOCK	Logical Co-Processing Kernel
LPC	Linear Predictive Coding
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LRIP	Limited Rate Initial Preproduction
LSI	Large Scale Integration
MAC	1. Mandatory Access Control 2. Message Authentication Code
MAN	1. Mandatory Modification 2. Metropolitan Area Network
MATSYM (C.F.D.)	Material Symbol
MCCB (C.F.D.)	Modification/Configuration Control Board
MDC (C.F.D.)	Manipulation Detection Code
MEECN (C.F.D.)	Minimum Essential Emergency Communications Network

MEP (C.F.D.)	Management Engineering Plan
MER	Minimum Essential Requirements
MHS	Message Handling System
MI	Message Indicator
MIB	Management Information Base
MIJI (C.F.D.)	Meaconing, Intrusion, Jamming, and Interference
MINTERM	Miniature Terminal
MISSI	Multilevel Information Systems Security Initiative
MLS	Multilevel Security
MRT (C.F.D.)	Miniature Receiver Terminal
MSE	Mobile Subscriber Equipment
NACAM	National COMSEC Advisory Memorandum
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NAK	Negative Acknowledge
NCCD	Nuclear Command and Control Document
NCS	1. National Communications System 2. National Cryptologic School 3. Net Control Station
NCSC	National Computer Security Center
NISAC	National Industrial Security Advisory Committee
NIST	National Institute of Standards and Technology
NKSR (C.F.D.)	Nonkernel Security Related
NLZ	No-Lone Zone
NSA	National Security Agency
NSAD (C.F.D.)	Network Security Architecture and Design

NSD	National Security Directive
NSDD	National Security Decision Directive
NSEP	National Security Emergency Preparedness
NSI	National Security Information
NSO (C.F.D.)	Network Security Officer
NSTAC	National Security Telecommunications Advisory Committee
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory/Information Memorandum
NSTISSC	National Security Telecommunications and Information Systems Security Committe
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTCB	Network Trusted Computing Base
NTIA	National Telecommunications and Information Administration
NTISSAM	National Telecommunications and Information Systems Security Advisory/Information Memorandum
NTISSD	National Telecommunications and Information Systems Security Directive
NTISSI	National Telecommunications and Information Systems Security Instruction
NTISSP	National Telecommunications and Information Systems Security Policy
OADR	Originating Agency's Determination Required

OPCODE	Operations Code
OPSEC	Operations Security
ORA	Organizational Registration Authority
OTAD	Over-the-Air Key Distribution
OTAR	Over-the-Air Rekeying
OTAT	Over-the-Air Key Transfer
OTP	One-Time Pad
OTT	One-Time Tape
PAA	Policy Approving Authority
PAAP (C.F.D.)	Peer Access Approval
PAE (C.F.D.)	Peer Access Enforcement
PAL	Permissive Action Link
PC	Personal Computer
PCA	Policy Certification Authority
PCMCIA	Personal Computer Memory Card International Association
PCZ (C.F.D.)	Protected Communications Zone
PDR	Preliminary Design Review
PDS	1. Protected Distribution Systems 2. Practices Dangerous to Security
PDU (C.F.D.)	Protocol Data Unit
PES	Positive Enable System
PKA (C.F.D.)	Public Key Algorithm
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PKSD	Programmable Key Storage Device

P model	Preproduction Model
PNEK	Post-Nuclear Event Key
PPL	Preferred Products List (a section in the INFOSEC Products and Services Catalogue)
PRBAC (C.F.D.)	Partition Rule Base Access Control
PROM	Programmable Read-Only Memory
PROPIN	Proprietary Information
PSL (C.F.D.)	Protected Services List
PWDS	Protected Wireline Distribution System
RACE (C.F.D.)	Rapid Automatic Cryptographic Equipment
RAMP	Rating Maintenance Program
RQT (C.F.D.)	Reliability Qualification Tests
SA	System Administrator
SABI	Secret and Below Interoperability
SAO	Special Access Office
SAP	1. System Acquisition Plan 2. Special Access Program
SARK	SAVILLE Advanced Remote Keying
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDNRIU (C.F.D.)	Secure Digital Net Radio Interface Unit
SDNS	Secure Data Network System
SDR	System Design Review
SFA	Security Fault Analysis
SHA	Secure Hash Algorithm

SFUG	Security Features Users Guide
SI	Special Intelligence
SIGSEC (C.F.D.)	Signals Security
SISS	Subcommittee on Information Systems Security
SMU	Secure Mobile Unit
SPK	Single Point Key(ing)
SPS (C.F.D.)	Scratch Pad Store
SRA (C.F.D.)	Sub-Registration Authority
SRR	Security Requirements Review
SSO	Special Security Officer
SSP	System Security Plan
ST&E	Security Test and Evaluation
STE	Secure Terminal Equipment
STS	Subcommittee on Telecommunications Security
STU	Secure Telephone Unit
TA	Traffic Analysis
TACTED (C.F.D.)	Tactical Trunk Encryption Device
TACTERM	Tactical Terminal
TAG	TEMPEST Advisory Group
TCB	Trusted Computing Base
TCD (C.F.D.)	Time Compliance Data
TCSEC (C.F.D.)	DoD Trusted Computer System Evaluation Criteria
TD (C.F.D.)	Transfer Device
TED	Trunk Encryption Device
TEK	Traffic Encryption Key

TEP	TEMPEST Endorsement Program
TFM	Trusted Facility Manual
TFS	Traffic Flow Security
TLS	Top-Level Specification
TNI (C.F.D.)	Trusted Network Interpretation
TNIEG (C.F.D.)	Trusted Network Interpretation Environment Guideline
TPC	Two-Person Control
TPEP	Trusted Products Evaluation Program
TPI	Two-Person Integrity
TRANSEC	Transmission Security
TRB	Technical Review Board
TRI-TAC	Tri-Service Tactical Communications System
TSCM	Technical Surveillance Countermeasures
TSEC	Telecommunications Security
TSK (C.F.D.)	Transmission Security Key
UA	User Agent
UIRK (C.F.D.)	Unique Interswitch Rekeying Key
UIS	User Interface System
UPP	User Partnership Program
USDE (C.F.D.)	Undesired Signal Data Emanations
V model (C.F.D.)	Advanced Development Model
VPN	Virtual Private Network
XDM/X Model (C.F.D.)	Experimental Development Model/Exploratory Development Model

Page 3956 of 3957

SECTION III

REFERENCES

a. National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, 5 July 1990.

b. Executive Order 12958, National Security Information, dated 29 September 1995.

c. Executive Order 12333, United States Intelligence Activities, dated 4 December 1981.

d. Public Law 100-235, Computer Security Act of 1987, dated 8 January 1988.

e. 10 United States Codes Section 2315.

f. 44 United States Code Section 3502(2), Public Law 104-13, Paperwork Reduction Act of 1995, dated 22 May 1995.

g. Information Technology Management Reform Act of 1996 (within Public Law 104-106, DoD Authorization Act of 1996).

h. NSA Information Systems Security Organization Regulation 90-16, dated 29 October 1996.

Page 3957 of 3957